COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/529/2022

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 **Coordinación de Servicios Administrativos Morelos,** la **Coordinación de Vinculación y Transferencia Tecnológica,** la **Dirección General de Cómputo y Tecnologías de Información y Comunicación,** la **Dirección General de Repositorios Universitarios,** la **Dirección General de Comunicación Social**, el **Instituto de Ciencias del Mar y Limnología,** la **Coordinación General de Estudios de Posgrado** y la **Dirección General de Asuntos Jurídicos,** en relación con sus respectivos **Documentos de Seguridad**, se procede a dictar la presente resolución con base en los siguientes:

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

I. Con fecha 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, 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 Púbica 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 **CSAMorelos/533.01/0289/2022**, recibido fecha 18 de agosto del 2022, dirigido a la Presidencia del Comité de Transparencia, la **Coordinación de Servicios Administrativos Morelos,** 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[1]; 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.*

[1] *DOF: 26 de noviembre de 2021*

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 obra en el Sistema de Gestión de Seguridad de Datos Personales de esta área universitaria. El documento de seguridad contiene los siguientes apartados, cuya autorización de reserva total se solicita a ese Comité:

Anexos o Políticas	***Contenido y su afectación***	***Páginas***
a) Análisis de riesgos	*El análisis de riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica de esta área universitaria, y otorga herramientas a las personas para implementar un ataque informático a los activos críticos y no críticos.*	*16 -40*
b) Análisis de brecha	*El análisis de brecha integra información relativa a la seguridad de la infraestructura tecnológica; enlistan los controles de seguridad con los que cuenta esta área; y menciona las herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información.*	*16 -40*
c) Plan de Trabajo	*El plan de trabajo define los controles de seguridad a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes con base en el riesgo real detectado. El uso de esta información permite inferir nuestros riesgos, por cuánto tiempo seguirán así hasta el momento que se implementen nuevos controles.*	*16 -40*

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 ... 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 riego real el hecho de que toda persona que quiera ocasionar la pérdida, destrucción, robo, copia, uso, acceso o tratamiento no autorizado, daño, alteración o modificación no autorizada de datos personales, puede hacerlo si cuenta con la información exacta de las vulnerabilidades de un área universitaria, lo que esta serie de documentos les otorga directamente si se difundiera la información.*

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

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

La prueba de daño precitada, 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.

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).

VIII. Mediante oficio **CVTT/038/2022**, recibido fecha 18 de agosto del 2022, dirigido a la Presidencia del Comité de Transparencia, la **Coordinación de Vinculación y Transferencia Tecnológica** 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[2]; 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

[2] *DOF: 26 de noviembre de 2021*

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:

Anexos o Políticas	***Contenido y su afectación***	***Páginas***
Anexo 1. Inventario de sistemas de tratamiento de datos personales	*El inventario de los sistemas de tratamiento de datos personales contiene información sobre las rutas de acceso a soportes digitales de la información y cuentas, los cuales pueden ser utilizados para un ataque informático a los activos críticos y no críticos.*	*12-95*
Anexo 2. Estructura y descripción de los sistemas de tratamiento de datos personales	*La estructura y descripción de los sistemas de tratamiento de datos personales contiene información sobre las rutas y métodos de acceso a soportes digitales y físicos de la información, los cuales pueden ser utilizados para un ataque a los activos críticos y no críticos.*	*97-128*
Anexo 3. Diagramas de arquitectura	*Los diagramas de arquitectura de los soportes digitales contienen el flujo de información entre los componentes, sus rutas de acceso a soportes digitales y describe las medidas de seguridad implementadas, información que puede ser utilizada para un ataque informático a los activos críticos y no críticos.*	*130-156*

Anexo 5. Análisis de riesgos y análisis de brecha	*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.* *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.*	*270-381*
Anexo 6. Plan de Trabajo	*El plan de trabajo define los controles de seguridad a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes con base en el riesgo real detectado. El uso de esta información permite inferir nuestros riesgos, por cuánto tiempo seguirán así hasta el momento que se implementen nuevos controles.*	*383-389*

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 inventario, estructura y descripción de los sistemas de tratamiento de datos personales, diagramas de arquitectura, análisis de riesgo, el análisis de brecha ... y el plan de trabajo de esta dependencia contienen información de cómo se protegen los datos personales de los titulares que nos confiaron su información personal y que es nuestra responsabilidad garantizar. Es un riesgo real el hecho de que toda persona que quiera ocasionar la pérdida, destrucción, robo, copia, uso, acceso o tratamiento no autorizado, daño, alteración o modificación no autorizada de datos personales, puede hacerlo si cuenta con la información exacta de las vulnerabilidades de un área universitaria, lo que esta serie de documentos les otorga directamente si se difundiera la información.*

- *Divulgar el inventario, estructura y descripción de los sistemas de tratamiento de datos personales, diagramas de arquitectura, análisis de riesgo, el análisis de brecha ... y el plan de trabajo de esta dependencia evidencian los nuevos*

controles que estamos pendientes de implementar, describen la forma en cómo almacenamos técnicamente los datos personales, cómo protegemos los sistemas automatizados de información, qué medidas de seguridad administrativas, físicas y técnicas planeamos establecer de manera gradual y de conformidad con las prioridades y presupuestos otorgado.

- *En este sentido la revelación de la información que obra el inventario, estructura y descripción de los sistemas de tratamiento de datos personales, diagramas de arquitectura, 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, 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 inventario, estructura y descripción de los sistemas de tratamiento de datos personales, diagramas de arquitectura, análisis de riesgo, el análisis de brecha, las políticas de respaldo 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 inventario, estructura y descripción de los sistemas de tratamiento de datos personales, diagramas de arquitectura, 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).

IX. Mediante oficio **ET/DGTIC/040/2022**, recibido con fecha 19 de agosto del 2022, dirigido a la Presidencia del Comité de Transparencia, la **Dirección General de Cómputo y Tecnologías de Información y Comunicación** 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[3]; 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

[3] *DOF: 26 de noviembre de 2021*

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 dependencia universitaria. El documento de seguridad contiene los siguientes apartados cuya autorización de reserva … se solicita a ese Comité de la siguiente forma:

Reserva total o parcial	***Anexos o Políticas***	***Contenido y su afectación***	***Páginas***
Reserva Parcial	***a)*** *Inventario de datos personales*	*El inventario contiene información técnica y operativa que permite identificar los espacios físicos e infraestructura tecnológica en que se resguardan datos personales*	*19 de 47*
Reserva Total	***b)*** *Análisis de riesgos*	*El análisis de riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica de esta área universitaria, y otorga herramientas a las personas para implementar un ataque informático a los activos críticos y no críticos.*	*63*
Reserva Total	***c)*** *Análisis de brecha*	*El análisis de brecha integra información relativa a la seguridad de la infraestructura tecnológica; enlistan los controles de seguridad con los que cuenta esta área; y menciona las herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información.*	*20*
Reserva Total	***d)*** *Plan de Trabajo y Medidas de Seguridad.*	*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.*	*1*
Reserva	***e)*** *Política de*	*Las políticas contienen información*	*4*

Total	*autenticación y control de acceso*	*del conjunto de reglas diseñadas para determinar a quién se le concede acceso a un lugar restringido o a una información restringida relacionada con los datos personales en posesión de la dependencia.*	
Reserva Total	***f)** Política de seguridad física y ambiental*	*Las políticas contienen información sobre las medidas que se adoptarán para proteger los sistemas, los edificios y la infraestructura de apoyo de los sistemas de datos personales contra las amenazas asociadas con ambiente físico.*	*4*

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 el inventario de datos personales, análisis de riesgo, el análisis de brecha, las políticas de autenticación y control de acceso, así como de seguridad física y ambiental 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 inventario de datos personales, análisis de riesgo, el análisis de brecha, las políticas de autenticación y control de acceso, así como de seguridad física y ambiental 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 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 … 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, 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 inventario de datos personales, análisis de riesgo, el análisis de brecha las políticas de autenticación y control de acceso, así como de Seguridad física y ambiental y el plan de trabajo de esta dependencia 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 dependencia, 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 inventario de datos personales, análisis de riesgo, al análisis de brecha, las políticas de autenticación y control de acceso, así como de Seguridad física y ambiental y al plan de trabajo de esta dependencia 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 parcial del inventario de datos personales, y la reserva total del análisis de riesgo, el análisis de brecha, las políticas de autenticación y control de acceso, así como de Seguridad física y ambiental y el plan de trabajo cada uno de esos documentos, que obran como anexos y políticas del documento de seguridad de esta dependencia 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 **DGRU/DG/090/2022/am** recibido con fecha 19 de agosto del 2022, dirigido a la Presidencia del Comité de Transparencia, la **Dirección General de Repositorios Universitarios** 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[4]; 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.

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:

[4] *DOF: 26 de noviembre de 2021*

COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/529/2022

Anexos o Políticas	***Contenido y su afectación***	***Páginas***
a) *Análisis de riesgos*	*El análisis de riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica de esta área universitaria, y otorga herramientas a las personas para implementar un ataque informático a los activos críticos y no críticos.*	*Anexo 1. 38-44* *Anexo 2. 91-101* *Anexo 3. 154-163* *Anexo 4. 201-210* *Anexo 5. 254-266* *Anexo 6. 317-329* *Anexo 7. 377-393* *Anexo 8. 437-457* *Anexo 9. 514-529* *Anexo 10. 579-586*
b) *Análisis de brecha*	*El análisis de brecha integra información relativa a la seguridad de la infraestructura tecnológica; enlistan los controles de seguridad con los que cuenta esta área; y menciona las herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información.*	*Anexo 1. 45-48* *Anexo 2. 101-106* *Anexo 3. 163-165* *Anexo 4. 210-214* *Anexo 5. 266-270* *Anexo 6. 329-332* *Anexo 7. 393-398* *Anexo 8. 457-462* *Anexo 9. 529-533* *Anexo 10. 586-589*
c) *Plan de Trabajo*	*El plan de trabajo define los controles de seguridad a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes con base en el riesgo real detectado. El uso de esta información permite inferir nuestros riesgos, por cuánto tiempo seguirán así hasta el momento que se implementen nuevos controles.*	*Anexo 1. 49-50* *Anexo 2. 106-108* *Anexo 3. 165* *Anexo 4. 214-215* *Anexo 5. 270-272* *Anexo 6. 333-334* *Anexo 7. 398-399* *Anexo 8. 462-465* *Anexo 9. 534-536* *Anexo 10. 589-590*
d) *Políticas de Respaldos*	*Las políticas de respaldo contienen información del momento que se hacen los respaldos, 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.*	*Anexo 1. 65-66* *Anexo 2. 127-128* *Anexo 3. 182-183* *Anexo 4. 230-232* *Anexo 5. 287-289* *Anexo 6. 352-354* *Anexo 7. 412-413* *Anexo 8. 486-488* *Anexo 9. 557-560* *Anexo 10. 604-606*
e) *Medidas de Seguridad*	*Las medidas de seguridad técnicas contienen las acciones implementadas o por implementar para proteger los datos*	*Anexo 12. 618-705*

Técnicas	*personales que se encuentren en formato digital, así como de los sistemas informáticos que les dan tratamiento.*	

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, el plan de trabajo y medidas de seguridad técnicas 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, el plan de trabajo y medidas de seguridad técnicas 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, el plan de trabajo y medidas de seguridad técnicas 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, 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, las políticas de respaldo, el plan de trabajo y medidas de seguridad técnicas 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, las políticas de respaldo, el plan de trabajo y medidas de seguridad técnicas 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).

XI. Mediante oficio **DGCS/016/2022**, recibido fecha 22 de agosto del 2022, dirigido a la Presidencia del Comité de Transparencia, la **Dirección General de Comunicación Social** 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[5]; exige elaborar versión pública del documento de seguridad de esta área universitaria.

[5] *DOF: 26 de noviembre de 2021*

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:

Anexos o Políticas	***Contenido y su afectación***	***Páginas***
a) Análisis de riesgos	*El análisis de riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica de esta área universitaria, y otorga herramientas a las personas para implementar un ataque informático a los activos críticos y no críticos.*	
b) Análisis de brecha	*El análisis de brecha integra información relativa a la seguridad de la infraestructura tecnológica; enlistan los controles de seguridad con los que cuenta esta área; y menciona las herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información.*	
c) Plan de Trabajo	*El plan de trabajo define los controles de seguridad a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de*	

	brecha, priorizando las medidas de seguridad más relevantes con base en el riesgo real detectado. El uso de esta información permite inferir nuestros riesgos, por cuánto tiempo seguirán así hasta el momento que se implementen nuevos controles.	

Los fundamentos y motivos se exponen a continuación:

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

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

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

La prueba de daño precitada, 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.

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).

XII. Mediante oficio **ICML/DIR/241/2022**, recibido con fecha 23 de agosto del 2022, dirigido a la Presidencia del Comité de Transparencia, el **Instituto de Ciencias del Mar y Limnología** 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[6]; exige elaborar versión pública del documento de seguridad de esta área universitaria.

[6] *DOF: 26 de noviembre de 2021*

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:

Anexos o Políticas	***Contenido y su afectación***	***Páginas***
Anexo 1. Inventario de sistemas de tratamiento de datos personales	*Se testaron algunas partes del inventario de los sistemas de tratamiento de datos personales, las cuales contienen información sobre las rutas de acceso a soportes digitales de la información y cuentas, los cuales pueden ser utilizados para un ataque informático a los activos críticos y no críticos.*	*11, 13, 26 y 36*
Anexo 2. Estructura y descripción de los sistemas de tratamiento de datos personales	*Se testaron algunas partes de la estructura y descripción de los sistemas de tratamiento de datos personales, las cuales contienen información sobre las rutas y métodos de acceso a soportes digitales y físicos de la información y la descripción y características de los lugares de resguardo, los cuales pueden ser utilizados para un ataque a los activos críticos y no críticos. Adicionalmente, los diagramas de arquitectura contenidos en dicho anexo contienen flujo de*	*43-49*

	información entre los componentes, sus rutas de acceso a soportes digitales y describe las medidas de seguridad implementadas, información que poder ser utilizada para un ataque informático a los activos críticos y no críticos.	
Anexo 3. Análisis de riesgos	*El análisis de riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica de esta área universitaria, y otorga herramientas a las personas para implementar un ataque informático a los activos críticos y no críticos.*	*50-66*
Anexo 4. Análisis de brecha	*El análisis de brecha integra información relativa a la seguridad de la infraestructura tecnológica; enlistan los controles de seguridad con los que cuenta esta área; y menciona las herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información.*	*67-96*
Anexo 5. Plan de Trabajo	*El plan de trabajo define los controles de seguridad a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes con base en el riesgo real detectado. El uso de esta información permite inferir nuestros riesgos, por cuánto tiempo seguirán así hasta el momento que se implementen nuevos controles.*	*97-98*

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 inventario, estructura y descripción de los sistemas de tratamiento de datos personales, diagramas de arquitectura, análisis de riesgo, el análisis de brecha ... y el plan de trabajo de esta dependencia contienen información de cómo se protegen los datos personales de los titulares que nos confiaron su información personal y que es nuestra responsabilidad garantizar. Es un riesgo real el hecho de que toda persona que quiera ocasionar la pérdida, destrucción, robo, copia, uso, acceso o tratamiento no autorizado, daño, alteración o modificación no autorizada de datos personales, puede hacerlo si cuenta con la información exacta de las vulnerabilidades de un área universitaria, lo que esta serie de documentos les otorga directamente si se difundiera la información.*

- *Divulgar el inventario, estructura y descripción de los sistemas de tratamiento de datos personales, diagramas de arquitectura, análisis de riesgo, el análisis de brecha ... y el plan de trabajo de esta dependencia evidencian los nuevos controles que estamos pendientes de implementar, describen la forma en cómo almacenamos técnicamente los datos personales, cómo protegemos los sistemas automatizados de información, qué medidas de seguridad administrativas, físicas y técnicas 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 inventario, estructura y descripción de los sistemas de tratamiento de datos personales, diagramas de arquitectura, análisis de riesgo, el análisis de brecha … y el plan de trabajo de esta área revela y hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales que obran en nuestros archivos y dejaría imposibilitada a esta área para reaccionar ante posibles amenazas.*

La prueba de daño precitada, 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 inventario, estructura y descripción de los sistemas de tratamiento de datos personales, diagramas de arquitectura, 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 inventario, estructura y descripción de los sistemas de tratamiento de datos personales, diagramas de arquitectura, análisis de riesgo, el análisis de brecha y el 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).

XIII. Mediante oficio **CGEP/0493/2022**, recibido con fecha 23 de agosto del 2022, dirigido a la Presidencia del Comité de Transparencia, la **Coordinación General de Estudios de Posgrado** 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[7]; 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

[7] *DOF: 26 de noviembre de 2021*

COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/529/2022

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:

Anexos o Políticas	***Contenido y su afectación***	***Páginas***
a) Estructura y descripción de los sistemas de tratamiento de datos personales	*La estructura y descripción de los sistemas de tratamiento de datos personales, refiere especificidades de cada uno de los sistemas a cargo de esta área, como son: la URL para acceder, el tipo de sistema en el que fue desarrollado, así como el responsable de su desarrollo. El uso de esta información podría ocasionar ataques informáticos dirigidos particularmente a los sistemas que resguarden el catálogo de datos personales que resulten de mayor interés para la comisión de un ilícito.*	*16 a 18*
b) Análisis de riesgos	*El análisis de riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica de esta área universitaria, y otorga herramientas a las personas para implementar un ataque informático a los activos críticos y no críticos.*	*18 a 20*
c) Análisis de brecha	*El análisis de brecha integra información relativa a la seguridad de la infraestructura tecnológica; enlistan los controles de seguridad con los que cuenta esta área; y menciona las herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información.*	*20*
d) Plan de Trabajo	*El plan de trabajo define los controles de seguridad a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes con base en el riesgo real detectado. El uso de esta información permite inferir nuestros riesgos, por cuánto tiempo seguirán así hasta el momento que se implementen nuevos controles.*	*21*

e) Medidas de seguridad implementadas	*Con las medidas de seguridad se darían a conocer aspectos relacionados con los sistemas e infraestructura con los que cuenta esta área universitaria, así como el dictamen del análisis de vulnerabilidades de la información en los que se enuncian el inventario de sistemas, puertos de comunicación, versiones y características de las comunicaciones y equipos integrados a la red de datos, e incluso los mecanismos de seguridad y de control de la información.*	*21 a 25*
f) Mecanismos de monitoreo y revisión de medidas de seguridad	*Los mecanismos de monitoreo y revisión de medias de seguridad indican las herramientas que son utilizadas para el monitoreo de la protección de datos, así como la periodicidad en la que se realiza la revisión correspondiente, por lo que, existe un riesgo en que dicha información se utilizada para que a través de ingeniería inversa o procesos análogos se tenga acceso a los sistemas de tratamiento de datos personales.*	*25*

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 consistentes en la estructura y descripción de los sistemas de tratamiento de datos personales, el análisis de riesgo, el análisis de brecha, el plan de trabajo, las medidas de seguridad implementadas en esta dependencia y los mecanismos de monitoreo y revisión de dichas de seguridad, 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 los apartados consistentes en la estructura y descripción de los sistemas de tratamiento de datos personales, el análisis de riesgo, el análisis de brecha, el plan de trabajo, las medidas de seguridad implementadas en esta dependencia y los mecanismos de monitoreo y revisión de dichas de seguridad, 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 planemos establecer de manera gradual y de conformidad con las prioridades y presupuestos otorgado.

- *En este sentido la revelación de la información que obra en los apartados consistentes en la estructura y descripción de los sistemas de tratamiento de datos personales, el análisis de riesgo, el análisis de brecha, el plan de trabajo, las medidas de seguridad implementadas en esta dependencia y los mecanismos de monitoreo y revisión de dichas de seguridad, revelan y hacen 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, 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.

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 de cada uno de esos apartados que obran en el documento de seguridad de esta área universitaria (anexo), 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).

XIV. Mediante oficio **DGAJ/SP/DCS/6577/2022**, recibido con fecha 23 de agosto del 2022, dirigido a la Presidencia del Comité de Transparencia, la **Dirección General de Asuntos Jurídicos** 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[8]; 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.

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

[8] *DOF: 26 de noviembre de 2021*

de Seguridad de Datos Personales de esta área universitaria. El documento de seguridad contiene los siguientes apartados cuya autorización de reserva total se solicita a ese Comité:

Anexos o Políticas	***Contenido y su afectación***	***Páginas***
a) Análisis de riesgos	*El análisis de riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica de esta área universitaria, y otorga herramientas a las personas para implementar un ataque informático a los activos críticos y no críticos.*	*Numeral 3, páginas 77 a 89.*
b) Análisis de brecha	*El análisis de brecha integra información relativa a la seguridad de la infraestructura tecnológica; enlistan los controles de seguridad con los que cuenta esta área; y menciona las herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información.*	*Numeral 4, páginas 90 a 93.*
c) Plan de Trabajo y Medidas de seguridad que hagan evidente vulnerabilidades	*El plan de trabajo y las medidas de seguridad que hagan evidente vulnerabilidades, definen 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.*	*Numeral 5, páginas 94 a 99 y numeral 6, fracción I, páginas 100 y 101, fracción III, numerales 1, 2, 3, 4, 5 y 6 páginas 102 y 103, fracción IV, numeral 3, cuatro líneas de la página 104, fracción V, numeral 2, página 105,*

		fracciones VII, VIII y IX, página 106.

Los fundamentos y motivos se exponen a continuación:

I. *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 … así como el plan de trabajo y las medidas de seguridad de esta dependencia universitaria 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 riego 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.*

II. *Divulgar el análisis de riesgo, el análisis de brecha … así como el plan de trabajo y las medidas de seguridad de esta dependencia universitaria 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 planemos establecer de manera gradual y de conformidad con las prioridades y presupuestos otorgado.*

III. *En este sentido la revelación de la información que obra el análisis de riesgo, el análisis de brecha … así como el plan de trabajo y las medidas de seguridad 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 Dirección General para reaccionar ante posibles amenazas.*

La prueba de daño señalada, 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 el plan de trabajo y las medidas de seguridad 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 previstos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

En tal sentido, proteger la información de los documentos relativos al análisis de riesgo, al análisis de brecha, así como al plan de trabajo y a las medidas de seguridad de esta área universitaria, 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 de la comunidad universitaria sino de cualquier persona que ponga la confianza en esta Universidad para resguardar sus datos personales.

Por tales motivos, respetuosamente, se propone la reserva total de cada uno de esos documentos, que obran como anexos y políticas del documento de seguridad de esta área universitaria, por un periodo de ***cinco (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:

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

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 Asuntos Jurídicos**, dependiente de la Oficina de la Abogacía General, en este acto el Abogado General y Presidente del Comité de Transparencia, Alfredo Sánchez Castañeda, así como el Director General de Asuntos Jurídicos y Secretario Técnico de este Comité, Lic. Jorge Barrera Gutiérrez, formalmente se excusan 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 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 **Coordinación de Servicios Administrativos Morelos,** la **Coordinación de Vinculación y Transferencia Tecnológica,** la **Dirección General de Cómputo y Tecnologías de Información y Comunicación,** la **Dirección General de Repositorios Universitarios,** la **Dirección General de Comunicación Social**, el **Instituto de Ciencias del Mar y Limnología,** la **Coordinación General de Estudios de Posgrado y la Dirección General de Asuntos Jurídicos,** 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 **Coordinación de Servicios Administrativos Morelos,** la **Coordinación de Vinculación y Transferencia Tecnológica,** la **Dirección General de Cómputo y Tecnologías de Información y Comunicación,** la **Dirección General de Repositorios Universitarios,** la **Dirección General de Comunicación Social**, el **Instituto de Ciencias del Mar y Limnología,** la **Coordinación General de Estudios de Posgrado y la Dirección General de Asuntos Jurídicos,** clasificaron como información reservada, por un periodo de **cinco años**, la relativa: al **Inventario de sistemas de tratamiento de datos personales (rutas de acceso a soportes digitales de la información y cuentas; información técnica y operativa); a la Estructura y descripción de los sistemas de tratamiento de datos personales (el tipo de soporte, la descripción y las características del lugar donde se resguardan los soportes; las rutas y los métodos de acceso a soportes digitales y físicos de la información; la URL para acceder, el tipo de sistema en el que fue desarrollado, así como el responsable de su desarrollo); a los Diagramas de Arquitectura; al Análisis de Riesgos; al Análisis de Brecha; al Plan de Trabajo; a la Política de Autenticación y Control de Acceso; a la Política de seguridad física y ambiental; a las Medidas de seguridad implementadas; a los Mecanismos de monitoreo y revisión de medidas de seguridad; a las Políticas de Respaldos, así como las Medidas de Seguridad Técnicas y aquéllas que hagan evidentes vulnerabilidades**; lo anterior, conforme a lo expuesto, en cada caso, en los antecedentes VII, VIII, IX, X, XI, XII, XIII y XIV 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:

> *"**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 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 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, el análisis 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 tal orden de ideas, el segundo párrafo del artículo 5 de las Normas Complementarias sobre Medidas de Seguridad Técnicas, Administrativas y Físicas para la Protección de Datos Personales en Posesión de la Universidad, dispone que el documento de seguridad, deberá contener las medidas de seguridad 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.

Por ende, de difundirse la información contenida en los apartados relativos: **al Inventario de sistemas de tratamiento de datos personales (rutas de acceso a soportes digitales de la información y cuentas; información técnica y operativa); a la Estructura y descripción de los sistemas de tratamiento de datos personales (el tipo de soporte, la descripción y las características del lugar donde se resguardan los soportes; las rutas y los métodos de acceso a soportes digitales y físicos de la información; la URL para acceder, el tipo de sistema en el que fue desarrollado, así como el responsable de su desarrollo); a los Diagramas de Arquitectura; al Análisis de Riesgos; al Análisis de Brecha; al Plan de Trabajo; a la Política de Autenticación y Control de Acceso; a la Política de seguridad física y ambiental; a las Medidas de seguridad implementadas; a los Mecanismos de monitoreo y revisión de medidas de seguridad; a las Políticas de Respaldos; a las Medidas de Seguridad Técnicas y aquéllas que hagan evidentes vulnerabilidades;** 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 **Inventario de sistemas de tratamiento de datos personales (rutas de acceso a soportes digitales de la información y cuentas; información técnica y operativa); la Estructura y descripción de los sistemas de tratamiento de datos personales (el tipo de soporte, la descripción y las características del lugar donde se resguardan los soportes; las rutas y los métodos de acceso a soportes digitales y físicos de la información; la URL para acceder, el tipo de sistema en el que fue desarrollado, así como el responsable de su desarrollo); los Diagramas de Arquitectura; el Análisis de Riesgos; el Análisis de Brecha; el Plan de Trabajo; la Política de Autenticación y Control de Acceso; la Política de seguridad física y ambiental; las Medidas de seguridad implementadas; los Mecanismos de monitoreo y revisión de medidas de seguridad; las Políticas de Respaldos; las Medidas de Seguridad Técnicas;** 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 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 **Inventario de sistemas de tratamiento de datos personales (rutas de acceso a soportes digitales de la información y cuentas; información técnica y operativa); a la Estructura y descripción de los sistemas de tratamiento de datos personales (el tipo de soporte, la descripción y las características del lugar donde se resguardan los soportes; las rutas y los métodos de acceso a soportes digitales y físicos de la información; la URL para acceder, el tipo de sistema en el que fue desarrollado, así como el responsable de su desarrollo); a los Diagramas de Arquitectura; al Análisis de Riesgos; al Análisis de Brecha; al Plan de Trabajo; a la Política de Autenticación y Control de Acceso; a la Política de seguridad física y ambiental; a las Medidas de seguridad implementadas; a los Mecanismos de monitoreo y revisión de medidas de seguridad; a las Políticas de Respaldos; a las Medidas de Seguridad Técnicas y aquéllas que hagan evidentes vulnerabilidades**, 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 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.

De difundirse la información contenida en el **Inventario de sistemas de tratamiento de datos personales (rutas de acceso a soportes digitales de la información y cuentas; información técnica y operativa); la Estructura y descripción de los sistemas de tratamiento de datos personales (el tipo de soporte, la descripción y las características del lugar donde se resguardan los soportes; las rutas y los métodos de acceso a soportes digitales y físicos de la información; la URL para acceder, el tipo de sistema en el que fue desarrollado, así como el responsable de su desarrollo); los Diagramas de Arquitectura; el Análisis de Riesgos; el Análisis de Brecha; el Plan de Trabajo; la Política de Autenticación y Control de Acceso; la Política de seguridad física y ambiental; las Medidas de seguridad implementadas; los Mecanismos de monitoreo y revisión de medidas de seguridad; las Políticas de Respaldos; las Medidas de Seguridad Técnicas y aquéllas que hagan evidentes vulnerabilidades,** 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 **Inventario de sistemas de tratamiento de datos personales (rutas de acceso a soportes digitales de la información y cuentas; información técnica y operativa); la Estructura y descripción de los sistemas de tratamiento de datos personales (el tipo de soporte, la descripción y las características del lugar donde se resguardan los soportes; las rutas y los métodos de acceso a soportes digitales y físicos de la información; la URL para acceder, el tipo de sistema en el que fue desarrollado, así como el responsable de su desarrollo); los Diagramas de Arquitectura; el Análisis de Riesgos; el Análisis de Brecha; el Plan de Trabajo; la Política de Autenticación y Control de Acceso; la Política de seguridad física y ambiental; las Medidas de seguridad implementadas; los Mecanismos de monitoreo y revisión de medidas de seguridad; las Políticas de Respaldos; las Medidas de Seguridad Técnicas y aquéllas que hagan evidentes vulnerabilidades,** 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.

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 **Coordinación de Servicios Administrativos Morelos,** la **Coordinación de Vinculación y Transferencia Tecnológica,** la **Dirección General de Cómputo y Tecnologías de Información y Comunicación,** la **Dirección General de Repositorios Universitarios,** la **Dirección General de Comunicación Social**, el **Instituto de Ciencias del Mar y Limnología,** la **Coordinación General de Estudios de Posgrado y la Dirección General de Asuntos Jurídicos,** 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 **Inventario de sistemas de tratamiento de datos personales (rutas de acceso a soportes digitales de la información y cuentas; información técnica y operativa); a la Estructura y descripción de los sistemas de tratamiento de datos personales (el tipo de soporte, la descripción y las características del lugar donde se resguardan los soportes; las rutas y los métodos de acceso a soportes digitales y físicos de la información; la URL para acceder, el tipo de sistema en el que fue desarrollado, así como el responsable de su desarrollo); a los Diagramas de Arquitectura; al Análisis de Riesgos; al Análisis de Brecha; al Plan de Trabajo; a la Política de Autenticación y Control de Acceso; a la Política de seguridad física y ambiental; a las Medidas de seguridad implementadas; a los Mecanismos de monitoreo y revisión de medidas de seguridad; a las Políticas de Respaldos; a las Medidas de Seguridad Técnicas y aquéllas que hagan evidentes vulnerabilidades**, 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:

  - 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:

COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/529/2022

R E S U E L V E

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 **Coordinación de Servicios Administrativos Morelos,** la **Coordinación de Vinculación y Transferencia Tecnológica,** la **Dirección General de Cómputo y Tecnologías de Información y Comunicación,** la **Dirección General de Repositorios Universitarios,** la **Dirección General de Comunicación Social**, el **Instituto de Ciencias del Mar y Limnología,** la **Coordinación General de Estudios de Posgrado y la Dirección General de Asuntos Jurídicos,** en relación con: el **Inventario de sistemas de tratamiento de datos personales (rutas de acceso a soportes digitales de la información y cuentas; información técnica y operativa); la Estructura y descripción de los sistemas de tratamiento de datos personales (el tipo de soporte, la descripción y las características del lugar donde se resguardan los soportes; las rutas y los métodos de acceso a soportes digitales y físicos de la información; la URL para acceder, el tipo de sistema en el que fue desarrollado, así como el responsable de su desarrollo); los Diagramas de Arquitectura; el Análisis de Riesgos; el Análisis de Brecha; el Plan de Trabajo; la Política de Autenticación y Control de Acceso; la Política de seguridad física y ambiental; las Medidas de seguridad implementadas; los Mecanismos de monitoreo y revisión de medidas de seguridad; las Políticas de Respaldos; las Medidas de Seguridad Técnicas y aquéllas que hagan evidentes vulnerabilidades**, 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.**

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 **Coordinación de Servicios Administrativos Morelos,** a la **Coordinación de Vinculación y Transferencia Tecnológica,** a la **Dirección General de Cómputo y Tecnologías de Información y Comunicación,** a la **Dirección General de Repositorios Universitarios,** a la **Dirección General de Comunicación Social**, al **Instituto de Ciencias del Mar y Limnología,** a la **Coordinación General de Estudios de Posgrado,** a la **Dirección General de Asuntos**

Jurídicos, 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., 24 de agosto de 2022

Archivo	03-ctunam-529-2022-docto-seg-4.pdf		
Identificador único (hash)	7ea1352b88c3430d8fed8338941833551612904 0e57b16f3d4c8dadf738fabe9		
Fecha y hora de cierre	24/08/2022 19:14:12	**Fecha y hora de emisión**	24/08/2022 19:35:46
Número de páginas	42	**Firmantes**	5

Firmantes

Nombre	Lic. MARIA ELENA GARCIA MELENDEZ	**Fecha y hora de firma**	24/08/2022 16:08:25
Directora General para la Prevención y Mejora de la Gestión Institucional y Suplente del Contralor			
Hash Firma	af63b93b888bc04e10a2246f6609ccd5cf4c5136859d7432285e4b32d6301d670ca81bf6e5dd3f98e0f50ef4b5ca130f		

Nombre	Dra. Guadalupe Barrena Nájera	**Fecha y hora de firma**	24/08/2022 16:36:33
Titular de la Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género			
Hash Firma	934427d85bb1890d0ba0b7038eae904df96ad6004d5058b5cca1c8a2f887ec4bd06c8d86465ff3ff367c42f4c0684937		

Nombre	Ing. Ricardo Ramírez Ortiz	**Fecha y hora de firma**	24/08/2022 15:52:42
Director General de Servicios Generales y Movilidad			
Hash Firma	c192cd7805a02e4223fb9c95b3ff52b73d61fa338708aeccf4dda623b8f47e5b4b436deca270e424ba4eaf7dde9f6089		

Nombre	JOSE MELJEM MOCTEZUMA	**Fecha y hora de firma**	24/08/2022 17:57:01
Titular de la Unidad de Transparencia			
Hash Firma	e826eb06c8e40bfbed24f0f81ab50624c871e30f1085bd4b37991331c936ed4965a7b9b4ff85ae52896a51fc145d02ef		

Nombre	Dra. Jacqueline Peschard Mariscal	**Fecha y hora de firma**	24/08/2022 19:14:12
Especialista			
Hash Firma	155d4b30a5034a8da015b961a57db05b2ec0bf0832913877034d642ce5cd3ba748a5f504ad999eab93165beb93861fd3		

DGTIC UNAM

DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

DOCUMENTO DE SEGURIDAD

SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES (SGSDP)

Código:	DGTIC-SGSDP-04-01-DocumentoDeSeguridad			
Versión	1.0	**Fecha:**	16 de agosto de 2022	
Vigencia	**Inicio**	16 de agosto del 2022	**Fin**	15 de agosto del 2023
				Firmas
Creado / redactado por:	M. en C. Carlos R. Tlahuel Pérez (CRTP)			
Edición / corrección:	Mtra. Elizabeth Rangel Gutiérrez (ERG)			
Revisión / comentarios:	Dra. Marcela Peñaloza Báez (MPB)			
	M. en C. Lourdes Velázquez Pastrana (LVP)			
	Ing. Leopoldo Vega Correa (LVC)			
	M. en C. Cristina Muzquiz Fragoso (CMF)			
	Dra. Ana Yuri Ramírez Molina (ARM)			
	Mtro. Miguel Ángel Villanueva Vélez (MAVV)			
Aprobación:	Dr. Héctor Benítez Pérez (HBP) - *Presidente del Comité del SGSDP*			
Nivel de confidencialidad:	Alto			

Histórico de versiones

Fecha	Versión	Creado por	Descripción de cambios
25 mayo 2022	0.1	DSSI. Coordinación de Seguridad de la Información (CRTP)	Creación de documento
01 de junio 2022	0.2	Unidad Jurídica	Se incorporó la normatividad universitaria aplicable, en materia de datos personales, en concordancia con la normatividad federal.
15 de agosto de 2022	0.3	Coordinación de Seguridad de la Información. Unidad Jurídica.	Actualización de alcance del Documento de Seguridad.
16 de agosto del 2022	1.0	Dr. Héctor Benítez Pérez	Aprobación del documento

Contenido

Justificación

La protección de datos personales es un derecho humano, reconocido en los artículos 6 y 16 de la Constitución Política de los Estados Unidos Mexicanos, toda persona tiene derecho a la protección de sus datos personales, y se reconoce el derecho de acceso, rectificación y cancelación y oposición en los términos que las leyes establezcan.

La DGTIC debe procurar un tratamiento legítimo, transparente, controlado e informado de los datos personales en los Sistemas de Tratamiento de Datos Personales (STDP) establecidos en el alcance, a efecto de cumplir con el REGLAMENTO DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA D E MÉXICO publicado el 26 de agosto de 2016, ACUERDO POR EL QUE SE ESTABLECEN LOS LINEAMIENTOS PARA LA PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, publicado el 25 de febrero de 2019, así como de las NORMAS COMPLEMENTARIAS SOBRE MEDIDAS DE SEGURIDAD TÉCNICAS, ADMINISTRATIVAS Y FÍSICAS PARA LA PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LA UNIVERSIDAD publicadas el 10 de enero de 2020 y reducir riesgos asociados al tratamiento de datos personales como daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado.

LA DGTIC ha desarrollado un modelo para el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora continua de un SGSDP. Para ello se ha considerado los siguientes estándares y/o guías:

- BS 10012:2009 Data protection – Specification for a personal information management system.
- ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems – Requirements.
- ISO/IEC 27002:2013, Information technology – Security techniques – Code of practice for information security controls.
- ISO/IEC 29100:2011 Information technology – Security techniques – Privacy framework.
- NIST SP 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems.
- Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales, INAI.
- Recomendaciones para el manejo de Incidentes de Seguridad de Datos Personales.

La DGTIC debe identificar los riesgos, vulnerabilidades y amenazas presentes en los activos que forman parte del proceso de Manejo de Incidentes y establecer los criterios de evaluación de riesgos.

Asimismo, la DGTIC debe constatar que ejerce medidas que contribuyen a la protección de la información a su cargo y resguardar de forma segura sus activos (información, sistemas, software, hardware, personal) considerando las acciones internas e incluso legales si así fuese requerido.

Objetivo del documento de seguridad

El presente documento tiene el objetivo de documentar las medidas de seguridad administrativas, físicas y técnicas comprendidas en el Sistema de Gestión de la Seguridad de Datos Personales (SGSDP) de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC) con el propósito del tratamiento legítimo, transparente, controlado e informado de los datos personales, a efecto de cumplir con la normativa aplicable y reducir riesgos asociados al tratamiento de datos personales como daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizados.

Ciclo de SGSDP

Para el establecimiento de un SGSDP, la DGTIC establece que la implementación será realizada con base en el ciclo de Mejora continua de Deming que comprende cuatro fases que se mencionan a continuación:

- Planeación (Plan)
- Implementación (Do)
- Evaluación (Check)
- Actuar (Act)

La implementación del ciclo del SGSDP se realiza en el mismo orden hasta llegar a la finalización de este; una vez concluido, comienza nuevamente la planeación de la implementación del siguiente ciclo del SGSDP, y de acuerdo con la última fase del ciclo de Mejora Continua, se incorporan las oportunidades de mejora, observaciones, acciones correctivas y demás elementos de mejora detectados.

En términos generales, en la fase de Planeación (Plan) se va a diseñar el SGSDP, se van a establecer las políticas, el alcance, la comunicación y otros elementos como línea base del Sistema. En la fase de Implementación (Do) se realiza la implementación y operación de los controles y el análisis de riesgos. En la fase de Evaluación (Check) se revisa y evalúa el desempeño y eficacia del Sistema y finalmente en la fase de Actuar (Act) se realizan los análisis causa-raíz, los planes de acciones correctivas y los ajustes necesarios para que el Sistema incorpore mejoras.

Planeación SGSDP

Alcance

El cumplimiento de las medidas de seguridad contenidas en este Documento de Seguridad es de aplicación obligatoria para todos los integrantes de DGTIC y para los recursos y procesos definidos dentro del alcance del SGSDP. El alcance comprende los siguientes los sistemas de tratamiento de datos personales (STDP):

Dirección	Coordinación, Jefatura o Área	Sistema de Tratamiento de Datos Personales	Observaciones
DT	Coordinación del Centro de Atención a usuarios	STDP01.Atención a usuarios	Contiene 10 sistemas informáticos
DSSI	Área de Servicio Social y Becas	STDP02.SISBEC	
DDTIC	Coordinación de Seguridad de la Información	STDP03.Plan de Becarios de SI	
DCV	Departamento de Desarrollo de Competencias en TICs	STDP04.Becarios Ingeniería de software	
DSSI	Departamento de Firma Electrónica Avanzada	STDP05.RU-TIC	
DIDT	Red Universitaria de Aprendizaje (RUA)	STDP06.RUA	
DIDT	Coordinación de Tecnología para la Docencia	STDP07.Seminario Moodle UNAM México	
DSSI	Departamento de Acervos Digitales	STDP08.Revista TIES	
DSSI	Departamento de Firma Electrónica	STDP09. Firma Electrónica Avanzada	

Funciones y responsabilidades

A continuación, se describen los roles y responsabilidades en el SGSDP.

Comité de SGSDP

El comité debe determinar y proveer los recursos necesarios para establecer, implementar, operar y mantener el SGSDP. Para asegurar que la gestión de los datos personales sea parte de los valores de la organización de manera efectiva, el responsable debe:

- Comunicar a todos los involucrados en el tratamiento de los datos personales (internos y externos) la importancia de:
  - cumplir la política de gestión de datos personales;
  - conocer los objetivos del SGSDP, y
  - mejorar el SGSDP de manera continua;
- Definir los roles, responsabilidades, cadena de rendición de cuentas y estructura organizacional para el SGSDP, y
- Asegurar que todos los trabajadores tengan claro sus roles y funciones, así como su contribución para el logro de los objetivos del SGSDP de la organización y las consecuencias del incumplimiento.
- En su caso de que los trabajadores incumplan con las Normas complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la Universidad, podrá amonestar de manera pública o privada.

Presidente del Comité
Titular de la DGTIC

- Participar en la revisión y actualización del Documento de Seguridad y aprobar o rechazar los cambios propuestos al SGSDP, así como de los procesos que requieran de controles de seguridad que el Comité identifique.
- Emitir resoluciones de carácter conclusivo e inapelable en la toma de decisiones del comité de seguridad.

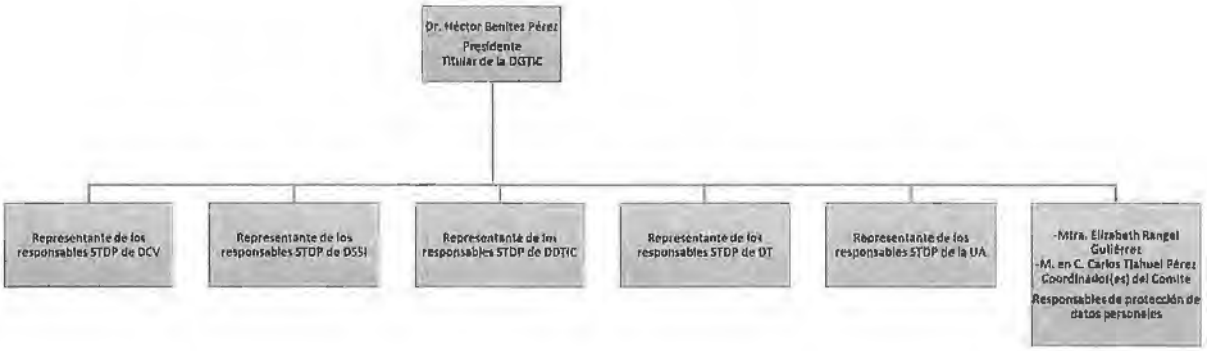
Coordinador(es) del Comité
Personal designado como Responsables de Protección de datos Personales de la DGTIC

- Convocar a las sesiones de Comité
- Conocer los procesos institucionales en los que recaen los STDP
- Proponer soluciones reales, viables y aplicables al SGSDP de la DGTIC
- Elaborar el plan del ciclo del SGSI y dar seguimiento para su cumplimiento
- Definir los protocolos de auditoría interna, así como actuar como facilitadores ante posibles auditorías externas

Representantes de los responsables STDP en el Comité
Directores o el responsable del STDP más significativo del área

- Discutir e implementar soluciones reales, viables y aplicables al SGSDP de la DGTIC.
- Comunicar inquietudes de los responsables, encargados y usuarios de los STDP de su área ante del comité
- Representar a las áreas:
    - Dirección de Colaboración y Vinculación
    - Dirección de Sistemas y Servicios Institucionales
    - Dirección de Docencia en TIC
    - Dirección de Telecomunicaciones

- Unidad Administrativa



DCV	Ing. Teresa Hernández Elenes (THE)
DSSI	Mtra. Lizbeth Angélica Barreto Zúñiga (LABZ)
DDTIC	Lic. Rosario Salinas Cuellar (RSC)
DT	M.I.A. Yazmín Diana Reyes Torres (YDRT),
UA	Lic. Juan Carlos Osnaya Gamboa (JCOG)

Responsables de los STDP

Coordinadores, Jefe de Departamento o Responsable de los procesos institucionales, definidos en el Manual de la Organización, en los que recaen los STDP (Dueño de riesgo)

- Participar activamente en la fase de inventario de STDP, análisis de riesgos, análisis de brecha y en el plan de tratamientos de riesgos.

Encargado de los STDP

Personal de la DGTIC con acceso a los contenedores de datos personales. Los contenedores pueden ser físicos o electrónicos, los contenedores deberán estar asociados a uno o más STDP y a su vez, un STDP deberá estar asociados a uno o más procesos institucionales. El acceso debe ser otorgado por el responsable del STDP.

Usuarios de los STDP

Persona autorizada por el responsable que dé tratamiento y/o tenga acceso a los datos y/o a los sistemas de datos personales

Objetivo de la organización

La DGTIC "Es la entidad universitaria encargada de supervisar los sistemas centrales de cómputo, de operar y extender las telecomunicaciones, del esfuerzo más amplio de capacitación en tecnologías de la información; y de la prospección, innovación y asimilación de estas tecnologías en beneficio de la Universidad y de la sociedad en general.

Misión de la organización

La Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC), contribuye al logro de los objetivos de la UNAM como punto de unión de la comunidad universitaria para aprovechar los beneficios que las tecnologías de la información y las telecomunicaciones pueden aportar a la docencia, la investigación, la difusión de la cultura y la administración universitaria.

Atribuciones de la organización

De conformidad con lo establecido en el Acuerdo que reorganiza las funciones y estructura de la Secretaría de Desarrollo Institucional de la Universidad Nacional Autónoma de México, publicado en Gaceta UNAM el 5 de noviembre de 2018, la DGTIC tiene las siguientes atribuciones:

1. Establecer y operar la infraestructura central de cómputo (supercómputo y centro de datos) y de telecomunicaciones (red alámbrica e inalámbrica de voz, datos y video), para las entidades académicas y dependencias universitarias, para su personal y para los alumnos, y vigilar su operación adecuada;

2. Normar y supervisar la gobernanza institucional de las Tecnologías de Información y Comunicación (TIC), en coordinación con los cuerpos colegiados aplicables, para lograr el uso adecuado y la interoperabilidad efectiva de los sistemas en toda la Universidad;

3. Consolidar y operar un sistema de información universitaria que permita lograr la inteligencia organizacional necesaria para la toma de decisiones;

4. Orientar y asesorar a las entidades y dependencias universitarias en la gestión de infraestructura y soluciones de cómputo y telecomunicaciones para cumplir los objetivos del Plan de Desarrollo de la UNAM, así como en la adquisición y mantenimiento de equipos de cómputo y en el aprovechamiento óptimo de los recursos institucionales;

5. Establecer e incrementar la vinculación de las unidades de las TIC con otras instituciones;

6. Contribuir de manera permanente al desarrollo de los planes y programas que la UNAM tiene establecidos para la actualización y superación académica de su comunidad de las TIC;

7. Integrar, evaluar y asesorar proyectos que impulsen el uso y aprovechamiento de las TIC en beneficio de la Universidad y del país, favoreciendo la proyección de la UNAM en los ámbitos nacional e internacional;

8. Impulsar la clasificación, visibilidad y uso con acceso abierto de los contenidos digitales en la docencia, la investigación y la difusión de la cultura;

9. Formar y actualizar a los miembros de la comunidad universitaria, en particular a los profesores y alumnos, así como a la sociedad en general, en el ámbito de las TIC;

10. Promover la integración de las TIC para mejorar la enseñanza y el aprendizaje en todas las modalidades y niveles educativos;

11. Propiciar el desarrollo institucional a través de la innovación e investigación aplicada en tecnologías y servicios de cómputo;

12. Participar en los comités y demás cuerpos colegiados en los que la normativa universitaria le designe como representante, y

13. Las que le confiera la persona titular de la Secretaría de Desarrollo Institucional y la Legislación Universitaria

Objetivos específicos para el establecimiento del SGSDP

La DGTIC cumplirá con los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales en cumplimiento de lo establecido en los *Lineamientos para la Protección de Datos Personales en Posesión de la Universidad Nacional Autónoma de México*, en los siguientes términos:

1. Tratará los datos personales en su posesión conforme las atribuciones que les confiere la Legislación Universitaria y los obtendrá a través de los medios previstos por las mismas disposiciones, con estricto apego y cumplimiento de lo dispuesto por la legislación nacional e internacional que resulte aplicable (principio de licitud)

2. Todo tratamiento de datos personales estará justificado por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable le confiere (principio de finalidad)
   Podrá tratar datos personales para finalidades distintas a aquéllas establecidas en el aviso de privacidad, siempre y cuando cuenten con atribuciones conferidas por la Ley y los Lineamientos antes referidos.

3. No obtendrá ni tratará datos personales, a través de medios engañosos o fraudulentos, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad. (principio de lealtad)

4. Contará con el consentimiento previo del titular para el tratamiento de los datos personales (principio de consentimiento):

   - Libre: Sin que medie error, mala intención, violencia o dolo que puedan afectar la manifestación de voluntad del titular;
   - Específica: Referida a finalidades concretas, lícitas, explícitas y legítimas que justifiquen el tratamiento, e
   - Informada: Que el titular tenga conocimiento del aviso de privacidad previo al tratamiento a que serán sometidos sus datos personales.

5. Adoptará las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere, la veracidad de éstos. (principio de calidad)

6. Tratará los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento. (principio de proporcionalidad)

7. Informará al titular, a través del aviso de privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto. (principio de información)

8. Garantizará el adecuado tratamiento de los datos personales que se encuentren bajo su custodia en términos de la normatividad universitaria y Federal, incluyendo las actividades que se encomienden para dicho tratamiento a una tercera persona denominada encargado. (principio de responsabilidad)

Alineación de los objetivos del SGSDP con respecto a los objetivos de la DGTIC

Objetivo de la organización	**Objetivo del área o del STDP**	**Sistema de Tratamiento de Datos Personales**
Orientar y asesorar a las entidades y dependencias universitarias en la gestión de infraestructura de telecomunicaciones para cumplir los objetivos del Plan de Desarrollo de la UNAM.	Actuar como único punto de contacto para la comunidad universitaria en la atención de fallas y recepción de solicitudes de los servicios que presta la DGTIC, y supervisar la calidad de los mismos.	STDP01.Atención a usuarios
Formar y actualizar a los miembros de la comunidad universitaria, en particular a los profesores y alumnos, así como a la sociedad en general, en el ámbito de las TIC		STDP02.SISBEC
Formar y actualizar a los miembros de la comunidad universitaria, en particular a los profesores y alumnos, así como a la sociedad en general, en el ámbito de las TIC;	Formar recursos humanos especializados en seguridad de la información en el marco del programa de becarios de la DGTIC.	STDP03.Plan de Becarios de SI
Formar y actualizar a los miembros de la comunidad universitaria, en particular a los profesores y alumnos, así como a la sociedad en general, en el ámbito de las TIC;	Desarrollar instrumentos especializados para fortalecer las competencias en procesos, gestión y gobernanza de Tecnologías de Información y Comunicación (TIC) del personal de la UNAM y del capital humano de la Dirección de Colaboración y Vinculación	STDP04.Becarios Ingeniería de software

Objetivo de la organización	Objetivo del área o del STDP	Sistema de Tratamiento de Datos Personales
Promover la integración de las TIC para mejorar la enseñanza y el aprendizaje en todas las modalidades y niveles educativos;	Apoyar la simplificación, certeza, seguridad, integridad y modernización de las actividades universitarias por medio de infraestructura y servicios de firma electrónica avanzada para la comunidad de la UNAM	STDP05.RU-TIC
Promover la integración de las TIC para mejorar la enseñanza y el aprendizaje en todas las modalidades y niveles educativos;	Apoyar los procesos de enseñanza y aprendizaje por medio de recursos educativos asociados a los planes de estudio y avalados por profesores.	STDP06.RUA
Formar y actualizar a los miembros de la comunidad universitaria, en particular a los profesores y alumnos, así como a la sociedad en general, en el ámbito de las TIC;	Apoyar la docencia universitaria mediante la generación de contenidos educativos en línea de libre acceso para la comunidad en general y contribuir en la generación de proyectos tecnológicos orientados a la educación para actores específicos de la sociedad.	STDP07.Seminario Moodle UNAM México
Propiciar el desarrollo institucional a través de la innovación e investigación aplicada en tecnologías y servicios de cómputo;	Analizar, desarrollar e implementar productos de software de alcance institucional que contribuyan al mejoramiento informático de las áreas universitarias.	STDP08.Revista TIES
Promover la integración de las TIC para mejorar la enseñanza y el aprendizaje en todas las modalidades y niveles educativos;	Apoyar la simplificación, certeza, seguridad, integridad y modernización de las actividades universitarias por medio de infraestructura y servicios de firma electrónica avanzada para la comunidad de la UNAM	STDP09.Firma Electrónica Avanzada

Inventario de Datos Personales

Anexo A

Análisis de Riesgos

Anexo B

Análisis de Brecha

Anexo C

Implementación y operación del SGSDP

Plan de Trabajo

Anexo D

Monitoreo y revisión SGSDP

Efectividad

OBJETIVO	MÉTRICA	FÓRMULA	FRECUENCIA	RESPONSABLE
Aprender, difundir, mejorar y socializar las actividades de la DGTIC revisando por cada ciclo del SGSDP el contenido, validez y estructura de al menos 50% de la cantidad de documentos y actualizando la información en caso de ser necesario.	El total de documentos registrados en la lista maestra	(Número de documentos revisados / Total de Documentos) * 100	Ciclo del SGSDP	Comité de SGSDP
Asegurar el cumplimiento de las medidas de seguridad físicas, técnicas y administrativas estableciendo como máximo aceptable 50 incidentes por ciclo del SGSDP, promoviendo e incentivando el reporte de incidentes.	El número de incidentes	Número de incidentes por incumplimiento	Ciclo del SGSDP	Coordinador del Comité

Sanciones

Los incidentes generados por el incumplimiento accidental o deliberado de las políticas serán evaluados por el Comité de SGSDP, y derivado de dicho análisis, podrá llevar a cabo las siguientes acciones:

I. El Comité de SGSDP podrá amonestar de manera pública o privada en los casos de incumplimientos de las Normas complementarias sobre medidas de seguridad técnicas,

administrativas y físicas para la protección de datos personales en posesión de la Universidad.

II. En caso de tratarse de tratarse de conductas o incidentes que incurran en responsabilidad administrativa por incumplimiento grave, o no grave de las obligaciones establecidas en el Reglamento de Responsabilidades Administrativas de las y los funcionarios y empleados de la Universidad Nacional Autónoma de México, y el Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, se dará parte al Comité de Transparencia de la UNAM, para que este último evalúe y determine si pone en conocimiento a la Contraloría de la Universidad sobre los hechos, para que ésta inicie el procedimiento administrativo sancionador.

III. En caso de que la conducta del Funcionario o Trabajador Universitario sea constitutiva de algún delito, la Contraloría y el Área Universitaria correspondiente iniciarán las acciones penales pertinentes, de acuerdo con lo provisto en el artículo 63 párrafo último del *Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México*.

Mejoramiento del SGSDP

- Dentro de la capacitación para la comunidad de la DGTIC, se estarán estableciendo:
- Charlas informáticas sobre temas de protección de datos personales
- Correos masivos con información sobre es SGSDP
- Generación de infografías con información de protección de datos personales

Esta capacitación debe de incluir los siguientes temas

- Los requerimientos y actualizaciones del SGSDP
- Las consecuencias del incumplimiento de los requerimientos legales
- La legislación vigente en materia de protección de datos personales y las mejores prácticas relacionadas
- Las herramientas tecnológicas relacionadas o utilizadas para el tratamiento de los datos personales y para la implementación de las medidas de seguridad

Anexos Adicionales

- Política de autenticación y control de acceso
- Política de seguridad física

ANEXO A.

INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Al 16 de agosto de 2022

Contenido

Dirección General de Tecnologías de Información y Comunicación	
Identificador único	**DGTIC-001-DT**
Nombre del sistema	**Red Inalámbrica Universitaria** **www.riu.unam.mx**
Datos personales contenidos en el sistema:	Nombre, apellido paterno, apellido materno, RFC y CURP
Responsable	
Nombre:	**Yazmín Diana Reyes Torres**
Cargo:	**Coordinadora del Centro de atención a usuarios**
Funciones:	Administrar el sistema; verificar que el sistema se encuentre completo, otorga y actualiza accesos; verifica que solo accede personal autorizado.
Obligaciones:	Proteger los datos personales de los solicitantes. Actualizar la información de datos personales. No difundir la información de datos personales contenidos en el registro a personas no autorizadas. Utilizar el sistema de acuerdo con los permisos que les fueron otorgados y no más allá.
Encargados	
Nombre del Encargado 1	**Jorge Manuel Salazar Frausto**
Cargo:	**Técnico Académico Asociado B TC**
Funciones:	Administrar el sistema; verificar que el sistema se encuentre completo, otorga y actualiza accesos; verifica que solo accede personal autorizado.
Obligaciones:	Proteger los datos personales de los solicitantes. Actualizar la información de datos personales. No difundir la información de datos personales contenidos en el registro a personas no autorizadas. Utilizar el sistema de acuerdo con los permisos que les fueron otorgados y no más allá.
Usuarios	
Nombre del Usuario 1	**Rosa María González Hernández**
Cargo:	**Técnico de base**
Funciones:	Gestión y administración del sistema. Consulta de información para su atención. Altas, bajas y modificaciones de datos. Seguimiento a solicitudes.
Obligaciones:	Proteger los datos personales de los solicitantes. Actualizar la información de datos personales. No difundir la información de datos personales contenidos en el registro a personas no autorizadas. Utilizar el sistema de acuerdo con los permisos que les fueron otorgados y no más allá.
Nombre del Usuario 2	**Sergio Ibarra Frías**
Cargo:	**Técnico de base**
Funciones:	Gestión y administración del sistema.

	Consulta de información para su atención. Altas, bajas y modificaciones de datos. Seguimiento a solicitudes.
Obligaciones:	Proteger los datos personales de los solicitantes. Actualizar la información de datos personales. No difundir la información de datos personales contenidos en el registro a personas no autorizadas. Utilizar el sistema de acuerdo con los permisos que les fueron otorgados y no más allá.
Nombre del Usuario 3	**Rita Barrera Pérez**
Cargo:	**Técnico de base**
Funciones:	Gestión y administración del sistema. Consulta de información para su atención. Altas, bajas y modificaciones de datos. Seguimiento a solicitudes.
Obligaciones:	Proteger los datos personales de los solicitantes. Actualizar la información de datos personales. No difundir la información de datos personales contenidos en el registro a personas no autorizadas. Utilizar el sistema de acuerdo con los permisos que les fueron otorgados y no más allá.
Nombre del Usuario 4	**Olga Leticia Arroyo Domínguez**
Cargo:	**Técnico de base**
Funciones:	Gestión y administración del sistema. Consulta de información para su atención. Altas, bajas y modificaciones de datos. Seguimiento a solicitudes.
Obligaciones:	Proteger los datos personales de los solicitantes. Actualizar la información de datos personales. No difundir la información de datos personales contenidos en el registro a personas no autorizadas. Utilizar el sistema de acuerdo con los permisos que les fueron otorgados y no más allá.
Nombre del Usuario 5	**Mireya Silva Salcedo**
Cargo:	**Técnico de base**
Funciones:	Gestión y administración del sistema. Consulta de información para su atención. Altas, bajas y modificaciones de datos. Seguimiento a solicitudes.
Obligaciones:	Proteger los datos personales de los solicitantes. Actualizar la información de datos personales. No difundir la información de datos personales contenidos en el registro a personas no autorizadas. Utilizar el sistema de acuerdo con los permisos que les fueron otorgados y no más allá.
Nombre del Usuario 6	**Patricia Guadalupe Jiménez Téllez**
Cargo:	**Jefa del Departamento de Calidad y Mejora en Servicios de TIC**
Funciones:	Gestión y administración del sistema. Consulta de información para su atención.

	Altas, bajas y modificaciones de datos. Seguimiento a solicitudes.
Obligaciones:	Proteger los datos personales de los solicitantes. Actualizar la información de datos personales. No difundir la información de datos personales contenidos en el registro a personas no autorizadas. Utilizar el sistema de acuerdo con los permisos que les fueron otorgados y no más allá.
Nombre del Usuario 7	**Sarai García Rodriguez**
Cargo:	**Asistente Ejecutiva**
Funciones:	Gestión y administración del sistema. Consulta de información para su atención. Altas, bajas y modificaciones de datos. Seguimiento a solicitudes.
Obligaciones:	Proteger los datos personales de los solicitantes. Actualizar la información de datos personales. No difundir la información de datos personales contenidos en el registro a personas no autorizadas. Utilizar el sistema de acuerdo con los permisos que les fueron otorgados y no más allá.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Dirección General de Tecnologías de Información y Comunicación	
Identificador único	**DGTIC-001-DT**
Nombre del sistema	**Red Inalámbrica Universitaria** **www.riu.unam.mx**
Tipo de soporte:	Electrónico
Descripción:	Eliminado: Información operativa y técnica Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México. Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.
Características del lugar donde se resguardan los soportes:	

Dirección General de Tecnologías de Información y Comunicación	
Identificador único	**DGTIC-002-DT**
Nombre del sistema	**Sistema de Gestión de Servicios de TIC (GTIC)** **www.gtic.unam.mx**
Datos personales contenidos en el sistema:	Nombre, apellido paterno, apellido materno, Firma digitalizada, Correo personal e Identificación
Responsable	
Nombre:	**Yazmín Diana Reyes Torres**
Cargo:	**Coordinadora del Centro de atención a usuarios**
Funciones:	Administrar el sistema; verificar que el sistema se encuentre completo y sin alteraciones; generar respaldos; monitorea, actualiza y realiza mantenimiento del sistema; otorga y actualiza accesos; verifica que solo accede personal autorizado.
Obligaciones:	Proteger los datos personales de los solicitantes. Actualizar la información de datos personales. No difundir la información de datos personales contenidos en el registro a personas no autorizadas. Utilizar el sistema de acuerdo con los permisos que les fueron otorgados y no más allá.
Encargados	
Nombre del Encargado 1	**Jorge Manuel Salazar Frausto**
Cargo:	**Técnico Académico Asociado B TC**
Funciones:	Administrar el sistema; verificar que el sistema se encuentre completo y sin alteraciones; generar respaldos; monitorea, actualiza y realiza mantenimiento del sistema; otorga y actualiza accesos; verifica que solo accede personal autorizado.
Obligaciones:	Proteger los datos personales de los solicitantes. Actualizar la información de datos personales. No difundir la información de datos personales contenidos en el registro a personas no autorizadas. Utilizar el sistema de acuerdo con los permisos que les fueron otorgados y no más allá.
Usuarios	
Nombre del Usuario 1	Staff con perfil **Super-Admin** (Ver tipo de privilegios por persona)
Cargo:	(Ver tipo de privilegios por persona)
Funciones:	Gestión y administración del sistema. Consulta de información para su atención. Altas, bajas y modificaciones de datos. Seguimiento a solicitudes.
Obligaciones:	Proteger los datos personales de los solicitantes. Actualizar la información de datos personales. No difundir la información de datos personales contenidos en el registro a personas no autorizadas. Utilizar el sistema de acuerdo con los permisos que les fueron otorgados y no más allá.

Nombre del Usuario 2	Staff con perfil **Admin** (Ver tipo de privilegios por persona)
Cargo:	(Ver tipo de privilegios por persona)
Funciones:	Consulta de información para su atención. Altas y modificaciones de datos. Seguimiento a solicitudes.
Obligaciones:	Proteger los datos personales de los solicitantes. Actualizar la información de datos personales. No difundir la información de datos personales contenidos en el registro a personas no autorizadas. Utilizar el sistema de acuerdo con los permisos que les fueron otorgados y no más allá.
Nombre del Usuario 3	Staff con perfil **Observer** (Ver tipo de privilegios por persona)
Cargo:	(Ver tipo de privilegios por persona)
Funciones:	Consulta de información para su atención. Seguimiento a solicitudes.
Obligaciones:	Proteger los datos personales de los solicitantes. Actualizar la información de datos personales. No difundir la información de datos personales contenidos en el registro a personas no autorizadas. Utilizar el sistema de acuerdo con los permisos que les fueron otorgados y no más allá.

Tipo de privilegios por persona

Super-Admin	1	Yazmin Diana Reyes Torres	Coordinador
	2	Jorge Manuel Salazar Frausto	Técnico Académico Asociado "B" TC

Admin	1	Rosa Maria González Hernández	Técnico de base
	2	Sergio Ibarra Frías	Técnico de base
	3	Rita Barrera Pérez	Técnico de base
	4	Olga Leticia Arroyo Domínguez	Técnico de base
	5	Mireya Silva Salcedo	Técnico de base
	6	Patricia Guadalupe Jiménez Téllez	Jefa del Departamento de Calidad y Mejora en Servicio de TIC
	7	Sarai García Rodriguez	Asistente Ejecutiva

Observer	1	Yazmín Diana Reyes Torres	Coordinador

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Dirección General de Tecnologías de Información y Comunicación	
Identificador único	**DGTIC-002-DT**
Nombre del sistema	**Sistema de Gestión de Servicios de TIC (GTIC) www.gtic.unam.mx**
Tipo de soporte	Electrónico
Descripción:	
Características del lugar donde se resguardan los soportes:	Eliminado: Información operativa y técnica Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México. Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Dirección General de Tecnologías de Información y Comunicación	
Identificador único	**DGTIC-003-DT**
Nombre del sistema	**Sistema de actualización de cuentas de correo 2017-2019** **www.actualizacioncorrero.unam.mx**
Datos personales contenidos en el sistema	Nombre, apellido paterno, apellido materno, RFC, CURP, correo electrónico e Identificación.
Responsable	
Nombre:	**Yazmín Diana Reyes Torres**
Cargo:	**Coordinadora del Centro de atención a usuarios**
Funciones:	Administrar el sistema; verificar que el sistema se encuentre completo y sin alteraciones; generar respaldos; monitorea, actualiza y realiza mantenimiento del sistema; otorga y actualiza accesos; verifica que solo accede personal autorizado.
Obligaciones:	Proteger los datos personales de los solicitantes. Actualizar la información de datos personales. No difundir la información de datos personales contenidos en

	el registro a personas no autorizadas. Utilizar el sistema de acuerdo con los permisos que les fueron otorgados y no más allá.
Encargados	
Nombre del Encargado 1	**Jorge Manuel Salazar Frausto**
Cargo:	**Técnico Académico Asociado B TC**
Funciones:	Administrar el sistema; verificar que el sistema se encuentre completo y sin alteraciones; generar respaldos; monitorea, actualiza y realiza mantenimiento del sistema; otorga y actualiza accesos; verifica que solo accede personal autorizado.
Obligaciones:	Proteger los datos personales de los solicitantes. Actualizar la información de datos personales. No difundir la información de datos personales contenidos en el registro a personas no autorizadas. Utilizar el sistema de acuerdo con los permisos que les fueron otorgados y no más allá.
Usuarios	
Nombre del Usuario 1	Staff con perfil **Manager** (Tipo de privilegio por persona)
Cargo:	(Tipo de privilegio por persona)
Funciones:	Gestión y administración del sistema. Consulta de información para su atención. Altas, bajas y modificaciones de datos. Seguimiento a solicitudes.
Obligaciones:	Proteger los datos personales de los solicitantes. Actualizar la información de datos personales. No difundir la información de datos personales contenidos en el registro a personas no autorizadas. Utilizar el sistema de acuerdo con los permisos que les fueron otorgados y no más allá.
Nombre del Usuario 2	Staff con perfil **CAU** (Tipo de privilegio por persona)
Cargo:	(Tipo de privilegio por persona)
Funciones:	Consultar y actualizar información para su atención. Seguimiento a solicitud.
Obligaciones:	Proteger los datos personales de los solicitantes. Actualizar la información de datos personales. No difundir la información de datos personales contenidos en el registro a personas no autorizadas. Utilizar el sistema de acuerdo con los permisos que les fueron otorgados y no más allá.

Tipo de privilegio por persona

Manager	1	Yazmín Diana Reyes Torres	Coordinador
	2	Jorge Manuel Salazar Frausto	Técnico Académico Asociado "B" TC

CCAU	1	Rosa María González Hernández	Técnico de Base
	2	Sergio Ibarra Frías	Técnico de Base
	3	Rita Barrera Pérez	Técnico de Base
	4	Olga Leticia Arroyo Domínguez	Técnico de Base
	5	Mireya Silva Salcedo	Técnico de Base
	6	Patricia Guadalupe Jiménez Téllez	Jefa del Departamento Calidad y Mejora en Servi de TIC
	7	Sarai García Rodríguez	Asistente Ejecutiva

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Dirección General de Tecnologías de Información y Comunicación	
Identificador único	**DGTIC-003-DT**
Nombre del sistema	**www.actualizacioncorrero.unam.mx**
Tipo de soporte	Electrónico
Descripción	
Características del lugar donde se resguardan los soportes	Eliminado: Información operativa y técnica Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México. Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Dirección General de Tecnologías de Información y Comunicación	
Identificador único	**DGTIC-004-DT**
Nombre del sistema	**Sistema Gestión DGTIC** **www.gestiondgtic.unam.mx**
Datos personales contenidos en el sistema:	Nombre, apellido paterno, apellido materno, correo electrónico y firma digitalizada.
Responsable	
Nombre:	**Yazmín Diana Reyes Torres**
Cargo:	**Coordinadora del Centro de atención a usuarios**
Funciones:	Administrar el sistema; verificar que el sistema se encuentre completo y sin alteraciones; generar respaldos; monitorea, actualiza y realiza mantenimiento del sistema; otorga y actualiza accesos; verifica que solo accede personal autorizado.
Obligaciones:	Proteger los datos personales de los solicitantes. Actualizar la información de datos personales. No difundir la información de datos personales contenidos en el registro a personas no autorizadas. Utilizar el sistema de acuerdo con los permisos que les fueron otorgados y no más allá.
Encargados	
Nombre del Encargado 1	**Jorge Manuel Salazar Frausto**
Cargo:	**Técnico Académico Asociado B TC**
Funciones:	Administrar el sistema; verificar que el sistema se encuentre completo y sin alteraciones; generar respaldos; monitorea, actualiza y realiza mantenimiento del sistema; otorga y actualiza accesos; verifica que solo accede personal autorizado.
Obligaciones:	Proteger los datos personales de los solicitantes. Actualizar la información de datos personales. No difundir la información de datos personales contenidos en el registro a personas no autorizadas. Utilizar el sistema de acuerdo con los permisos que les fueron otorgados y no más allá.
Usuarios	
Nombre del Usuario 1	Staff con perfil **Manager** (Ver Tipo de privilegio por persona)
Cargo:	(Ver Tipo de privilegio por persona)
Funciones:	Gestión y administración del sistema. Consulta de información para su atención. Altas, bajas y modificaciones de datos. Seguimiento a solicitudes.
Obligaciones:	Proteger los datos personales de los solicitantes. Actualizar la información de datos personales. No difundir la información de datos personales contenidos en el registro a personas no autorizadas. Utilizar el sistema de acuerdo con los permisos que les fueron otorgados y no más allá.

Tipo de privilegio por persona

Manager	1	Yazmín Diana Reyes Torres	Coordinador
	2	Jorge Manuel Salazar Frausto	Técnico Académico Asociado "B" TC

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Dirección General de Tecnologías de Información y Comunicación	
Identificador único	**DGTIC-004-DT**
Nombre del sistema	**Sistema Gestión DGTIC** **www.gestiondgtic.unam.mx**
Tipo de soporte	Electrónico
Descripción	
Características del lugar donde se resguardan los soportes	Eliminado: Información operativa y técnica Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México. Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Dirección General de Tecnologías de Información y Comunicación	
Identificador único	**DSSI-005-DT**
Nombre del sistema	**Sistema de gestión de la Sala de Servicios de Misión Crítica** **www.gestionssmc.unam.mx**
Datos personales contenidos en el sistema:	Nombre, apellido paterno y apellido materno.
Responsable	
Nombre:	**Yazmín Diana Reyes Torres**
Cargo:	**Coordinadora del Centro de atención a usuarios**
Funciones:	Administrar el sistema; verificar que el sistema se encuentre completo y sin alteraciones; generar respaldos; monitorea, actualiza y realiza mantenimiento del sistema; otorga y actualiza accesos; verifica que solo accede personal autorizado.
Obligaciones:	Proteger los datos personales de los solicitantes. Actualizar la información de datos personales. No difundir la información de datos personales contenidos en el registro a personas no autorizadas. Utilizar el sistema de acuerdo con los permisos que les fueron otorgados y no más allá.
Encargados	
Nombre del Encargado 1	**Jorge Manuel Salazar Frausto**
Cargo:	**Técnico Académico Asociado B TC**
Funciones:	Administrar el sistema; verificar que el sistema se encuentre completo y sin alteraciones; generar respaldos; monitorea, actualiza y realiza mantenimiento del sistema; otorga y actualiza accesos; verifica que solo accede personal autorizado
Obligaciones:	Proteger los datos personales de los solicitantes. Actualizar la información de datos personales. No difundir la información de datos personales contenidos en el registro a personas no autorizadas. Utilizar el sistema de acuerdo con los permisos que les fueron otorgados y no más allá.
Usuarios	
Nombre del Usuario 1	Staff con perfil **Manager** (Ver Tipo de privilegio por persona)
Cargo:	(Ver Tipo de privilegio por persona)
Funciones:	Gestión y administración del sistema. Consulta de información para su atención. Altas, bajas y modificaciones de datos. Seguimiento a solicitudes.
Obligaciones:	Proteger los datos personales de los solicitantes. Actualizar la información de datos personales. No difundir la información de datos personales contenidos en el registro a personas no autorizadas.

	Utilizar el sistema de acuerdo con los permisos que les fueron otorgados y no más allá.

Tipo de privilegio por persona

Manager	1	Yazmín Diana Reyes Torres	Coordinador
	2	Jorge Manuel Salazar Frausto	Técnico Académico Asociado "B" TC

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Dirección General de Tecnologías de Información y Comunicación	
Identificador único	**DSSI-005-DT**
Nombre del sistema	**Sistema de gestión de la Sala de Servicios de Misión Crítica www.gestionssmc.unam.mx**
Tipo de soporte:	Electrónico
Descripción:	
Características del lugar donde se resguardan los soportes:	Eliminado: Información operativa y técnica Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México. Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Dirección General de Tecnologías de Información y Comunicación	
Identificador único	**DGTIC-006-DT**
Nombre del sistema	**Sistema Ayuda** **www.ayuda.telecom.unam.mx**
Datos personales contenidos en el sistema:	Nombre, apellido paterno, apellido materno, correo electrónico.
Responsable	
Nombre:	**Yazmín Diana Reyes Torres**
Cargo:	**Coordinadora del Centro de atención a usuarios**
Funciones:	Administrar el sistema; verificar que el sistema se encuentre completo y sin alteraciones; generar respaldos; monitorea, actualiza y realiza mantenimiento del sistema; otorga y actualiza accesos; verifica que solo accede personal autorizado.
Obligaciones:	Proteger los datos personales de los solicitantes. Actualizar la información de datos personales. No difundir la información de datos personales contenidos en el registro a personas no autorizadas. Utilizar el sistema de acuerdo con los permisos que les fueron otorgados y no más allá.
Encargados	
Nombre del Encargado 1:	**Jorge Manuel Salazar Frausto**
Cargo:	**Técnico Académico Asociado B TC**
Funciones:	Administrar el sistema; verificar que el sistema se encuentre completo y sin alteraciones; generar respaldos; monitorea, actualiza y realiza mantenimiento del sistema; otorga y actualiza accesos; verifica que solo accede personal autorizado
Obligaciones:	Proteger los datos personales de los solicitantes. Actualizar la información de datos personales. No difundir la información de datos personales contenidos en el registro a personas no autorizadas. Utilizar el sistema de acuerdo con los permisos que les fueron otorgados y no más allá.
Usuarios	
Nombre del Usuario 1	Staff con perfil **Manager** (Ver Tipo de privilegio por persona)
Cargo:	(Ver Tipo de privilegio por persona)
Funciones:	Gestión y administración del sistema. Consulta de información para su atención. Altas, bajas y modificaciones de datos. Seguimiento a solicitudes.
Obligaciones:	Proteger los datos personales de los solicitantes. Actualizar la información de datos personales. No difundir la información de datos personales contenidos en el registro a personas no autorizadas.

	Utilizar el sistema de acuerdo con los permisos que les fueron otorgados y no más allá.
Nombre del Usuario 2	Staff con perfil **CCAU** (Ver Tipo de privilegio por persona)
Cargo:	(Ver Tipo de privilegio por persona)
Funciones:	Consulta de información para validar identidad. Altas y modificaciones de datos. Seguimiento a solicitudes.
Obligaciones:	Proteger los datos personales de los solicitantes. Actualizar la información de datos personales. No difundir la información de datos personales contenidos en el registro a personas no autorizadas. Utilizar el sistema de acuerdo con los permisos que les fueron otorgados y no más allá.

Tipo de privilegios por persona

Manager	1	Yazmin Diana Reyes Torres	Coordinador
	2	Jorge Manuel Salazar Frausto	Técnico Académico Asociado "B" TC

CCAU	1	Rosa María González Hernández	Técnico de Base
	2	Sergio Ibarra Frías	Técnico de Base
	3	Rita Barrera Pérez	Técnico de Base
	4	Olga Leticia Arroyo Domínguez	Técnico de Base
	5	Mireya Silva Salcedo	Técnico de Base
	6	Patricia Guadalupe Jiménez Téllez	Jefa del Departamento Calidad y Mejora en Servi de TIC
	7	Saraí García Rodriguez	Asistente ejecutiva

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Dirección General de Tecnologías de Información y Comunicación	
Identificador único	**DGTIC-006-DT**
Nombre del sistema	**Sistema Ayuda** **www.ayuda.telecom.unam.mx**
Tipo de soporte:	Electrónico
Descripción:	
Características del lugar donde se resguardan los soportes:	Eliminado: Información operativa y técnica Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México. Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Dirección General de Tecnologías de Información y Comunicación	
Identificador único	**DGTIC-007-DT**
Nombre del sistema	**Sistema Chat** **www.chat.unam.mx**
Datos personales contenidos en el sistema:	Nombre, apellido paterno, apellido materno, RFC, y correo electrónico.
Responsable	
Nombre:	**Yazmín Diana Reyes Torres**
Cargo:	**Coordinadora del Centro de atención a usuarios**
Funciones:	Administrar el sistema; verificar que el sistema se encuentre completo y sin alteraciones; generar respaldos; monitorea, actualiza y realiza mantenimiento del sistema; otorga y actualiza accesos; verifica que solo accede personal autorizado.
Obligaciones:	Proteger los datos personales de los solicitantes. Actualizar la información de datos personales. No difundir la información de datos personales contenidos en

	el registro a personas no autorizadas. Utilizar el sistema de acuerdo con los permisos que les fueron otorgados y no más allá.
Encargados	
Nombre del Encargado 1	**Jorge Manuel Salazar Frausto**
Cargo:	**Técnico Académico Asociado B TC**
Funciones:	Administrar el sistema; verificar que el sistema se encuentre completo y sin alteraciones; generar respaldos; monitorea, actualiza y realiza mantenimiento del sistema; otorga y actualiza accesos; verifica que solo accede personal autorizado.
Obligaciones:	Proteger los datos personales de los solicitantes. Actualizar la información de datos personales. No difundir la información de datos personales contenidos en el registro a personas no autorizadas. Utilizar el sistema de acuerdo con los permisos que les fueron otorgados y no más allá.
Usuarios	
Nombre del Usuario 1	Staff con perfil **Admin** (Ver Tipo de privilegio por persona)
Cargo:	(Ver Tipo de privilegio por persona)
Funciones:	Gestión y administración del sistema. Consulta de información para su atención. Altas, bajas y modificaciones de datos. Seguimiento a solicitudes.
Obligaciones:	Proteger los datos personales de los solicitantes. Actualizar la información de datos personales. No difundir la información de datos personales contenidos en el registro a personas no autorizadas. Utilizar el sistema de acuerdo con los permisos que les fueron otorgados y no más allá.
Nombre del Usuario 2	Staff con perfil **agentes** (Ver Tipo de privilegio por persona)
Cargo:	(Ver Tipo de privilegio por persona)
Funciones:	Solicitar información para validar identidad. Seguimiento a solicitud.
Obligaciones:	Proteger los datos personales de los solicitantes. Actualizar la información de datos personales. No difundir la información de datos personales contenidos en el registro a personas no autorizadas. Utilizar el sistema de acuerdo con los permisos que les fueron otorgados y no más allá.

Tipo de privilegio por persona

Manager	1	Yazmin Diana Reyes Torres	Coordinador
	2	Jorge Manuel Salazar Frausto	Técnico Académico Asociado "B" TC

Agentes	1	Rosa María González Hernández	Técnico de Base
	2	Sergio Ibarra Frías	Técnico de Base

	3	Rita Barrera Pérez	Técnico de Base
	4	Olga Leticia Arroyo Domínguez	Técnico de Base
	5	Mireya Silva Salcedo	Técnico de Base
	6	Patricia Guadalupe Jiménez Téllez	Jefa del Departamento de Calidad y Mejora en Servicio de TIC
	7	Sarai García Rodríguez	Asistente ejecutiva

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Dirección General de Tecnologías de Información y Comunicación	
Identificador único	**DGTIC-007-DT**
Nombre del sistema	**Sistema Chat** **www.chat.unam.mx**
Tipo de soporte:	Ninguno
Descripción:	
Características del lugar donde se resguardan los soportes:	Eliminado: Información operativa y técnica Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México. Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Dirección General de Tecnologías de Información y Comunicación	
Identificador único	**DGTIC-008-DT**
Nombre del sistema	**Sistema Correo Electrónico Comunidad UNAM www.comunidad.unam.mx**
Datos personales contenidos en el sistema:	Nombre, apellido paterno, apellido materno, correo electrónico, RFC, CURP e identificación.
Responsable	
Nombre:	**Yazmín Diana Reyes Torres**
Cargo:	**Coordinadora del Centro de atención a usuarios**
Funciones:	Administrar el sistema; verificar que el sistema se encuentre completo y sin alteraciones; generar respaldos; monitorea, actualiza y realiza mantenimiento del sistema; otorga y actualiza accesos; verifica que solo accede personal autorizado.
Obligaciones:	Proteger los datos personales de los solicitantes. Actualizar la información de datos personales. Asegura la información que se recibe en la cuenta soporte@comunidad.unam.mx, referente a solicitudes de cambios. No difundir la información de datos personales contenidos en el registro a personas no autorizadas. Utilizar el sistema de acuerdo con los permisos que les fueron otorgados y no más allá.
Encargados	
Nombre del Encargado 1	**Jorge Manuel Salazar Frausto**
Cargo:	**Técnico Académico Asociado B TC**
Funciones:	Administrar el sistema; verificar que el sistema se encuentre completo y sin alteraciones; generar respaldos; monitorea, actualiza y realiza mantenimiento del sistema; otorga y actualiza accesos; verifica que solo accede personal autorizado.
Obligaciones:	Proteger los datos personales de los solicitantes. Actualizar la información de datos personales. Asegura la información que se recibe en la cuenta soporte@comunidad.unam.mx, referente a solicitudes de cambios. No difundir la información de datos personales contenidos en el registro a personas no autorizadas. Utilizar el sistema de acuerdo con los permisos que les fueron otorgados y no más allá.

Usuarios	
Nombre del Usuario 1	Staff con perfil **CCAU** (Ver Tipo de privilegio por persona)
Cargo:	(Ver Tipo de privilegio por persona)
Funciones:	Consulta de información para validar identidad. Altas, bajas y modificaciones de datos. Seguimiento a solicitudes.
Obligaciones:	Validar la identidad del solicitante antes de atender su solicitud. Proteger los datos personales de los solicitantes. Actualizar la información de datos personales. Asegura la información que se recibe en la cuenta soporte@comunidad.unam.mx, referente a solicitudes de cambios. No difundir la información de datos personales contenidos en el registro a personas no autorizadas. Utilizar el sistema de acuerdo con los permisos que les fueron otorgados y no más allá.
Nombre del Usuario 2	Staff con perfil **Manager** (Ver Tipo de privilegio por persona)
Cargo:	(Ver Tipo de privilegio por persona)
Funciones:	Gestión y administración del sistema. Consulta de información para su atención. Altas, bajas y modificaciones de datos. Seguimiento a solicitudes.
Obligaciones:	Proteger los datos personales de los solicitantes. Actualizar la información de datos personales. No difundir la información de datos personales contenidos en el registro a personas no autorizadas. Utilizar el sistema de acuerdo con los permisos que les fueron otorgados y no más allá.

Tipo de privilegio por persona

CCAU	1	Rosa María González Hernández	Técnico de Base
	2	Sergio Ibarra Frías	Técnico de Base
	3	Rita Barrera Pérez	Técnico de Base
	4	Olga Leticia Arroyo Domínguez	Técnico de Base
	5	Mireya Silva Salcedo	Técnico de Base
	6	Patricia Guadalupe Jiménez Téllez	Jefa del Departamento Calidad y Mejora en Servi de TIC
	7	Saraí García Rodríguez	Asistente ejecutiva

Manager	1	Yazmín Diana Reyes Torres	Coordinador
	2	Jorge Manuel Salazar Frausto	Técnico Académico Asociado "B" TC

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Dirección General de Tecnologías de Información y Comunicación	
Identificador único	**DGTIC-008-DT**
Nombre del sistema	**Sistema Correo Electrónico Comunidad UNAM www.comunidad.unam.mx**
Tipo de soporte:	Electrónico
Descripción:	
Características del lugar donde se resguardan los soportes:	Eliminado: Información operativa y técnica Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México. Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.
Tipo de soporte:	Físico
Descripción:	
Características del lugar donde se resguardan los soportes:	Eliminado: Información de identificación física Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México. Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Dirección General de Tecnologías de Información y Comunicación	
Identificador único	**DGTIC-009-DT**
Nombre del sistema	**Sistema eduGAIN** **www.edugain.unam.mx**
Datos personales contenidos en el sistema:	Nombre, apellido paterno, apellido materno, RFC y CURP
Responsable	
Nombre:	**Yazmín Diana Reyes Torres**
Cargo:	**Coordinadora del Centro de atención a usuarios**
Funciones:	Administrar el sistema; verificar que el sistema se encuentre completo, otorga y actualiza accesos; verifica que solo accede personal autorizado.
Obligaciones:	Proteger los datos personales de los solicitantes. Actualizar la información de datos personales. No difundir la información de datos personales contenidos en el registro a personas no autorizadas. Utilizar el sistema de acuerdo con los permisos que les fueron otorgados y no más allá.
Encargados	
Nombre del Encargado 1	**Jorge Manuel Salazar Frausto**
Cargo:	**Técnico Académico Asociado B TC**
Funciones:	Administrar el sistema; verificar que el sistema se encuentre completo, otorga y actualiza accesos; verifica que solo accede personal autorizado.
Obligaciones:	Proteger los datos personales de los solicitantes. Actualizar la información de datos personales. No difundir la información de datos personales contenidos en el registro a personas no autorizadas. Utilizar el sistema de acuerdo con los permisos que les fueron otorgados y no más allá.
Usuarios	
Nombre del Usuario 1	Conexión de forma automatizada con los datos del sistema www.riu.unam.mx
Cargo:	
Funciones:	Validar información.
Obligaciones:	

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Dirección General de Tecnologías de Información y Comunicación	
Identificador único	**DGTIC-009-DT**
Nombre del sistema	**Sistema Edugain** **www.edugain.unam.mx**
Tipo de soporte:	Electrónico
Descripción:	
Características del lugar donde se resguardan los soportes:	Eliminado: Información operativa y técnica Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México. Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Dirección General de Tecnologías de Información y Comunicación	
Identificador único	**DGTIC-010-DT**
Nombre del sistema	**Sistema Eduroam** **www.eduroam.unam.mx**
Datos personales contenidos en el sistema:	Nombre, apellido paterno, apellido materno, RFC y CURP
Responsable*	
Nombre:	**Yazmín Diana Reyes Torres**
Cargo:	**Coordinadora del Centro de atención a usuarios**
Funciones:	Administrar el sistema; verificar que el sistema se encuentre completo, otorga y actualiza accesos; verifica que solo accede personal autorizado.
Obligaciones:	Proteger los datos personales de los solicitantes. Actualizar la información de datos personales. No difundir la información de datos personales contenidos en el registro a personas no autorizadas. Utilizar el sistema de acuerdo con los permisos que les fueron otorgados y no más allá.
Encargados	
Nombre del Encargado 1	**Jorge Manuel Salazar Frausto**
Cargo:	**Técnico Académico Asociado B TC**
Funciones:	Administrar el sistema; verificar que el sistema se encuentre completo, otorga y actualiza accesos; verifica que solo accede personal autorizado.
Obligaciones:	Proteger los datos personales de los solicitantes. Actualizar la información de datos personales. No difundir la información de datos personales contenidos en el registro a personas no autorizadas. Utilizar el sistema de acuerdo con los permisos que les fueron otorgados y no más allá.
Usuarios de sistema	
Nombre del Usuario 1	Usuario de consulta
Cargo:	Usuarios de sistema para consulta
Funciones:	Consulta de forma automatizada la información de la base de datos de RIU.
Obligaciones:	Utilizar el sistema de acuerdo con los permisos que les fueron otorgados y no más allá.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Dirección General de Tecnologías de Información y Comunicación	
Identificador único	**DGTIC-010-DT**
Nombre del sistema	**Sistema Eduroam** **www.eduroam.unam.mx**
Tipo de soporte:	Electrónico
Descripción:	
Características del lugar donde se resguardan los soportes:	Eliminado: Información operativa y técnica Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México. Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Dirección General de Tecnologías de Información y Comunicación	
Identificador único	**DGTIC-011-DSSI**
Nombre del sistema:	**Sistema de tratamiento de datos personales del Plan de Becarios en Seguridad Informática**
Datos personales contenidos en el sistema:	Historial académico; comprobante de inscripción a materias o modalidad de titulación; apellido paterno; apellido materno; nombre(s); correo electrónico personal; carrera; escuela o facultad; institución universitaria; créditos de carrera; promedio en carrera; número de cuenta en carrera; semestre de inscripción de la carrera; resultado de examen de conocimientos; resultado de entrevista; resultado de pruebas psicométricas; correo de becario; situación de participación; observaciones; fotografía; calificación obtenida en cada unidad temática; calificación obtenida en curso; promedio general en el PBSI; calle; número exterior de la calle; número interior; colonia; código postal; alcaldía, entidad o municipio; clave de municipio; clave de localidad; teléfono fijo; teléfono celular; CURP; RFC; antecedentes en DGTIC; empleo actual; horario de empleo actual; otras remuneraciones; firma digitalizada; fecha de nacimiento [dd/mm/aaaa]; edad: [años, meses cumplidos]; estado civil; nacionalidad; nombre de la tesis; fecha de examen profesional; nombre completo de la escuela de bachillerato; número de años cursados en bachillerato; año de inicio del bachillerato; año de término del bachillerato; promedio de bachillerato; nombre completo de la escuela de secundaria; número de años cursados en secundaria; año de inicio del secundaria; año de término del secundaria; promedio de secundaria; porcentaje de dominio de lectura de idioma; porcentaje de dominio hablado de idioma; porcentaje de dominio de escritura de idioma; porcentaje de dominio de comprensión de idioma; distinciones; cursos o talleres de actualización profesional; cursos o talleres impartidos; puesto en que se tiene experiencia; empresa donde ejerció ese puesto; duración en ese empleo.
Responsable	
Nombre:	Beatriz Verónica Gutiérrez Galán
Cargo:	Técnico académico de tiempo completo
Funciones:	Responsable de datos personales de los participantes en el Plan de Becarios en Seguridad Informática, en todos los procesos en que se recabe y haga uso de su información.
Obligaciones:	Manejo ético de información de participantes en el Plan de Becarios en Seguridad Informática, durante todos los procesos que se realizan en dicha capacitación.

Encargados	
Nombre:	Veronica Gutierrez Galán
Cargo:	Técnica Académica
Funciones:	Responsable del Programa de Becas
Obligaciones:	Control documental del Plan de Becarios de Seguridad de la Información
Usuarios	
Nombre:	M. en C. Carlos Raúl Tlahuel Pérez
Cargo:	Coordinador de Seguridad de la Información
Funciones:	Conocer información de los estudiantes durante toda su participación en el Plan de Becarios en Seguridad Informática, desde el proceso de Convocatoria y registro hasta su egreso.
Obligaciones:	Manejo ético de la información de los participantes en el Plan de Becarios en Seguridad Informática

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Dirección General de Tecnologías de Información y Comunicación	
Identificador único:	**DGTIC-011-DSSI**
Nombre del sistema:	**Sistema de tratamiento de datos personales del Plan de Becarios en Seguridad**
Tipo de soporte:	Electrónico
Descripción:	
Características del lugar donde se resguardan los soportes:	Eliminado: Información operativa y técnica Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México. Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Dirección General de Tecnologías de Información y Comunicación	
Identificador único	**DGTIC-012-DDTIC**
Nombre del sistema	**Sistema de Becas – SISBEC** (Sistema desarrollado y compartido por la Dirección General de Planeación de la UNAM y que solicita al Área de Becas de la DGTIC la recopilación y captura de diferentes datos de los estudiantes que participan en el Programa de Becas de Formación en Tecnologías de Información, desarrollado en la Dirección General de Cómputo y de Tecnologías de Información.
Datos personales contenidos en el sistema:	Nombre, no. de cuenta, CURP, fecha de nacimiento, nacionalidad, entidad de nacimiento, sexo, no. de teléfono, no. de celular, correo electrónico, estado civil, domicilio (estado, municipio, localidad, tipo de vialidad, calle, número interior y exterior, asentamiento, colonia, código postal), nivel educativo, escuela, carrera, monto de beca. Clave de la dependencia, nombre del programa de becas, clave de beca.
Responsable	
Nombre:	
Cargo:	
Funciones:	
Obligaciones:	
Encargados	
Nombre del Encargado 1	
Cargo:	
Funciones:	
Obligaciones:	
Usuarios	
Nombre del Usuario 1	Rosario Salinas Cuéllar
Cargo:	Técnico Académico
Funciones:	Recopilación de información de los estudiantes que participan en el Programa de Becas de la DGTIC. Análisis de información Captura de datos Generación de informes Respuesta a requerimientos de datos reportes e información solicitada por autoridades universitarias y nivel federal.
Obligaciones:	Cargar la información solicitada de los becarios del Programa de Becas de la DGTIC (trimestralmente) No modificar la información de datos personales del sistema.

	No difundir, distribuir o comercializar la información de datos personales contenidos en el sistema a personas no autorizadas. Utilizar el sistema de gestión de acuerdo con los permisos que les fueron otorgados y no más allá.
Nombre del Usuario 2	Nancy Escorcia Martínez
Cargo:	Técnico Académico
Funciones:	Captura de datos Análisis de información Generación de informes Respuesta a requerimientos de datos reportes e información solicitada por autoridades universitarias y nivel federal.
Obligaciones:	Cargar la información solicitada de los becarios del Programa de Becas de la DGTIC (trimestralmente) No modificar la información de datos personales del sistema. No difundir, distribuir o comercializar la información de datos personales contenidos en el sistema a personas no autorizadas. Utilizar el sistema de gestión de acuerdo con los permisos que les fueron otorgados y no más allá.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Dirección General de Tecnologías de Información y Comunicación	
Identificador único	**DGTIC-012-DDTIC**
Nombre del sistema	**Sistema de Becas – SISBEC**
Tipo de soporte:	Soporte electrónico
Descripción:	
Características del lugar donde se resguardan los soportes:	Eliminado: Información de identificación física Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México. Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.
Tipo de soporte:	Soporte físico
Descripción:	
Características del lugar donde se resguardan los soportes:	Eliminado: Información de identificación física Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México. Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Dirección General de Tecnologías de Información y Comunicación	
Identificador único	**DGTIC-013-DCV**
Nombre del sistema	**Proceso de selección y seguimiento académico de aspirantes a becarios de la línea de Ingeniería de Software**
Datos personales contenidos en el sistema:	**Datos de identificación**: Nombre, apellidos, domicilio, teléfono particular, teléfono celular, correo electrónico institucional, firma autógrafa, firma digitalizada, RFC, CURP, lugar de nacimiento, fecha de nacimiento, edad, fotografía. **Datos académicos:** Carrera y Facultad de procedencia, avance en créditos, promedio, trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos **Datos personales sensibles:** Resultados de examen psicométrico.
Responsable	
Nombre:	**Ing. María Teresa Hernández Elenes**
Cargo:	**Jefe de departamento**
Funciones:	Administrar el sistema de tratamiento; verificar que el sistema se encuentre completo y sin alteraciones; generar respaldos, monitoreo, actualizar y realizar mantenimiento del sistema, otorga y actualiza accesos; verifica que solo accede personal autorizado.
Obligaciones:	Proteger los datos personales de los solicitantes. No modificar la información de datos personales. No difundir la información de datos personales contenidos en el registro a personas no autorizadas. Mantener la información de datos personales en el servidor local de la DGTIC, no generar copias de los documentos en sus equipos personales y generar copias en equipos de trabajo solo para su tratamiento o análisis de información para borrarlo periódicamente.
Encargados	
Nombre del Encargado 1	**Ing. María Teresa Hernández Elenes**
Cargo:	**Jefe de departamento**
Funciones:	Capturar la información relacionada. Consulta de información Análisis de información y generación de reportes e informes.
Obligaciones:	Proteger los datos personales de los solicitantes. No modificar la información de datos personales del sistema. No difundir, distribuir o comercializar la información de datos personales contenidos en el sistema a personas no autorizadas. Mantener la información de datos personales en el servidor local de la DGTIC y no generar copias de los documentos

	en sus equipos de trabajo. Utilizar el sistema de gestión de acuerdo con los permisos que les fueron otorgados y no más allá.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Dirección General de Tecnologías de Información y Comunicación	
Identificador único	**DGTIC-013-DCV**
Nombre del sistema	**Proceso de selección y seguimiento académico de aspirantes a becarios de la línea de Ingeniería de Software**
Tipo de soporte:	Electrónico
Descripción:	Eliminado: Información operativa y técnica Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México. Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.
Características del lugar donde se resguardan los soportes:	

Descripción:	Eliminado: Información operativa y técnica Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México. Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.
Características del lugar donde se resguardan los soportes:	

Dirección General de Tecnologías de Información y Comunicación	
Identificador único	**DGTIC-014-DSSI**
Nombre del sistema	**Dspace del Repositorio RU-TIC**
Datos personales contenidos en el sistema:	1) **Datos personales en general:** a) **Datos de identificación**: Nombre, apellido paterno, apellido materno, CURP, CVU, ORCID, RFC, correo electrónico, CURP, idioma o lengua, firma digitalizada. **b) Datos laborales:** puesto, institución de adscripción, domicilio de trabajo, correo electrónico institucional, teléfono institucional, país.
Responsable	
Nombre:	**LDG. Lizbeth Luna González**
Cargo:	**Responsable del repositorio de la DGTIC**
Funciones:	Administrar el sistema de tratamiento; verificar que el sistema se encuentre completo y sin alteraciones; otorga y actualiza accesos. Definir la integración de metadatos de calidad al sistema. Desarrollar e implementar procesos para la alimentación del repositorio. Proteger los datos personales contenidos en el sistema de accesos no autorizados. Desarrollo de normatividades para el sistema. Aplicación de normativas que rigen el sistema.
Obligaciones:	Apoyar en el buen funcionamiento del sistema. Coordinar la integración de objetos digitales y de su correcta catalogación y visibilización. Mantener la información de datos personales en el servidor local de la DGTIC. Verificar que los objetos sean visibles en el sistema y la descripción de objetos. Proteger los datos personales de los solicitantes. No modificar la información de datos personales. No difundir la información de datos personales a nadie que no tenga autorización correspondiente. Mantener la información de datos personales en el servidor local de la DGTIC y en equipos autorizados por al DGTIC. Utilizar el sistema de acuerdo con los permisos que le fueron otorgados y no más allá.
Encargados	
Nombre del Encargado 1	**MAO Miguel Ángel Mejía Argueta**
Cargo:	**Responsable del área de Acervos Digitales**
Funciones:	Administrar el servidor del sistema; verificar que el sistema se encuentre completo y sin alteraciones; generar respaldos; monitorea, actualiza y realiza mantenimiento del sistema; verifica que solo accede personal autorizado.
Obligaciones:	Mantener el servidor y la base de datos funcionando en un 95% del tiempo y que pueda acceder a la información. Proteger los datos personales de los solicitantes. No modificar la información de datos personales. No difundir la información de datos personales a nadie que no tenga autorización correspondiente. Mantener la información de datos personales en el servidor

	local de la DGTIC y en equipos autorizados por al DGTIC. Utilizar el sistema de acuerdo con los permisos que les fueron otorgados y no más allá.
Nombre del Encargado 2	**Liliana Minerva Mendoza Castillo**
Cargo:	**Asistente editorial**
Funciones:	Apoyar en la alimentación de recursos del sistema. Catalogación de objetos digitales
Obligaciones:	Verificar que los objetos sean visibles en el sistema y la descripción de objetos. Proteger los datos personales de los solicitantes. No modificar la información de datos personales. No difundir la información de datos personales a nadie que no tenga autorización correspondiente. Mantener la información de datos personales en equipos autorizados por la DGTIC. Utilizar el sistema de acuerdo con los permisos que le fueron otorgados y no más allá.
Nombre del Encargado 3	**Oscar Isaías Del Río Martínez**
Cargo:	**Editor de medios**
Funciones:	Edición de los objetos digitales, descripción de los objetos que se integran al sistema. Verificar que los objetos sean visibles en el sistema y la descripción de objetos. Proteger los datos personales de los solicitantes. No modificar la información de datos personales. No difundir la información de datos personales a nadie que no tenga autorización correspondiente. Mantener la información de datos personales en el servidor local de la DGTIC y en equipos autorizados por al DGTIC. Utilizar el sistema de acuerdo con los permisos que les fueron otorgados y no más allá.
Obligaciones:	Catalogar y verificar que los objetos sean correctamente descritos. Edición de textos, audio y video.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Dirección General de Tecnologías de Información y Comunicación	
Identificador único	**DGTIC-014-DSSI**
Nombre del sistema	**Dspace del Repositorio RU-TIC**
Tipo de soporte:	Soporte electrónico.
Descripción:	Eliminado: Información operativa y técnica Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México. Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.
Características del lugar donde se resguardan los soportes:	

Dirección General de Tecnologías de Información y Comunicación	
Identificador único	**DGTIC-015-DIDT**
Nombre del sistema	**Red Universitaria de Aprendizaje (RUA)**
Datos personales contenidos en el sistema:	Plataforma RUA: nombre completo, correo electrónico, teléfonos de oficina, celular (en algunos casos), número de trabajador, RFC (en algunos casos)
Responsable	
Nombre del responsable 1:	**Pascual Juárez**
Cargo:	**Técnico Académico de la DGTIC**
Funciones:	Administrar el sistema de tratamiento; verificar que el sistema se encuentre completo y sin alteraciones; generar respaldos; monitorea, actualiza y realiza mantenimiento del sistema.
Obligaciones:	Proteger los datos personales de los participantes. No modificar la información de datos personales. No difundir la información de datos personales contenidos en el registro a personas no autorizadas. Mantener la información de datos personales en la plataforma de la RUA. Utilizar el sistema de acuerdo con los permisos que les fueron otorgados y no más allá.
Nombre del responsable 2:	**Mtro. Cristian Ricardo Ortega Ramírez (técnico Académico Titular A de tiempo completo)**
Cargo:	**Técnico Académico Titular A de tiempo completo.**
Funciones:	Otorga y actualiza accesos. Verifica que solo accede personal autorizado.
Obligaciones:	Proteger los datos personales de los participantes. No modificar la información de datos personales. No difundir la información de datos personales contenidos en el registro a personas no autorizadas. Mantener la información de datos personales en la plataforma de la RUA. Utilizar el sistema de acuerdo con los permisos que les fueron otorgados y no más allá.
Encargados	
Nombre del Encargados 1, 2, 3	• Cristian Ricardo Ortega Ramírez (Técnico Académico Titular A de tiempo completo). • María Juana Linares Altamirano (Técnico Académico Titular A de tiempo completo definitivo). • Gabriela Alejandra López Gómez (honorarios).
Cargo:	Responsable de la DGTIC (atención a proyectos de publicación)
Funciones:	Capturar información relacionada.

	Da acompañamiento en el proceso de publicación en la RUA de los recursos educativos obtenidos como resultado de los proyectos especiales (Académicos y de la DGAPA: PAPIIT, PAPIME e INFOCAB).
Obligaciones:	Proteger los datos personales de los participantes. No modificar la información de datos personales. No difundir la información de datos personales contenidos en el registro a personas no autorizadas. Mantener la información de datos personales en la plataforma de la RUA. Utilizar el sistema de acuerdo con los permisos que les fueron otorgados y no más allá.
Usuarios	
Nombre del Usuario 1	**Mtra. Rebeca Valenzuela Argüelles**
Cargo:	**Coordinadora de Tecnología para la Docencia**
Funciones:	Consulta de información Análisis de información y generación de informes.
Obligaciones:	Proteger los datos personales de los solicitantes. No modificar la información de datos personales del sistema. No difundir, distribuir o comercializar la información de datos personales contenidos en el sistema a personas no autorizadas. Mantener la información de datos personales en el servidor local de la DGTIC y no generar copias de los documentos en sus equipos de trabajo. Utilizar el sistema de acuerdo con los permisos que les fueron otorgados y no más allá.
Nombre del Usuario 2	**Gabriela Bañuelos Sandoval**
Cargo:	**Jefa del Departamento de Gestión de Contenido y Diseño Instruccional**
Funciones:	Consulta de información. Análisis de información y generación de informes. Seguimiento a solicitudes. Revisión de información para el otorgamiento de constancias.
Obligaciones:	Proteger los datos personales de los solicitantes. No modificar la información de datos personales del sistema. No difundir, distribuir o comercializar la información de datos personales contenidos en el sistema a personas no autorizadas. Mantener la información de datos personales en el servidor local de la DGTIC y no generar copias de los documentos en sus equipos de trabajo. Utilizar el sistema de acuerdo con los permisos que les fueron otorgados y no más allá.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Dirección General de Tecnologías de Información y Comunicación	
Identificador único	**DGTIC-015-DIDT**
Nombre del sistema	**Red Universitaria de Aprendizaje (RUA)**
Tipo de soporte:	Soporte electrónico.
Descripción:	Eliminado: Información operativa y técnica Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México. Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.
Características del lugar donde se resguardan los soportes:	

SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Dirección General de Tecnologías de Información y Comunicación	
Identificador único	**DGTIC-016-DIDT**
Nombre del sistema	**Seminario Moodle UNAM México**
Datos personales contenidos en el sistema:	Plataforma Moodle: nombre completo (nombres, apellido paterno, apellido materno), correo electrónico, país, ciudad, entidad o institución de procedencia y grado de estudios. Listas de asistencia en papel: Nombre completo (nombres, apellido paterno, apellido materno), correo electrónico, procedencia y firma.
Responsable	
Nombre:	**Rebeca Valenzuela Argüelles**
Cargo:	**Coordinadora de Tecnología para la Docencia**
Funciones:	Revisión de información con fines estadísticos. Revisión de información para el otorgamiento de constancias de asistencia.
Obligaciones:	Proteger los datos personales de los participantes. No modificar la información de datos personales. Baja de participantes a solicitud de los mismos. No difundir la información de datos personales contenidos en el registro a personas no autorizadas. Mantener la información de datos personales en el servidor local de la DGTIC y hacer respaldos periódicos de los mismos, al ser un evento permanente. Utilizar el sistema de acuerdo con los permisos que les fueron otorgados y no más allá.
Encargados	
Nombre del Encargado 1	**Miguel Zúñiga González**
Cargo:	**Académico**
Funciones:	Administrador de la plataforma Moodle
Obligaciones:	Proteger los datos personales contenidos en el sistema de accesos no autorizados. Generar los respaldos de la información contenida en el Sistema, así como del sistema, siguiendo la política de respaldos de la DGTIC.
Usuarios	
Nombre del Usuario 1	**Rebeca Valenzuela Argüelles**
Cargo:	**Coordinadora de Tecnología para la Docencia**
Funciones:	Consulta de información. Captura de datos. Análisis de información y generación de informes.

Obligaciones:	Proteger los datos personales de los solicitantes. No modificar la información de datos personales del sistema. No difundir, distribuir o comercializar la información de datos personales contenidos en el sistema a personas no autorizadas. Mantener la información de datos personales en el servidor local de la DGTIC y no generar copias de los documentos en sus equipos de trabajo. Utilizar el sistema de gestión de acuerdo con los permisos que les fueron otorgados y no más allá.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Dirección General de Tecnologías de Información y Comunicación	
Identificador único	**DGTIC-016-DIDT**
Nombre del sistema	**Seminario Moodle UNAM México**
Tipo de soporte:	
Descripción:	
Características del lugar donde se resguardan los soportes:	Eliminado: Información operativa y técnica Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México. Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.
Tipo de soporte:	Soporte Físico
Descripción:	Nombre completo (nombres, apellido paterno, apellido materno), correo electrónico, entidad o institución de procedencia, área, firma de asistencia
Características del lugar donde se resguardan los soportes:	Eliminado: Información de identificación física Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México. Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Dirección General de Tecnologías de Información y Comunicación	
Identificador único	**DGTIC-017-DSSI**
Nombre del sistema	**Revista TIES**
Datos personales contenidos en el sistema:	2) **Datos personales en general:** b) **Datos de identificación**: Nombre, apellido paterno, apellido materno, CURP, CVU, ORCID, RFC, idioma o lengua, firma digitalizada. **b) Datos laborales:** puesto, institución de adscripción, domicilio de trabajo, correo electrónico institucional, teléfono institucional, país.
Responsable	
Nombre:	**LDG. Lizbeth Luna González**
Cargo:	**Directora Editorial de la Revistas**
Funciones:	Manejo, recepción y seguimiento del proceso editorial de la revista. Manejo del editorial del gestor de revistas. Administrar el sistema de tratamiento; verificar que el sistema se encuentre completo y sin alteraciones; otorga y actualiza accesos. Desarrollo de normatividades para la revista. Aplicación de normativas que rigen la revista.
Obligaciones:	Proponer políticas para el aseguramiento de los datos personales en los servidores y Bases de Datos. Diseño y gestión de los procesos. Edición de los objetos digitales, descripción de los objetos que se integran al sistema. Verificar que los objetos sean visibles en el sistema y la descripción de objetos. Proteger los datos personales de los solicitantes. No modificar la información de datos personales. No difundir la información de datos personales a nadie que no tenga autorización correspondiente. Mantener la información de datos personales en el servidor local de la DGTIC y en equipos autorizados por al DGTIC. Utilizar el sistema de acuerdo con los permisos que le fueron otorgados y no más allá.
Encargados	
Nombre del Encargado 1	**MAO Miguel Ángel Mejía Argueta**
Cargo:	**Responsable del área de Acervos Digitales**
Funciones:	Administrar el servidor del sistema; verificar que el sistema se encuentre completo y sin alteraciones; generar respaldos; monitorea, actualiza y realiza mantenimiento del sistema; verifica que solo accede personal autorizado.
Obligaciones:	Mantener el servidor y la base de datos funcionando en un 95% del tiempo y que pueda acceder a la información. Proteger los datos personales de los solicitantes. No modificar la información de datos personales. No difundir la información de datos personales a nadie que no tenga autorización correspondiente. Generar los respaldos de la información contenida en el Sistema, así como del sistema, siguiendo la política de respaldos de la DGTIC.

	Mantener actualizado el servidor donde se aloja el sistema de gestión. Mantener la información de datos personales en el servidor local de la DGTIC y en equipos autorizados por al DGTIC. Utilizar el sistema de acuerdo con los permisos que le fueron otorgados y no más allá.
Nombre del Encargado 2	**Liliana Minerva Mendoza Castillo**
Cargo:	**Asistente editorial**
Funciones:	Apoyo en el proceso editorial
Obligaciones:	Gestión de artículos en todo el proceso, envío de correos para notificaciones. Corrección de estilo. Edición de los objetos digitales, descripción de los objetos que se integran al sistema. Verificar que los objetos sean visibles en el sistema y la descripción de objetos. Proteger los datos personales de los solicitantes. No modificar la información de datos personales. No difundir la información de datos personales a nadie que no tenga autorización correspondiente. Mantener la información de datos personales en el servidor local de la DGTIC y en equipos autorizados por al DGTIC. Utilizar el sistema de acuerdo con los permisos que le fueron otorgados y no más allá.
Nombre del Encargado 3	**Oscar Isaías Del Río Martínez**
Cargo:	**Editor de medios**
Funciones:	Edición de los objetos digitales, descripción de los objetos que se integran al sistema. Edición de los objetos digitales, descripción de los objetos que se integran al sistema. Verificar que los objetos sean visibles en el sistema y la descripción de objetos. Proteger los datos personales de los solicitantes. No modificar la información de datos personales. No difundir la información de datos personales a nadie que no tenga autorización correspondiente. Mantener la información de datos personales en el servidor local de la DGTIC y en equipos autorizados por al DGTIC. Utilizar el sistema de acuerdo con los permisos que le fueron otorgados y no más allá.
Obligaciones:	Edición de textos, audio y video.
Usuarios	
Nombre del Usuario 1	
Cargo:	
Funciones:	
Obligaciones:	

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Dirección General de Tecnologías de Información y Comunicación	
Identificador único	**DGTIC-017-DSSI**
Nombre del sistema	**Revista TIES**
Tipo de soporte:	Soporte electrónico.
Descripción:	Eliminado: Información operativa y técnica Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México. Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.
Características del lugar donde se resguardan los servidores:	

SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Dirección General de Tecnologías de Información y Comunicación	
Identificador único	**DGTIC-018-DSSI**
Nombre del sistema	**Firma Electrónica Universitaria (FEU)**
Datos personales contenidos en el sistema:	CURP, primer apellido, segundo apellido, nombre, correo electrónico, entidad de adscripción/institución académica, Firma Electrónica Universitaria .
Responsable	
Nombre:	**Mtra. Lizbeth Angélica Barreto Zúñiga**
Cargo:	**Jefa del Departamento de Firma Electrónica**
Funciones:	Coordinar al personal a cargo y vigilar el cumplimiento de los procedimientos técnicos, políticas administrativas y reglas del Departamento de Firma Electrónica.
Obligaciones:	Definir las políticas de solicitud, manejo y uso de los datos personales de los servicios otorgados por el Departamento de Firma Electrónica, conforme a los Lineamientos para la protección de datos personales en posesión de la Universidad Nacional Autónoma de México, así como la Normas complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la universidad. Establecer, mantener y revisar las medidas de seguridad y controles de carácter administrativo, físico y técnico para la protección de los datos personales que los protejan contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, y garanticen su confidencialidad, integridad y disponibilidad, conforme a las Normas Complementarias vigentes. Cumplir con los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad, definidos en la norma. Supervisar el cabal cumplimiento de la protección de datos personales en los sistemas y procesos y servicios proporcionados por el Departamento de Firma Electrónica. Realizar las acciones pertinentes y notificar a los responsables en la entidad en caso de que se comprometan los datos personales, o se incumplan las políticas para daño, pérdida, alteración, destrucción, uso, acceso o tratamiento de los mismos.
Encargados	
Nombre del Encargado 1	**M. en C.C. Gabriel González García**

Cargo:	**Técnico académico titular "A" T.C.**
Funciones:	Desarrollar, implementar y mantener operativos sistemas y aplicaciones referentes a Firma Electrónica Universitaria. Gestionar y administrar las bases de datos y la información referente a los usuarios de los sistemas.
Obligaciones:	Cumplir con las políticas establecidas por el Depto. de FEA en lo que a protección de datos personales se refiera. Establecer, mantener y revisar las medidas de seguridad y controles de carácter técnico para la protección de los datos personales que los protejan contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, y garanticen su confidencialidad, integridad y disponibilidad, conforme a las Normas Complementarias vigentes. Proteger los datos personales de los usuarios de FEU. No modificar la información de datos personales. No difundir la información de datos personales contenidos en bases de datos a personas no autorizadas. Mantener la información de datos personales en servidores de la DGTIC y no generar copias de los archivos en sus equipos de trabajo, ni personales.
Usuarios	
Nombre del Usuario 1	**Federico Sánchez Morales**
Cargo:	**Jefe de área**
Funciones:	Dar seguimiento a las solicitudes de altas de usuarios, así como a la emisión de certificados digitales, asesorar a los usuarios finales sobre el uso de FEU.
Obligaciones:	Proteger los datos personales de los usuarios finales de FEU. No modificar la información de datos personales. No difundir la información de datos personales contenidos en bases de datos a personas no autorizadas. Mantener la información de datos personales en servidores de la DGTIC y no generar copias de los documentos en sus equipos de trabajo, ni personales.
Nombre del Usuario 2	**Remedios Domínguez Yáñez**
Cargo:	**Jefe de área**
Funciones:	Emisión de certificados digitales, conciliación de carta compromiso y asesoría a los usuarios finales sobre el uso de FEU.
Obligaciones:	Proteger los datos personales de los usuarios de FEU. No modificar la información de datos personales. No difundir la información de datos personales contenidos en bases de datos a personas no autorizadas. Mantener la información de datos personales en servidores de la DGTIC y no generar copias de los documentos en sus equipos de trabajo, ni personales.

Nombre del Usuario 3	**Bernabé Serrano Bernabé**
Cargo:	**Asistente de procesos**
Funciones:	Emisión de certificados digitales, conciliación de carta compromiso y asesoría a los usuarios finales sobre el uso de FEU.
Obligaciones:	Proteger los datos personales de los usuarios de FEU. No modificar la información de datos personales. No difundir la información de datos personales contenidos en bases de datos a personas no autorizadas. Mantener la información de datos personales en servidores de la DGTIC y no generar copias de los documentos en sus equipos de trabajo, ni personales.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Dirección General de Tecnologías de Información y Comunicación	
Identificador único	**DGTIC-018-DSSI**
Nombre del sistema	**Firma Electrónica Universitaria (FEU)**
Tipo de soporte:	Eliminado: Información operativa y técnica Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México. Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.
Descripción:	
Características del lugar donde se resguardan los soportes:	
Tipo de soporte:	
Descripción:	
Características del lugar donde se resguardan los soportes:	

ANEXO B.

ANÁLISIS DE RIESGOS

Al 16 de agosto de 2022

Contenido

[redacted]

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Anexo B. Análisis de riesgos

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

[redacted]

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

[redacted]

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los articulos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

[redacted]

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

[redacted]

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

[redacted]

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

[redacted]

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

[redacted]

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

[redacted]

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

[redacted]

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

[redacted]

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

[redacted]

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

[redacted]

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

[redacted]

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

[redacted]

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

[redacted]

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

[redacted]

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

[redacted]

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

[redacted]

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

[redacted]

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

[redacted]

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

[redacted]

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

[redacted]

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

[redacted]

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

[redacted]

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

[redacted]

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

[redacted]

Eliminado: Análisis de riesgos

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

ANEXO C.

ANÁLISIS DE BRECHA

Al 16 de agosto de 2022

Contenido

[redacted]

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Anexo C. Análisis de brecha

Eliminado: Análisis de brecha

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

[redacted]

Eliminado: Análisis de brecha

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

[redacted]

Eliminado: Análisis de brecha

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Eliminado: Análisis de brecha

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Eliminado: Análisis de brecha

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Eliminado: Análisis de brecha

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

[redacted]

Eliminado: Análisis de brecha

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

[redacted]

Eliminado: Análisis de brecha

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

[redacted]

Eliminado: Análisis de brecha

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Eliminado: Análisis de brecha

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Eliminado: Análisis de brecha

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Eliminado: Análisis de brecha

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

[redacted]

Eliminado: Análisis de brecha

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

[redacted]

Eliminado: Análisis de brecha

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

[redacted]

Eliminado: Análisis de brecha

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Eliminado: Análisis de brecha

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Eliminado: Análisis de brecha

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Eliminado: Análisis de brecha

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

PLAN DE TRABAJO SGSDP 2022

***Eliminado**: Plan de trabajo.*

***Fundamentación:** De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.*

***Motivación**: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.*

DGTIC UNAM

DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

POLÍTICA DE SEGURIDAD FÍSICA Y AMBIENTAL

SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES (SGSDP)

Código:	DGTIC-SGSDP-04-01-Politica_Autenticacion_y_ControlDeAcceso				
Versión	1.0	**Fecha:**	16 de agosto de 2022		
Vigencia	**Inicio**	16 de agosto de 2022	**Fin**	16 de agosto de 2022	
					Firmas
Creado / redactado por:	M. en C. Carlos R. Tlahuel Pérez (CRTP)				
Edición / corrección:	Mtra. Elizabeth Rangel Gutiérrez (ERG)				
Revisión / comentarios:	Dra. Marcela Peñaloza Báez (MPB)				
	M. en C. Lourdes Velázquez Pastrana (LVP)				
	Ing. Leopoldo Vega Correa (LVC)				
	M. en C. Cristina Muzquiz Fragoso (CMF)				
	Dra. Ana Yuri Ramírez Molina (ARM)				
	Mtro. Miguel Ángel Villanueva Vélez (MAVV)				
Aprobación:	Dr. Héctor Benítez Pérez (HBP) - *Presidente del Comité del SGSDP*				
Nivel de confidencialidad:	Alto				

Histórico de versiones

Fecha	Versión	Creado por	Descripción de cambios
25 marzo 2022	1.0	DSSI. Coordinación de Seguridad de la Información (CRTP)	Creación de documento

Contenido

[redacted]

Eliminado: Información operativa y técnica

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

[redacted]

Eliminado: Información operativa y técnica

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

DGTIC UNAM

DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

POLÍTICA DE AUTENTICACIÓN Y CONTROL DE ACCESO

SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES (SGSDP)

Código:	DGTIC-SGSDP-04-01-Politica_Autenticacion_y_ControlDeAcceso				
Versión	1.0	**Fecha:**	16 de agosto de 2022		
Vigencia	**Inicio**	16 de agosto de 2022	**Fin**	16 de agosto de 2022	
				Firmas	
Creado / redactado por:	M. en C. Carlos R. Tlahuel Pérez (CRTP)				
Edición / corrección:	Mtra. Elizabeth Rangel Gutiérrez (ERG)				
Revisión / comentarios:	Dra. Marcela Peñaloza Báez (MPB)				
	M. en C. Lourdes Velázquez Pastrana (LVP)				
	Ing. Leopoldo Vega Correa (LVC)				
	M. en C. Cristina Muzquiz Fragoso (CMF)				
	Dra. Ana Yuri Ramírez Molina (ARM)				
	Mtro. Miguel Ángel Villanueva Vélez (MAVV)				
Aprobación:	Dr. Héctor Benítez Pérez (HBP) - *Presidente del Comité del SGSDP*				
Nivel de confidencialidad:	Alto				

Histórico de versiones

Fecha	Versión	Creado por	Descripción de cambios
25 mayo 2022	1.0	DSSI. Coordinación de Seguridad de la Información (CRTP)	Creación de documento

Contenido

Eliminado: Información operativa y técnica

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.

Eliminado: Información operativa y técnica

Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 32 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de tratarse de información que obstruye la prevención o persecución de los delitos.