COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/525/2022

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 el **Instituto de Matemáticas,** el **Instituto de Fisiología Celular,** la **Dirección General de la Escuela Nacional Colegio de Ciencias** y **Humanidades,** la **Escuela Nacional Colegio de Ciencias y Humanidades Planteles Azcapotzalco, Vallejo, Naucalpan, Oriente y Sur**, la **Facultad de Filosofía y Letras,** la **Coordinación de Difusión Cultural**, la **Dirección General de Estudios de Legislación Universitaria,** el **Centro Universitario de Teatro,** la **Dirección General de Radio UNAM,** la **Secretaría de Desarrollo Institucional,** el **Instituto de Física**, el **Consejo Académico del Área de las Ciencias Biológicas, Químicas y de la Salud,** el **Comité de Análisis para las Intervenciones Urbanas, Arquitectónicas y de las Ingenierías,** el **Museo Universitario del Chopo,** la **Dirección General de Música,** la **Dirección de Danza,** el **Centro de Investigaciones en Geografía Ambiental, Campus Morelia,** el **Museo Universitario de Arte Contemporáneo,** la **Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género,** el **Instituto de Química,** la **Dirección de Literatura y Fomento a la Lectura,** la **Dirección General de Servicios Administrativos,** la **Dirección de Teatro UNAM,** el **Centro de Ciencias Genómicas,** la **Facultad de Artes y Diseño,** la **Dirección General de Televisión Universitaria,** el **Centro Cultural Universitario Tlatelolco,** la **Dirección General de Orientación y Atención Educativa,** el **Consejo Académico del Área de las Ciencias Sociales,** la **Escuela Nacional de Estudios Superiores, Unidad Mérida,** el **Instituto de Ecología,** la **Dirección General de Cooperación e Internacionalización,** el **Instituto de Investigaciones Biomédicas,** la **Casa del Lago "Mtro. Juan José Arreola",** la **Coordinación para la Igualdad de Género,** la **Dirección General de la Escuela Nacional Preparatoria** y la **Escuela Nacional Preparatoria, Planteles 3 "Justo Sierra"** y **4 "Vidal Castañeda y Nájera"** y la **Dirección General del Deporte Universitario,** 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. La Presidencia del Comité de Transparencia recibió diversos oficios, mediante los cuales las Áreas Universitarias sometieron a consideración de este Cuerpo Colegiado, la clasificación parcial de información reservada de sus Documentos de Seguridad, mismos que se enlistan a continuación:

COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/525/2022

Oficio	Área Universitaria	Fecha de presentación
IMAT/D048/2022	Instituto de Matemáticas	15/08/2022
IFCE/DIR/184/2022	Instituto de Fisiología Celular	
CCHDG/DIR/145/08/2022	Dirección General de la Escuela Nacional Colegio de Ciencias y Humanidades	
CCHA/DIR/415/VIII/2022	Plantel Azcapotzalco de la Escuela Nacional Colegio de Ciencias y Humanidades	
CCHN.91.20/580/2022	Plantel Naucalpan de la Escuela Nacional Colegio de Ciencias y Humanidades	
CCHO/DIR/445/2022	Plantel Oriente de la Escuela Nacional Colegio de Ciencias y Humanidades	
OF/CCHS/DIR/160/2022	Plantel Sur de la Escuela Nacional Colegio de Ciencias y Humanidades	
CCHV/OJ/135/2022	Plantel Vallejo de la Escuela Nacional Colegio de Ciencias y Humanidades	
FFLE/CP/034/2022	Facultad de Filosofía y Letras	
CODC/182/2022	Coordinación de Difusión Cultural	
DGEL/JT/3454/2022	Dirección General de Estudios de Legislación Universitaria	16/08/2022
CUTE/DIR/66/2022	Centro Universitario de Teatro	
DGRU/115/2022	Dirección General de Radio UNAM	
SDI/116/2022	Secretaría de Desarrollo Institucional	17/08/2022
IFIS/D/221/2022 IFIS/D/223/2022	Instituto de Física	
CJBS/112/22	Consejo Académico del Área de las Ciencias Biológicas, Químicas y de la Salud	
CAI/063/2022	Comité de Análisis para las Intervenciones Urbanas, Arquitectónicas y de las Ingenierías	
DIR/MUCH/0160/2022	Museo Universitario del Chopo	
DGMU/114/08/2022	Dirección General de Música	
DDAN/0356/2022	Dirección de Danza	
CIGA/D/133/2022	Centro de Investigaciones en Geografía Ambiental, Campus Morelia	
DiGAV/D/2315/2022	Museo Universitario de Arte Contemporáneo	
DDUIAVG/T/2427/2022	Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género	
IQUI 427/2022	Instituto de Química	
DLFL/208/2022	Dirección de Literatura y Fomento a la	

	Lectura	
DGSA/0381/2022	Dirección General de Servicios Administrativos	
DTEA/107/2022	Dirección de Teatro UNAM	
ENP3/DIRE/239/2022	Escuela Nacional Preparatoria, Plantel 3	
CCG/DIR/293/2022	Centro de Ciencias Genómicas	
FAD/DIR/445/2022	Facultad de Artes y Diseño	
DGTV/DG/197/2022	Dirección General de Televisión Universitaria	
CCUT/139/2022	Centro Cultural Universitario Tlatelolco	
ENPDG/314/2022	Dirección General de la Escuela Nacional Preparatoria	
DGOAE/416/2022	Dirección General de Orientación y Atención Educativa	
CJCS/124/2022	Consejo Académico del Área de las Ciencias Sociales	
ENES/MID/OFJ/199/2022	Escuela Nacional de Estudios Superiores, Unidad Mérida	
IECO/DIR/327/2022	Instituto de Ecología	
DGECI/DG/0869/2022	Dirección General de Cooperación e Internacionalización	
IIB/DIR/309/2022	Instituto de Investigaciones Biomédicas	
DCLA/Of.096/2022	Casa del Lago "Mtro Juan José Arreola"	
ENP4/DIR/108/2022	Escuela Nacional Preparatoria, Plantel 4	
CIG/C/320/2022	Coordinación para la Igualdad de Género	
DGDU/CJ/930/2022	Dirección General del Deporte Universitario	

En dichos oficios, las Áreas Universitarias informaron 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*

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

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

- *Divulgar el análisis de riesgo, el análisis de brecha … y el plan de trabajo … 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, 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 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).

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 **Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género**, así como por la **Dirección General de Estudios de Legislación Universitaria**, dependiente de la Oficina de la Abogacía General, en este acto, la Titular de la Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género e integrante de este Cuerpo Colegiado, Guadalupe Barrena Nájera, 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 el **Instituto de Matemáticas,** el **Instituto de Fisiología Celular,** la **Dirección General de la Escuela Nacional Colegio de Ciencias** y **Humanidades,** la **Escuela Nacional Colegio de Ciencias y Humanidades Planteles Azcapotzalco, Vallejo, Naucalpan, Oriente y Sur**, la **Facultad de Filosofía y Letras,** la **Coordinación de Difusión Cultural**, la **Dirección General de Estudios de Legislación Universitaria,** el **Centro Universitario de Teatro,** la **Dirección General de Radio UNAM,** la **Secretaría de Desarrollo Institucional,** el **Instituto de Física**, el **Consejo Académico del Área de las Ciencias Biológicas, Químicas y de la Salud,** el **Comité de Análisis para las Intervenciones Urbanas, Arquitectónicas y de las Ingenierías,** el **Museo Universitario del Chopo,** la **Dirección General de Música,** la **Dirección de Danza,** el **Centro de Investigaciones en Geografía Ambiental, Campus Morelia,** el **Museo Universitario de Arte Contemporáneo,** la **Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género,** el **Instituto de Química,** la **Dirección de Literatura y Fomento a la Lectura,** la **Dirección General de Servicios Administrativos,** la **Dirección de Teatro UNAM,** el **Centro de Ciencias Genómicas,** la **Facultad de Artes y Diseño,** la **Dirección General de Televisión Universitaria,** el **Centro Cultural Universitario Tlatelolco,** la **Dirección General de Orientación y Atención Educativa,** el **Consejo Académico del Área de las Ciencias Sociales,** la **Escuela Nacional de Estudios Superiores, Unidad Mérida,** el **Instituto de Ecología,** la **Dirección General de Cooperación e Internacionalización,** el **Instituto de Investigaciones Biomédicas,** la **Casa del Lago "Mtro. Juan José Arreola",** la **Coordinación para la Igualdad de Género,** la **Dirección General de la Escuela Nacional Preparatoria** y la **Escuela Nacional Preparatoria, Planteles 3 "Justo Sierra"** y **4 "Vidal Castañeda y Nájera"** y la **Dirección General del Deporte Universitario,** 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, el **Instituto de Matemáticas,** el **Instituto de Fisiología Celular,** la **Dirección General de la Escuela Nacional Colegio de Ciencias** y **Humanidades,** la **Escuela Nacional Colegio de Ciencias y Humanidades Planteles Azcapotzalco, Vallejo, Naucalpan, Oriente y Sur**, la **Facultad de Filosofía y Letras,** la **Coordinación de Difusión Cultural**, la **Dirección General de Estudios de Legislación Universitaria,** el **Centro Universitario de Teatro,** la **Dirección General de Radio UNAM,** la **Secretaría de Desarrollo Institucional,** el **Instituto de**

Física, el **Consejo Académico del Área de las Ciencias Biológicas, Químicas y de la Salud,** el **Comité de Análisis para las Intervenciones Urbanas, Arquitectónicas y de las Ingenierías,** el **Museo Universitario del Chopo,** la **Dirección General de Música,** la **Dirección de Danza,** el **Centro de Investigaciones en Geografía Ambiental, Campus Morelia,** el **Museo Universitario de Arte Contemporáneo,** la **Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género,** el **Instituto de Química,** la **Dirección de Literatura y Fomento a la Lectura,** la **Dirección General de Servicios Administrativos,** la **Dirección de Teatro UNAM,** el **Centro de Ciencias Genómicas,** la **Facultad de Artes y Diseño,** la **Dirección General de Televisión Universitaria,** el **Centro Cultural Universitario Tlatelolco,** la **Dirección General de Orientación y Atención Educativa,** el **Consejo Académico del Área de las Ciencias Sociales,** la **Escuela Nacional de Estudios Superiores, Unidad Mérida,** el **Instituto de Ecología,** la **Dirección General de Cooperación e Internacionalización,** el **Instituto de Investigaciones Biomédicas,** la **Casa del Lago "Mtro. Juan José Arreola",** la **Coordinación para la Igualdad de Género,** la **Dirección General de la Escuela Nacional Preparatoria** y la **Escuela Nacional Preparatoria, Planteles 3 "Justo Sierra"** y **4 "Vidal Castañeda y Nájera"** y la **Dirección General del Deporte Universitario,** clasificaron como información reservada, por un periodo de **cinco años**, la relativa al **Análisis de Riesgo**, al **Análisis de Brecha** y al **Plan de Trabajo**, conforme a lo expuesto en el antecedente VII 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, respectivamente.

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 podrá 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, de brecha, el plan de trabajo**, los mecanismos de monitoreo y revisión de las medidas de seguridad y el programa general de capacitación. Dicho documento deberá actualizarse cuando se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio de nivel de riesgo; como resultado de un proceso de mejora

continua, derivado del monitoreo y revisión del sistema de gestión; como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida; así como con la implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

En ese sentido, el segundo párrafo del artículo 5 de las Normas Complementarias sobre Medidas de Seguridad Técnicas, Administrativas y Físicas para la Protección de Datos Personales en Posesión de la Universidad, dispone que el documento de seguridad, deberá contener las medidas de seguridad administrativa, física y técnica aplicables a los sistemas de tratamiento de datos personales del Área Universitaria, con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información personal que éstos contienen.

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

En este sentido, de difundirse la información contenida en los apartados relativos al **Análisis de Riesgos, al Análisis de Brecha**, al **Plan de Trabajo**, así como a **toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados** o que **revele vulnerabilidades en la protección de los datos personales en poder de las Áreas Universitarias,** se haría del conocimiento público la falta o debilidad de seguridad en un activo o grupo de activos, físicos o electrónicos, que puede ser explotada por una o más amenazas, lo que conllevaría a la materialización de las mismas y ocasionar la pérdida, destrucción no autorizada o incluso la sustracción de los datos personales en posesión de la Universidad, así como el robo, extravío o copia no autorizada de los mismos, su uso, acceso o tratamiento no autorizado, además del daño, alteración o modificación no autorizada, incluso impidiendo su recuperación, vulnerando así la seguridad de los datos personales.

Bajo estos argumentos se advierte que la clasificación de la información contenida en el **Análisis de Riesgos,** en el **Análisis de Brecha**, en **Plan de Trabajo**, así como **toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados** o que **revele vulnerabilidades en la protección de los datos personales en poder de las Áreas Universitarias**, 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 **Análisis de Riesgos,** al **Análisis de Brecha**, al **Plan de Trabajo**¸ 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 el plan de trabajo, el análisis de riesgos y el análisis de brecha del documento de seguridad, se afectarían las medidas y acciones implementadas por las Áreas Universitarias para reducir el riesgo de que se cometa una conducta o un comportamiento que pueda dañar o convertir a esta Universidad y su comunidad en sujetos o víctimas de conductas ilícitas.

Lo anterior, toda vez que la publicidad de la información contenida en el **análisis de riesgos, de brecha** y el **plan de trabajo,** así como **toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados** o **revele vulnerabilidades en la protección de los datos personales en poder de las Áreas Universitarias**, representa un riesgo potencial para las Áreas Universitarias, pues a través

de dicha información se podrían identificar vulnerabilidades que pueden ser aprovechadas para realizar conductas contrarias a derecho, tales como actos vandálicos, o bien, ataques informáticos de diversa índole, disminuyendo la capacidad de las Áreas Universitarias para responder ante posibles amenazas.

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

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

El perjuicio que en su caso ocasionaría al interés público la divulgación de la información en cuestión, supera al perjuicio que se ocasionaría al no publicarla, pues con la difusión de la información contenida en el **análisis de riesgos, de brecha y el plan de trabajo,** así como **toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados** o **revele vulnerabilidades en la protección de los datos personales en poder de las Áreas Universitarias**, 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 el **Instituto de Matemáticas,** el **Instituto de Fisiología Celular,** la **Dirección General de la Escuela Nacional Colegio de Ciencias** y **Humanidades,** la **Escuela Nacional Colegio de Ciencias y Humanidades Planteles Azcapotzalco, Vallejo, Naucalpan, Oriente y Sur**, la **Facultad de Filosofía y Letras,** la **Coordinación de Difusión Cultural**, la **Dirección General de Estudios de Legislación Universitaria,** el **Centro Universitario de Teatro,** la **Dirección General de Radio UNAM,** la **Secretaría de Desarrollo Institucional,** el **Instituto de Física**, el **Consejo Académico del Área de las Ciencias Biológicas, Químicas y de la Salud,** el **Comité de Análisis para las Intervenciones Urbanas, Arquitectónicas y de las Ingenierías,** el **Museo Universitario del Chopo,** la **Dirección General de Música,** la **Dirección de Danza,** el **Centro de Investigaciones en Geografía Ambiental, Campus Morelia,** el **Museo Universitario de Arte Contemporáneo,** la **Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género,** el **Instituto de Química,** la **Dirección de Literatura y Fomento a la Lectura,** la **Dirección General de Servicios Administrativos,** la **Dirección de Teatro UNAM,** el **Centro de Ciencias Genómicas,** la **Facultad de Artes y Diseño,** la **Dirección General de Televisión Universitaria,** el **Centro Cultural Universitario Tlatelolco,** la **Dirección General de Orientación y Atención Educativa,** el **Consejo Académico del Área de las Ciencias Sociales,** la **Escuela Nacional de Estudios Superiores, Unidad Mérida,** el **Instituto de Ecología,** la **Dirección General de Cooperación e Internacionalización,** el **Instituto de Investigaciones Biomédicas,** la **Casa del Lago "Mtro. Juan José Arreola",** la **Coordinación para la Igualdad de Género,** la **Dirección General de la Escuela Nacional Preparatoria** y la **Escuela Nacional Preparatoria, Planteles 3 "Justo Sierra"** y **4 "Vidal Castañeda y Nájera"** y la **Dirección General del Deporte Universitario,** por un periodo de **cinco años**, que se computarán a partir de la fecha de la presente resolución, de conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

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

- Deberán testar las secciones o información correspondientes al "Análisis de Riesgo", al "Análisis de Brecha", al "Plan de Trabajo", 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 encuentran 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:

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 la información para la elaboración de la versión pública de los Documentos de Seguridad, propuesta por el **Instituto de Matemáticas,** el **Instituto de Fisiología Celular,** la **Dirección General de la Escuela Nacional Colegio de Ciencias** y **Humanidades,** la **Escuela Nacional Colegio de Ciencias y Humanidades Planteles Azcapotzalco, Vallejo, Naucalpan, Oriente y Sur**, la **Facultad de Filosofía y Letras,** la **Coordinación de Difusión Cultural**, la **Dirección General de Estudios de Legislación Universitaria,** el **Centro Universitario de Teatro,** la **Dirección General de Radio UNAM,** la **Secretaría de Desarrollo Institucional,** el **Instituto de Física**, el **Consejo Académico del Área de las Ciencias Biológicas, Químicas y de la Salud,** el **Comité de Análisis para las Intervenciones Urbanas, Arquitectónicas y de las Ingenierías,** el **Museo Universitario del Chopo,** la **Dirección General de Música,** la **Dirección de Danza,** el **Centro de Investigaciones en Geografía Ambiental, Campus Morelia,** el **Museo Universitario de Arte Contemporáneo,** la **Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género,** el **Instituto de Química,** la **Dirección de Literatura y Fomento a la Lectura,** la **Dirección General de Servicios Administrativos,** la **Dirección de Teatro UNAM,** el **Centro de Ciencias Genómicas,** la **Facultad de Artes y Diseño,** la **Dirección General de Televisión Universitaria,** el **Centro Cultural Universitario Tlatelolco,** la **Dirección General de Orientación y Atención Educativa,** el **Consejo Académico del Área de las Ciencias Sociales,** la **Escuela Nacional de Estudios Superiores, Unidad Mérida,** el **Instituto de Ecología,** la **Dirección General de Cooperación e Internacionalización,** el **Instituto de Investigaciones Biomédicas,** la **Casa del Lago "Mtro. Juan José Arreola",** la **Coordinación para la Igualdad de Género,** la **Dirección General de la**

Escuela Nacional Preparatoria y la **Escuela Nacional Preparatoria, Planteles 3 "Justo Sierra"** y **4 "Vidal Castañeda y Nájera"** y la **Dirección General del Deporte Universitario,** en relación con el **Análisis de Riesgos**, el **Análisis de Brecha** y el **Plan de Trabajo**, así como **toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados** o **revele vulnerabilidades en la protección de los datos personales en poder de las Áreas Universitarias**, 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 al **Instituto de Matemáticas,** al **Instituto de Fisiología Celular,** a la **Dirección General de la Escuela Nacional Colegio de Ciencias** y **Humanidades,** a la **Escuela Nacional Colegio de Ciencias y Humanidades Planteles Azcapotzalco, Vallejo, Naucalpan, Oriente y Sur**, a la **Facultad de Filosofía y Letras,** a la **Coordinación de Difusión Cultural**, a la **Dirección General de Estudios de Legislación Universitaria,** al **Centro Universitario de Teatro,** a la **Dirección General de Radio UNAM**, a la **Secretaría de Desarrollo Institucional,** al **Instituto de Física**, al **Consejo Académico del Área de las Ciencias Biológicas, Químicas y de la Salud,** al **Comité de Análisis para las Intervenciones Urbanas, Arquitectónicas y de las Ingenierías,** al **Museo Universitario del Chopo,** a la **Dirección General de Música,** a la **Dirección de Danza,** al **Centro de Investigaciones en Geografía Ambiental, Campus Morelia,** al **Museo Universitario de Arte Contemporáneo,** a la **Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género,** al **Instituto de Química,** a la **Dirección de Literatura y Fomento a la Lectura,** a la **Dirección General de Servicios Administrativos,** a la **Dirección de Teatro UNAM,** al **Centro de Ciencias Genómicas,** a la **Facultad de Artes y Diseño,** a la **Dirección General de Televisión Universitaria,** al **Centro Cultural Universitario Tlatelolco,** a la **Dirección General de Orientación y Atención Educativa,** al **Consejo Académico del Área de las Ciencias Sociales,** la **Escuela Nacional de Estudios Superiores, Unidad Mérida,** al **Instituto de Ecología,** a la **Dirección General de Cooperación e Internacionalización,** al **Instituto de Investigaciones Biomédicas,** a la **Casa del Lago "Mtro. Juan José Arreola",** a la **Coordinación para la Igualdad de Género,** a la **Dirección General de la Escuela Nacional Preparatoria** y a la **Escuela Nacional Preparatoria, Planteles 3 "Justo Sierra"** y **4 "Vidal Castañeda y Nájera",** a la **Dirección General del Deporte Universitario,** así como a la Unidad de Transparencia de esta Universidad, para los efectos procedentes.

Así lo resolvió por unanimidad de votos de sus integrantes, el Comité de Transparencia de la Universidad Nacional Autónoma de México, en términos de los artículos 1, 11, 15, 20 y 53,

fracción VI del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

POR MI RAZA HABLARÁ EL ESPÍRITU"
Ciudad Universitaria, Cd. Mx., 19 de agosto de 2022

Archivo	08-ctunam-525-2022-docto-seg-1.pdf		
Identificador único (hash)	5c7a552404c38ce4b052cc8e212d4579a13448672db8ce248b096c2e568ad6cf		
Fecha y hora de cierre	19/08/2022 16:28:33	**Fecha y hora de emisión**	19/08/2022 16:30:53
Número de páginas	19	**Firmantes**	4

Firmantes

Nombre	Lic. MARIA ELENA GARCIA MELENDEZ	**Fecha y hora de firma**	19/08/2022 15:18:41
Directora General para la Prevención y Mejora de la Gestión Institucional y Suplente del Contralor			
Hash Firma	cbaca6eb689a47d8770065a6f6ff297b80269e390ef3f832d480a433bf1abbfbf4ed2ced4f3f344361b247c806f9e1e2		

Nombre	Ing. Ricardo Ramírez Ortiz	**Fecha y hora de firma**	19/08/2022 15:41:03
Director General de Servicios Generales y Movilidad			
Hash Firma	1ad0c05aa515c5cfb0a9def95dd4b62ff2c74d8447fbdc4130479cece21b04b4035d4865b90866689b75f86c70c2ce60		

Nombre	JOSE MELJEM MOCTEZUMA	**Fecha y hora de firma**	19/08/2022 16:28:33
Titular de la Unidad de Transparencia			
Hash Firma	8d01b7ff1fe5c4c30fcea6d96019f992ef58adde4f23ce469572c785c60d3e1d5d9bbef4bfee618dddfc45f27edac3db		

Nombre	Dra. Jacqueline Peschard Mariscal	**Fecha y hora de firma**	19/08/2022 16:19:26
Especialista			
Hash Firma	460b366695dd8e79de4878edcf8017579ce607f70964c5cabc1bcba1cdfd08f60261a88559c3ef1d8ea03ae660538626		

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

CENTRO DE INVESTIGACIONES EN GEOGRAFÍA AMBIENTAL

Documento de Seguridad

VERSIÓN PÚBLICA

Versión: 1.0
Revisión: 2022

Centro de Investigaciones en Geografía Ambiental

Sistema de Gestión de Seguridad de Datos Personales
Documento de Seguridad de datos personales

ÍNDICE

Introducción

El presente documento de seguridad contiene las medidas de seguridad administrativa, física y técnica aplicables a los sistemas de tratamiento de datos personales del Centro de Investigaciones en Geografía Ambiental (CIGA), con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información personal que éstos contienen.

Su propósito es identificar los sistemas de tratamiento de datos personales que posee esta área universitaria, el tipo de datos personales que contiene cada uno, los responsables, encargados, usuarios de cada sistema y las medidas de seguridad concretas implementadas.

El marco jurídico del documento de seguridad se regula por el capítulo II de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada el 26 de enero de 2017, que establece un conjunto mínimo de medidas de seguridad que cada dependencia o entidad universitaria deberá considerar al perfilar su estrategia de seguridad para la protección de los datos personales bajo su custodia, según el tipo de soportes —físicos, electrónicos o ambos— en los que residen dichos datos y dependiendo del nivel de protección que tales datos requieran.

Específicamente los artículos 31, 32 y 33 de la Ley General, del 55 al 72 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, publicados en el Diario Oficial de la Federación el 26 de enero de 2018, así como del 20 al 31 de los Lineamientos para la protección de datos personales en posesión de la Universidad Nacional Autónoma de México, publicados en la Gaceta UNAM el 25 de febrero de 2019.

El cimiento del formato de documento de seguridad es la aplicación de un enfoque basado en los riesgos de los activos universitarios, específicamente los datos personales y los soportes que los resguardan. Además, el formato considera el tamaño y estructura de la institución, objetivos, clasificación de la información, requerimientos de seguridad y procesos que se precisan en razón de los activos que posee esta Máxima Casa de Estudios, lo cual se encuentran contemplado en el estándar internacional en materia de seguridad de la información ISO/IEC 27002:2013 "*Tecnología de la información - Técnicas de seguridad - Código de práctica para los controles de seguridad de la información*".

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Identificador	Nombre del Sistema	Área responsable
SIA01	Sistema de Información Académica	Secretaría Académica
SSAD01	Sistema de Solicitudes Administrativas	Delegación Administrativa
WEBP01	Perfiles de personal	Secretaría Técnica

*(Llenar una tabla para cada sistema. Campos con * son obligatorios. Borrar instrucciones en cursivas)*

Área: Secretaría Académica	
Identificador único*	**SIA01**
(Nombre del sistema A1) *	**Sistema de Información Académica**
Datos personales (sensibles o no) contenidos en el sistema*:	**Datos personales:** Nombre(s) y apellidos(s), domicilio, teléfono particular, RFC, CURP, nacionalidad. **Datos laborales:** Fecha contrato CIGA, Fecha contrato UNAM, Nivel PRIDE, nombramiento, correo electrónico institucional, teléfono institucional. **Datos académicos:** Formación académica, experiencia laboral, investigación y resultados, actividades académicas y de apoyo institucional, movilidad académica (nombres invitados, procedencia invitados), nombre y procedencia de tesistas, practicantes, asesorados y servicio social, premios y distinciones.
Responsable*	
Nombre*:	**Dr. Manuel Mendoza Cantú**
Cargo*:	**Secretario Académico**
Funciones*:	Realizar el análisis y la generación de indicadores de productividad de las actividades semestrales del personal académico del Centro. Apoyar en la generación del Informe Anual institucional.
Obligaciones*:	Decidir la incorporación de nuevos usuarios al sistema y definir sus roles. Decidir la implementación de nuevas funcionalidades al sistema. Dar uso a la información para los fines que fue recabada.
Encargados[1]	
(Nombre del Encargado 1*)	**M.T.I. Hugo Alejandro Zavala Vaca**
Cargo*:	**Encargado de Telecomunicaciones**
Funciones*:	Mantenimiento preventivo y correctivo del servidor.
Obligaciones*:	Dar mantenimiento al servidor para garantizar su correcto funcionamiento. Realizar el respaldo periódico del servidor.
(Nombre del Encargado 2*)	**M.C. Fabiola Araceli Velázquez Ayala**

[1] Se tienen que ingresar los datos de todos los Encargados del sistema de tratamiento de datos personales.

Cargo*:	**Administrador de sistema y desarrollador**
Funciones*:	Implementación de procesos que garanticen la funcionalidad del sistema. Implementación de nuevas funcionalidades al sistema. Generación de usuarios con roles administrativos.
Obligaciones*:	Garantizar la protección y respaldo de la información. Dar uso a la información para los fines que fue recabada.
	Usuarios:
(Nombre del Usuario 1*)	Lic. Cristina Valadez Buenrostro
Cargo*:	Asistente de Secretaría Académica
Funciones*:	Alta de usuarios académicos. Generación de reportes de la información recabada.
Obligaciones*:	Dar uso a la información para los fines que fue recabada.
Área: Delegación Administrativa	
Identificador único*	**SSAD01**
Sistema (Nombre del A2)*:	**Sistema de Solicitudes Administrativas**
Datos personales contenidos en el sistema*:	**Datos personales:** Nombre(s) y apellido(s) **Datos laborales**: Correo electrónico institucional, teléfono institucional, tipo de solicitud.
Responsable	
Nombre*:	**Mtra. Geraldy García Torres**
Cargo*:	**Delegada Administrativa**
Funciones*:	Realizar el seguimiento y autorización de las diversas solicitudes administrativas del Centro.
Obligaciones*:	Decidir la incorporación de nuevos usuarios al sistema y definir sus roles. Decidir la implementación de nuevas funcionalidades al sistema. Dar uso a la información para los fines que fue recabada.
Encargados	
(Nombre del Encargado 1*)	**M.T.I. Hugo Alejandro Zavala Vaca**
Cargo*:	**Encargado de Telecomunicaciones**
Funciones*:	Mantenimiento preventivo y correctivo del servidor.
Obligaciones*:	Dar mantenimiento al servidor para garantizar su correcto funcionamiento. Realizar el respaldo periódico del servidor
(Nombre del Encargado 2*)	**M.C. Fabiola Araceli Velázquez Ayala**
Cargo*:	**Administrador de sistema y desarrollador**
Funciones*:	Implementación de procesos que garanticen la funcionalidad del sistema. Implementación de nuevas funcionalidades al sistema. Generación de usuarios con roles administrativos.
Obligaciones*:	Garantizar la protección y respaldo de la información. Dar uso a la información para los fines que fue recabada.
	Usuarios:
(Nombre del Usuario 1*)	Mtra. Geraldy García Torres
Cargo*:	Delegada Administrativa
Funciones*:	Seguimiento y respuesta de solicitudes de presupuesto, proyectos y servicios generales.

Obligaciones*:	Dar uso a la información para los fines que fue recabada.
(Nombre del Usuario 2*)	C.P. Nidia Romero
Cargo*:	Responsable de proyectos PAPIIT y CONACYT
Funciones*:	Seguimiento y respuesta de solicitudes asociadas a proyectos.
Obligaciones*:	Dar uso a la información para los fines que fue recabada.
(Nombre del Usuario 3*)	C.P. Frank Chávez
Cargo*:	Servicios Generales
Funciones*:	Seguimiento y respuesta de solicitudes asociadas a presupuesto y servicios generales.
Obligaciones*:	Dar uso a la información para los fines que fue recabada.
(Nombre del Usuario 4*)	C. Walter Hernández
Cargo*:	Asistente de Dirección
Funciones*:	Alta de usuarios invitados para seguimiento de solicitudes. Seguimiento y respuesta de solicitudes asociadas a servicios generales.
Obligaciones*:	Dar uso a la información para los fines que fue recabada.
(Nombre del Usuario 5*)	C. Salud Tovar
Cargo*:	Asistente de la Delegada Administrativa
Funciones*:	Recepción y alta de solicitudes. Asignación de usuarios para dar seguimiento a las solicitudes.
Obligaciones*:	Dar uso a la información para los fines que fue recabada.
Área: Secretaría Técnica	
Identificador único*	**WEBP01**
Sistema (Nombre del A3)*:	**Perfiles de personal**
Datos personales contenidos en el sistema*:	**Datos personales:** Nombre(s) y apellido(s), fotografía. **Datos laborales:** correo electrónico institucional, teléfono institucional, nombramiento. **Datos académicos:** Curriculum, URL de página académica (Sitio web, Google Scholar, LinkedIn u otro), semblanza académica, líneas de investigación, publicaciones académicas, proyectos vigentes.
Responsable	
Nombre*:	**Dr. Luis Miguel Morales Manilla**
Cargo*:	**Secretario Técnico**
Funciones*:	Decidir con visto bueno del Consejo Interno sobre las nuevas funcionalidades del sistema. Decidir sobre la actualización del sistema en función de su diseño y tipo de información a publicar.
Obligaciones*:	Dar uso a la información para los fines que fue recabada.
Encargados	
(Nombre del Encargado 1*)	**M.T.I. Hugo Alejandro Zavala Vaca**
Cargo*:	**Encargado de Telecomunicaciones**
Funciones*:	Mantenimiento preventivo y correctivo del servidor.
Obligaciones*:	Dar mantenimiento al servidor para garantizar su correcto funcionamiento. Realizar el respaldo periódico del servidor
(Nombre del Encargado 2*)	**M.C. Fabiola Araceli Velázquez Ayala**
Cargo*:	**Administrador de sistema y desarrollador**

Funciones*:	Gestión y administración del contenido web. Implementación de procesos que garanticen la funcionalidad del sistema.
Obligaciones*:	Verificar la correcta publicación de la información. Dar uso a la información para los fines que fue recabada.
(Nombre de usuario 1)	M.C. Fabiola Araceli Velázquez Ayala
Cargo	Técnico académico en la Unidad de Cómputo y Telecomunicaciones.
Funciones	Administración y gestión de contenido de los perfiles del personal del Centro que se visualizan en la página web principal.
Obligaciones	Actualizar el sistema que gestiona el contenido web y su respaldo periódico. Dar uso a la información para los fines que fue recabada.

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

*(Llenar una tabla para cada sistema. Campos con * son obligatorios. Borrar instrucciones en cursivas)*

Secretaría Académica	
Identificador único*	**SIA01**
(Nombre del sistema A1) *	**Sistema de Información Académica**
Tipo de soporte[2]:*	Soporte electrónico
Descripción[3]:*	Base de datos relacional
Características del lugar donde se resguardan los soportes[4]:*	Alojamiento en Servidor de UNAM-CIGA
	Delegación Administrativa
Identificador único*	**SSAD01**

[2] En caso de que el área universitaria prevea cambiar el tipo de soporte que utiliza el sistema de tratamiento de datos personales por ejemplo de físico a electrónico o en el supuesto de que prevea en el futuro utilizar ambos tipos de soportes, deberá indicarse en este rubro.

[3] Describir el soporte en el que se encuentran los datos por ejemplo para soportes físicos podrían ser formatos, listados, documentos o expedientes, entre otros y para soportes electrónicos, hoja de cálculo o base de datos relacional, entre otros.

[4] Para describir las características del lugar donde se resguardan los soportes, se deberá considerar lo siguiente:

a)Para soportes físicos, el área universitaria deberá incluir una descripción escrita con detalles sobre las características físicas de la oficina, almacén o bodega donde resguarda dichos soportes;

b)Para soportes electrónicos, la descripción ofrecida por el área universitaria deberá incluir un diagrama de la arquitectura de seguridad en el cual sea posible apreciar el flujo de datos a través de la o las redes electrónicas que interconectan los equipos (clientes, servidores, cortafuegos, unidades de almacenamiento, entre otros) del sistema de tratamiento de datos personales. Además, deberá describir las medidas de seguridad física que ha implementado para la protección del centro de datos donde residen tales soportes.

c)En caso de que el sistema de tratamiento de datos personales ocupe ambos tipos de soportes, deberá presentar las descripciones correspondientes a cada uno, en términos de lo señalado en los incisos a) y b) anteriores.

Sistema (Nombre del A2)*:	**Sistema de Solicitudes Administrativas**
Tipo de soporte*:	Soporte electrónico
Descripción*:	Base de datos relacional
Características del lugar donde se resguardan los soportes*:	Alojamiento en Servidor de UNAM-CIGA
Unidad de Cómputo y Telecomunicaciones	
Identificador único*	**WEBP01**
Sistema (Nombre del A3)*:	**Perfiles de personal**
Tipo de soporte*:	Soporte electrónico
Descripción*:	Base de datos relacional
Características del lugar donde se resguardan los soportes*:	Alojamiento en Servidor de UNAM-CIGA

3. ANÁLISIS DE RIESGOS

ANEXO I: Información reservada

4. ANÁLISIS DE BRECHA

ANEXO II: Información reservada

5. PLAN DE TRABAJO

ANEXO III: Información reservada

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

*(Llenar una tabla para cada sistema. Campos con * son obligatorios. Borrar instrucciones en cursivas)*

Secretaría Académica*	
Identificador único*	***SIA01***
(Nombre del sistema A1)*	**Sistema de Información Académica (SIA)**
TRANSFERENCIAS DE DATOS PERSONALES	

Transferencias mediante el traslado de soportes físicos:[5]	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan transferencias de datos personales mediante el traslado sobre redes electrónicas.
Delegación Administrativa	
Identificador único*	**SSAD01**
Sistema (Nombre del A2)*:	**Sistema de Solicitudes Administrativas**
Transferencias mediante el traslado de soportes físicos:[6]	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales mediante el traslado de soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan transferencias de datos personales mediante el traslado sobre redes electrónicas.
Unidad de Cómputo y Telecomunicaciones	
Identificador único*	**WEBP01**

[5] **Ejemplo de medidas de seguridad para transmisiones mediante el traslado de soportes físicos:**
a) La transmisión de datos personales mediante el traslado de soportes físicos se lleva a cabo por la vía elegida de común acuerdo entre las partes: mensajero oficial, asistente secretarial, visita personal, servicio de mensajería externo, entre otras posibles. Se define un destinatario primario y otro secundario por si el mensajero no encuentra al primero.
b) El paquete con datos personales en soportes físicos viaja debidamente sellado, de forma tal que sea perceptible cualquier violación o apertura no autorizada del mismo.
c) La entrega del paquete se realiza sólo si el destinatario acredita su identidad. Para ello, el destinatario presenta una identificación oficial con fotografía y el mensajero recaba nombre, firma y un número de referencia que aparezca en tal identificación, además de la fecha de entrega.
d) El mensajero no entrega el paquete si el destinatario no puede acreditar su identidad. En este caso, el mensajero devuelve el paquete al transmisor.
e) El transmisor verifica que el mensajero haya entregado el paquete al destinatario. Si el transmisor detecta que dicho paquete fue entregado a otra persona, da inicio al proceso de atención de un incidente.
f) Se registran estas transmisiones en el Sistema de tratamiento de datos personales.

[6] **Ejemplo de medidas de seguridad para transmisiones mediante el traslado de soportes físicos:**
g) La transmisión de datos personales mediante el traslado de soportes físicos se lleva a cabo por la vía elegida de común acuerdo entre las partes: mensajero oficial, asistente secretarial, visita personal, servicio de mensajería externo, entre otras posibles. Se define un destinatario primario y otro secundario por si el mensajero no encuentra al primero.
h) El paquete con datos personales en soportes físicos viaja debidamente sellado, de forma tal que sea perceptible cualquier violación o apertura no autorizada del mismo.
i) La entrega del paquete se realiza sólo si el destinatario acredita su identidad. Para ello, el destinatario presenta una identificación oficial con fotografía y el mensajero recaba nombre, firma y un número de referencia que aparezca en tal identificación, además de la fecha de entrega.
j) El mensajero no entrega el paquete si el destinatario no puede acreditar su identidad. En este caso, el mensajero devuelve el paquete al transmisor.
k) El transmisor verifica que el mensajero haya entregado el paquete al destinatario. Si el transmisor detecta que dicho paquete fue entregado a otra persona, da inicio al proceso de atención de un incidente.
l) Se registran estas transmisiones en el Sistema de tratamiento de datos personales.

Sistema (Nombre del A3)*:	Perfiles de personal
Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales mediante el traslado de soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan transferencias de datos personales mediante el traslado sobre redes electrónicas.

I. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

Secretaría Académica*	
Identificador único*	**SIA01**
(Nombre del sistema A1)*	**Sistema de Información Académica (SIA)**
Resguardo de sistemas de tratamiento de datos personales con soportes físicos	Se utiliza soporte electrónico mediante una base de datos relacional. No se realiza tratamiento de datos personales con soporte físico.
Delegación Administrativa	
Identificador único*	**SSAD01**
Sistema (Nombre del A2)*:	**Sistema de Solicitudes Administrativas**
Resguardo de sistemas de tratamiento de datos personales con soportes físicos	Se utiliza soporte electrónico mediante una base de datos relacional. No se realiza tratamiento de datos personales con soporte físico.
Unidad de Cómputo y Telecomunicaciones	
Identificador único*	**WEBP01**
Sistema (Nombre del A3)*:	**Perfiles de personal**
Resguardo de sistemas de tratamiento de datos personales con soportes físicos	Se utiliza soporte electrónico mediante una base de datos relacional. No se realiza tratamiento de datos personales con soporte físico.

1. Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.[7]

2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.[8]

[7] Por ejemplo, se espera que precise si los formatos impresos, documentos, listados o expedientes están foliados, cosidos o engargolados, si los muebles o la estantería donde residen cuentan con cerradura, si existen mecanismos para regular la temperatura y la humedad, si existen sistemas de tratamiento de datos personales de detección y/o supresión de incendios, si cuenta con mecanismos para regular y mantener el suministro continuo de energía eléctrica, entre otras posibles medidas.

[8] En caso de ser muchas personas, se sugiere agregar el listado como Anexo al Documento de seguridad.

II. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. Los datos que se registran en las bitácoras:[9]

a) Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida;

b) Para soportes físicos: Número o clave del expediente utilizado, y

c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.

[9] Las áreas de informática y seguridad de la información han designado una persona que se encarga de realizar un análisis de las bitácoras generadas. Las siguientes características aplican al caso:

a) Se cuenta con la ayuda de una herramienta informática adquirida para tal propósito.
b) Cada semana se llevan a cabo análisis de bitácoras, pero no de todas ellas. Depende de la bitácora y de las amenazas detectadas en el entorno.

Ejemplo de medidas de seguridad aplicables a bitácoras para sistema de tratamiento de datos personales en soportes físicos: El responsable del sistema procurará un estricto control y registro de:

a) Las autorizaciones emitidas para facultar el acceso a un funcionario universitario a fin de que éste, en el ejercicio de sus funciones, pueda interactuar con uno o más de los sistemas de tratamiento de datos personales a su cargo.
b) La asignación, actualización y reemplazo de las llaves que entrega a los autorizados para que éstos puedan abrir el mecanismo de apertura de la puerta en la zona de acceso restringido. Las acciones que los autorizados llevan a cabo en el área de resguardo. Para ello, designa a un Encargadc quien anota lo siguiente: Quién solicita el acceso, cuándo se lleva a cabo (fecha y hora de entrada y salida), la razón que lo motiva y número del expediente utilizado.
c) El préstamo de expedientes es asistido por un sistema de tratamiento de datos personales de cómputo que utiliza códigos de barras en los gafetes del personal autorizado y en los expedientes.
d) El sistema de tratamiento de datos personales de préstamo de expedientes genera una bitácora electrónica que se respalda diariamente en un servidor dentro del centro de cómputo que administra el área de informática. Su integridad se garantiza copiando dicha bitácora en un CD-R diariamente.
e) El Encargado del sistema de tratamiento de datos personales es la persona designada para analizar la bitácora cada mes mediante una herramienta adquirida para tal fin.

Ejemplo de medidas de seguridad aplicables a bitácoras para sistema de tratamiento de datos personales en soportes electrónicos:

I. El responsable del sistema de tratamiento de datos personales -en coordinación con las áreas de informática y seguridad de la información- lleva un estricto control y registro de:

a) Las bitácoras de eventos ocurridos a nivel *sistema de tratamiento de datos personales operativo* en los equipos (servidores, cortafuegos, almacenamiento masivo) que habilitan la operación del sistema de tratamiento de datos personales. Entre otras, se generan bitácoras para desempeño del servidor: intentos de acceso (exitosos y fallidos); accesos denegados a usuarios y terminales; uso de herramientas para administración del servidor, y fecha y hora de los eventos anteriores.

b) Las bitácoras de eventos generados a nivel *software aplicativo* del sistema de tratamiento de datos personales. Entre otras, se generan bitácoras para mensajes de error; apertura, modificación y cierre de archivos; violaciones de seguridad detectadas por el software aplicativo, y fecha y hora de estos eventos.

c) Las bitácoras de eventos relativos a las actividades de usuarios (capturistas, Encargados, el propio responsable y el administrador del servidor) en su interacción con el sistema de tratamiento de datos personales. Entre otras, se generan bitácoras para: archivos servicios y recursos utilizados; intentos de acceso (exitosos y fallidos); comandos y operaciones iniciadas, y fecha y hora de dichos eventos.

d) El conjunto de bitácoras permite registrar, entre otros, los siguientes datos: Quién accede a los datos personales, desde dónde y con qué; accesos (intentos exitosos y fallidos) y salidas; propósito del acceso (sólo para modificaciones en el software aplicativo); operaciones llevadas a cabo; datos personales (registros y campos) utilizados de la base de datos, y fecha y hora de estos eventos.

e) Las bitácoras arriba mencionadas están todas en soportes electrónicos y se almacenan al menos por dos años en CD-R. Se tiene una copia en el centro de datos y otra se lleva a una bóveda bancaria subcontratada también para los respaldos.

II. La integridad de las bitácoras se garantiza copiándolas en un servidor del centro de datos el cual las graba en CD-R. Algunas se copian cada hora, otras a diario. La integridad de las copias se garantiza además con "resúmenes" creados por un algoritmo "digestor". Se cuenta con una herramienta de software que automatiza estas operaciones.

III. Se pueden realizar análisis focalizados a mayor profundidad en caso de presentarse un incidente que así lo requiera.

2. Si las bitácoras están en soporte físico o en soporte electrónico;[10] **3.** Lugar dónde almacena las bitácoras y por cuánto tiempo; **4.** La manera en que asegura la integridad de las bitácoras, y **5.** Respecto del análisis de las bitácoras: **a)** Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza, y **b)** Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.	
Secretaría Académica*	
Identificador único*	**SIA01**
(Nombre del sistema A1)*	**Sistema de Información Académica (SIA)**
1) El sistema guarda bitácoras de accesos de usuarios y de servidor, con acceso de administrador del sistema. 2) Las bitácoras se encuentran en soporte electrónico. 3) Se almacenan en el servidor, de manera semestral. 4) El acceso a las bitácoras es exclusivo al usuario administrador del sistema y del servidor. 5) El departamento de Cómputo y Telecomunicaciones realiza el análisis de las bitácoras de servidor. 6) Se utilizan herramientas de análisis evento de log de servidor de preferencia de software libre.	
Delegación Administrativa	
Identificador único*	**SSAD01**
Sistema (Nombre del A2)*:	**Sistema de Solicitudes Administrativas**
1) El sistema guarda bitácoras de accesos de usuarios y de servidor, con acceso de administrador del sistema. 2) Las bitácoras se encuentran en soporte electrónico. 3) Se almacenan en el servidor, de manera semestral. 4) El acceso a las bitácoras es exclusivo al usuario administrador del sistema y del servidor. 5) El departamento de Cómputo y Telecomunicaciones realiza el análisis de las bitácoras de servidor. 6) Se utilizan herramientas de análisis evento de log de servidor de preferencia de software libre.	
Unidad de Cómputo y Telecomunicaciones	
Identificador único*	**WEBP01**
Sistema (Nombre del A3)*:	**Perfiles de personal**
1) El sistema guarda bitácoras de accesos de usuarios y de servidor, con acceso de administrador del sistema. 2) Las bitácoras se encuentran en soporte electrónico. 3) Se almacenan en el servidor, de manera semestral. 4) El acceso a las bitácoras es exclusivo al usuario administrador del sistema y del servidor. 5) El departamento de Cómputo y Telecomunicaciones realiza el análisis de las bitácoras de servidor. 6) Se utilizan herramientas de análisis evento de log de servidor de preferencia de software libre.	

III. REGISTRO DE INCIDENTES:

[10] En caso de tener las bitácoras en soportes físicos, debe señalar si en el futuro planea incorporarlas a soportes electrónicos.

Describir el procedimiento de atención de incidentes que tiene implementado el área universitaria y especificar si lleva registro de los incidentes relativos a soportes físicos, como lo son la pérdida o alteración no autorizada de expedientes, y para el caso de soportes electrónicos, ofrecer detalles sobre el registro de incidentes en el cual consigne los procedimientos realizados para la recuperación de los datos o para permitir la disponibilidad del proceso.

1. Los datos que registra:
   a) La persona que resolvió el incidente;
   b) La metodología aplicada;[11]
   c) Para soportes físicos: Los oficios, documentos, expedientes, estantes o archiveros, tanto los dañados como los recuperados, y
   d) Para soportes electrónicos: Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados, el nombre de los sistemas y la infraestructura afectada, indicar si el incidente afectó el servidor principal y los servidores de respaldo, etc.
2. Si el registro está en soporte físico o en soporte electrónico;
3. Cómo asegura la integridad de dicho registro, y
4. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos.

Secretaría Académica*	
Identificador único*	**SIA01**
(Nombre del sistema A1)*	**Sistema de Información Académica (SIA)**
No se tiene un procedimiento para la atención de incidentes.	
Delegación Administrativa	
Identificador único*	**SSAD01**
Sistema (Nombre del A2)*:	**Sistema de Solicitudes Administrativas**
No se tiene un procedimiento para la atención de incidentes.	
Unidad de Cómputo y Telecomunicaciones	
Identificador único*	**WEBP01**
Sistema (Nombre del A3)*:	**Perfiles de personal**
No se tiene un procedimiento para la atención de incidentes.	

[11] **Ejemplo de procedimiento en caso de presentarse un incidente:**

a) El Encargado elabora y entrega un informe al responsable a más tardar al día siguiente de haber ocurrido el incidente. Dicho informe precisa los soportes físicos o electrónicos afectados y, en su caso, los recuperados.

b) El incidente se registra en una hoja de cálculo anotando quién resolvió el incidente y los soportes dañados y recuperados. Dicha hoja está protegida con una contraseña de acceso. Su integridad se garantiza generando y almacenando un resumen creado por un algoritmo digestor en un servidor del centro de datos y respaldándola en un CD-R después de registrar un incidente.

c) En caso de robo o extravío de datos personales, el responsable del sistema de tratamiento de datos personales, al tener conocimiento del incidente, da vista al titular de la dependencia o entidad para su conocimiento y al titular del área jurídica o aquél que tenga facultades para presentar denuncias o querellas ante el Ministerio Público para que, en el ámbito de sus atribuciones, determine lo conducente.

d) A no más de 3 días naturales de haber ocurrido el incidente, el responsable del sistema de tratamiento de datos personales da aviso al público mediante un desplegado de prensa que difunde el hecho por diversos medios, según la gravedad del caso, a escala local, regional o nacional.

e) En caso de robo o extravío de datos personales, se alerta a los titulares de los datos afectados para que tomen sus precauciones ante el posible uso ilegal de su información. Para tal efecto, el responsable del sistema de tratamiento de datos personales da aviso por escrito a dichos titulares, a más tardar cinco días naturales de haber ocurrido el incidente, recabando el acuse de recibo de esta notificación. Adicionalmente, se da aviso por correo electrónico o por teléfono.

V. ACCESO A LAS INSTALACIONES

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):

¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones? Por ejemplo, se espera que describa si cuenta con uno o más puntos de control de acceso y quienes los operan, si tiene vigilancia las 24 horas, si ha levantado bardas o cercas, si existe un sistema de tratamiento de datos personales de videovigilancia, entre otras posibles medidas.

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica? Se solicita la identificación de acceso vehicular a usuarios y visitantes en la caseta de entrada al campus, no se cuenta con proceso de identificación al acceso peatonal.

b) ¿Cómo las autentifica?

c) Acceso vehicular: Mediante la credencial UNAM, INE o listas de acceso enviadas a la caseta de entrada.

d) ¿Cómo les autoriza el acceso?
Acceso vehicular: Mediante listas de acceso o verificación telefónica en cada dependencia.

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema? Por ejemplo, se espera que precise el tipo de puertas y cerraduras instaladas, si tiene instalados controles biométricos, si administra la asignación de llaves y/o claves de acceso para abrir puertas y/o estantería, si cuenta con vigilancia las 24 horas, si hay un sistema de tratamiento de datos personales de videovigilancia, entre otras medidas.

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica?
   Mediante una lista de acceso de personal autorizado generada por la Administración.
2. ¿Cómo las autentifica?
   Mediante credencial y número de empleado.
3. ¿Cómo les autoriza el acceso?
   Mediante la lista de acceso autorizada.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

En este apartado se deberá establecer un mecanismo o procedimiento institucional para la actualización de la información personal contenida en el sistema, en donde se establezca la frecuencia con la que se efectúa y la forma en que se está solicitando al titular acreditar de manera idónea sus requerimientos de rectificación de datos inexactos.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.

1. Modelo de control de acceso (alguno de los siguientes):

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
b) ¿Es discrecional (matriz de control de acceso)?
c) ¿Está basado en roles (perfiles) o grupos?: **Se encuentra basado en roles (perfiles)**
d) ¿Está basado en reglas?

2. Perfiles de usuario y contraseñas en el sistema operativo de red:
- **a)** ¿Cuenta con un sistema operativo de red instalado en sus equipos? **Sí.**
- **b)** ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas? **Sí.**
- **c)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? **Sí.**

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:
- **a)** ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas? **Sí.**
- **b)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? **Sí.**

4. Administración de perfiles de usuario y contraseñas:
- **a)** ¿Quién da de alta nuevos perfiles? **Los usuarios con roles administrativos.**
- **b)** ¿Quién autoriza la creación de nuevos perfiles? **Los responsables de cada sistema.**
- **c)** ¿Se lleva registro de la creación de nuevos perfiles? **Desde los reportes del sistema.**

5. Acceso remoto al sistema de tratamiento de datos personales:
- **a)** ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema? **No, el acceso es posible mediante un equipo con conexión internet y navegador web.**
- **b)** ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas

de mantenimiento? **Sí.**

c) ¿Cómo se evita el acceso remoto no autorizado? **Se implementan controles de acceso basados en roles y privilegios.**

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
   a) Completos X, diferenciales ___ o incrementales___;
   b) De forma automática X o Manual ___.
   c) Periodicidad con que los realiza: Quincenal.
2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad:[12] Disco duro
3. Cómo y dónde archiva esos medios, Sistema de Almacenamiento resguardado por el Departamento de Cómputo y Telecomunicaciones y
4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero). El área universitaria

IX. PLAN DE CONTINGENCIA

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.
   No se tiene desarrollado un Plan de Contingencia.
2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.
   No se cuenta con un Plan de Contingencia
3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:
   a) El tipo de sitio (caliente, tibio o frío);[13]
   b) Si el sitio es propio o subcontratado con un tercero;

[12] Es deseable que precise si para almacenar dichos medios cuenta con al menos dos lugares distintos que cumplan con las condiciones de seguridad especificadas en el articulado del Capítulo V de los Lineamientos, conforme a la fracción III del Trigésimo primero de los Lineamientos; o bien, si utiliza un espacio externo seguro para guardar de manera sistemática dichos respaldos, según la fracción VIII del Trigésimo séptimo de tales Lineamientos.

[13] El tipo de sitio caliente, tibio o frío se refiere a la infraestructura, el equipo y el software disponibles en el sitio alterno; por lo que a mayor disponibilidad de dichos elementos resulta una menor demora para restablecer las operaciones de uno o más sistema de tratamiento de datos personales. Ejemplos de lo anterior son, en cuanto a **infraestructura:** aire acondicionado, cableado, suministro de energía eléctrica y enlaces de comunicaciones; en cuanto al **equipo**: servidores, almacenamiento y periféricos, y por lo que se refiere al **software:** sistema de tratamiento de datos personales operativos, manejadores de bases de datos y aplicaciones. Por lo tanto:
i) En un **sitio alterno caliente** se mantienen disponibles en todo momento la infraestructura, el equipo y el software; lo único que hace falta para iniciar operaciones son los datos y el personal. Este tipo de sitios alternos es el más costoso, pero supone tan solo unas cuantas horas para restaurar operaciones.
ii) El **sitio alterno tibio** cuenta con infraestructura no configurada y equipos equivalentes que pueden estar disponibles en pocas horas, pero no contienen software ni datos. Este tipo de sitios alternos es el punto medio en costo y tiempo para restaurar operaciones.
iii) El **sitio alterno frío** cuenta con un ambiente mínimo de infraestructura y no cuenta con el equipo. Este tipo de sitios alternos es el menos costoso, pero supone demora de algunos días para restablecer operaciones.

c) Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio y
d) Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia.

No se cuenta con un Sitio Redundante

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

(Llenar una tabla para cada sistema. Campos con * son obligatorios. Borrar instrucciones en cursivas)

Secretaría Académica*		
Identificador único*	*SIA01*	
(Nombre del sistema A1)*	*Sistema de Información Académica*	
Recurso*	**Descripción***	**Control***
Roles	*Control de acceso a las funciones del sistema de acuerdo con la definición de cada rol.*	*Se asigna el rol en la generación de las credenciales de usuario. Resp. Usuario administrador del sistema. M.C. Fabiola A. Velázquez Ayala*
Escaneo de puertos abiertos	*Revisión programada*	*Uso de herramientas de software libre para realizar el escaneo de puertos abiertos en el sistema. Resp. Encargado Unidad de Cómputo. M.T.I. Hugo Alejandro Zavala Vaca*
Delegación Administrativa*		
Identificador único*	*SSAD01*	
(Nombre del sistema A2)*	*Sistema de Solicitudes Administrativas*	
Recurso*	**Descripción***	**Control***
Roles	*Control de acceso a las funciones del sistema de acuerdo con la definición de cada rol.*	*Se asigna el rol en la generación de las credenciales de usuario. Resp. Usuario administrador del sistema. M.C. Fabiola A. Velázquez Ayala*
Escaneo de puertos abiertos	*Revisión programada*	*Uso de herramientas de software libre para realizar el escaneo de puertos abiertos en el sistema. Resp. Encargado Unidad de Cómputo. M.T.I. Hugo Alejandro Zavala Vaca*
Secretaría Técnica*		

Identificador único*	*WEBP01*	
(Nombre del sistema A3)*	*Perfiles de personal*	
Recurso*	**Descripción***	**Control***
Roles	*Control de acceso a las funciones del sistema de acuerdo con la definición de cada rol.*	*Se asigna el rol en la generación de las credenciales de usuario. Resp. Usuario administrador del sistema. M.C. Fabiola A. Velázquez Ayala*
Escaneo de puertos abiertos	*Revisión programada*	*Uso de herramientas de software libre para realizar el escaneo de puertos abiertos en el sistema. Encargado Unidad de Cómputo. M.T.I. Hugo Alejandro Zavala*
Actualización de paquetes de seguridad.	*Se verifica periódicamente los paquetes y actualizaciones de seguridad disponibles para el sistema operativo y el sistema web.*	*Paquetes de distribución del S.O. y Sistema Web. Responsable: M.C. Fabiola A. Velázquez Ayala.*

7.2. Procedimiento para la revisión de las medidas de seguridad

*(Llenar una tabla para cada sistema. Campos con * son obligatorios. Borrar instrucciones en cursivas)*

Secretaria Académica*		
Identificador único*	***SIA01***	
(Nombre del sistema A1)*	**Sistema de Información Académica**	
Medida de seguridad*	**Procedimiento***	**Responsable***
Generación de Respaldo	Verificación de la generación correcta de los respaldos.	Encargado de telecomunicaciones. M.T.I. Hugo Alejandro Zavala Duración: uno a tres días hábiles
Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM	Verificación de la sincronización con una instancia central de tiempo, en este caso el servidor NTP de la UNAM.	Encargado de telecomunicaciones. M.T.I. Hugo Alejandro Zavala Duración: un día hábil
Autenticación para las personas autorizadas con base en el principio del menor privilegio.	Verificación del tipo de control de acceso al sistema. Revisar que los privilegios de acceso sean los adecuados en función del rol del usuario.	Administrador del sistema. M.C. Fabiola A. Velázquez Ayala Duración: cuatro días hábiles
Instalación de las actualizaciones de seguridad más recientes disponibles.	Revisar y actualizar el sistema operativo.	Administrador del sistema. M.C. Fabiola A. Velázquez Ayala Duración: cuatro días hábiles.

Instalación y mantenimiento de software antimalware	Instalar y verificar la actualización del software antimalware.	Administrador del sistema. M.C. Fabiola A. Velázquez Ayala Duración: dos días hábiles
Delegación Administrativa*		
Identificador único*	***SSAD01***	
(Nombre del sistema A2)*	**Sistema de Solicitudes Administrativas**	
Medida de seguridad*	**Procedimiento***	**Responsable***
Generación de Respaldo	Verificación de la generación correcta de los respaldos.	Encargado de telecomunicaciones. M.T.I. Hugo Alejandro Zavala Duración: uno a tres días hábiles
Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM	Verificación de la sincronización con una instancia central de tiempo, en este caso el servidor NTP de la UNAM.	Encargado de telecomunicaciones. M.T.I. Hugo Alejandro Zavala Duración: un día hábil
Autenticación para las personas autorizadas con base en el principio del menor privilegio.	Verificación del tipo de control de acceso al sistema. Revisar que los privilegios de acceso sean los adecuados en función del rol del usuario.	Administrador del sistema. M.C. Fabiola A. Velázquez Ayala Duración: cuatro días hábiles
Instalación de las actualizaciones de seguridad más recientes disponibles.	Revisar y actualizar el sistema operativo.	Administrador del sistema. M.C. Fabiola A. Velázquez Ayala Duración: cuatro días hábiles.
Instalación y mantenimiento de software antimalware	Instalar y verificar la actualización del software antimalware.	Administrador del sistema. M.C. Fabiola A. Velázquez Ayala Duración: dos días hábiles
Secretaria Técnica*		
Identificador único*	***WEBP01***	
(Nombre del sistema A3)*	**Perfiles de Personal**	
Medida de seguridad*	**Procedimiento***	**Responsable***
Generación de Respaldo	Verificación de la generación correcta de los respaldos.	Encargado de telecomunicaciones. M.T.I. Hugo Alejandro Zavala Duración: uno a tres días hábiles
Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM	Verificación de la sincronización con una instancia central de tiempo, en este caso el servidor NTP de la UNAM.	Encargado de telecomunicaciones. M.T.I. Hugo Alejandro Zavala Duración: un día hábil
Autenticación para las personas autorizadas con base en el principio del menor privilegio.	Verificación del tipo de control de acceso al sistema. Revisar que los privilegios de acceso sean los	Administrador del sistema. M.C. Fabiola A. Velázquez Ayala Duración: cuatro días hábiles

	adecuados en función del rol del usuario.	
Instalación de las actualizaciones de seguridad más recientes disponibles.	Revisar y actualizar el sistema operativo.	Administrador del sistema. M.C. Fabiola A. Velázquez Ayala Duración: cuatro días hábiles.
Instalación y mantenimiento de software antimalware	Instalar y verificar la actualización del software antimalware.	Administrador del sistema. M.C. Fabiola A. Velázquez Ayala Duración: dos días hábiles

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

*(Llenar una tabla para cada sistema. Campos con * son obligatorios. Borrar instrucciones en cursivas)*

Secretaría Académica		
Identificador único*	**Sistema de Información Académica**	
(Nombre del sistema A1)*	**SIA01**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Generación de Respaldo	Se verificó la realización de los respaldos actualizados del sistema.	Encargado de telecomunicaciones. M.T.I. Hugo Alejandro Zavala
Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM	El servidor se encuentra sincronizados con el servidor NTP de la UNAM.	Encargado de telecomunicaciones. M.T.I. Hugo Alejandro Zavala
Autenticación para las personas autorizadas con base en el principio del menor privilegio.	Se revisó que los privilegios de acceso son los adecuados en función del rol del usuario.	Administrador del sistema. M.C. Fabiola A. Velázquez Ayala
Instalación de las actualizaciones de seguridad más recientes disponibles.	Se actualizó el sistema operativo.	Administrador del sistema. M.C. Fabiola A. Velázquez Ayala
Instalación y mantenimiento de software antimalware	Se actualizó software antimalware.	Administrador del sistema. M.C. Fabiola A. Velázquez Ayala
Delegación Administrativa		
Identificador único*	**Sistema de Solicitudes Administrativas**	
(Nombre del sistema A2)*	**SSAD01**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Generación de Respaldo	Se verificó la realización de los respaldos actualizados del sistema.	Encargado de telecomunicaciones. M.T.I. Hugo Alejandro Zavala
Sincronizar la fecha y hora con el servidor NTP	El servidor se encuentra sincronizados con el servidor NTP de la UNAM.	Encargado de telecomunicaciones. M.T.I. Hugo Alejandro Zavala

(Network Time Protocol) oficial de la UNAM		
Autenticación para las personas autorizadas con base en el principio del menor privilegio.	Se revisó que los privilegios de acceso son los adecuados en función del rol del usuario.	Administrador del sistema. M.C. Fabiola A. Velázquez Ayala
Instalación de las actualizaciones de seguridad más recientes disponibles.	Se actualizó el sistema operativo.	Administrador del sistema. M.C. Fabiola A. Velázquez Ayala
Instalación y mantenimiento de software antimalware	Se actualizó software antimalware.	Administrador del sistema. M.C. Fabiola A. Velázquez Ayala
Secretaría Técnica		
Identificador único*	**Páginas de personal**	
(Nombre del sistema A3)*	**WEBP01**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Generación de Respaldo	Se verificó la realización de los respaldos actualizados del sistema.	Encargado de telecomunicaciones. M.T.I. Hugo Alejandro Zavala
Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM	El servidor se encuentra sincronizados con el servidor NTP de la UNAM.	Encargado de telecomunicaciones. M.T.I. Hugo Alejandro Zavala
Autenticación para las personas autorizadas con base en el principio del menor privilegio.	Se revisó que los privilegios de acceso son los adecuados en función del rol del usuario.	Administrador del sistema. M.C. Fabiola A. Velázquez Ayala
Instalación de las actualizaciones de seguridad más recientes disponibles.	Se actualizó el sistema operativo.	Administrador del sistema. M.C. Fabiola A. Velázquez Ayala
Instalación y mantenimiento de software antimalware	Se actualizó software antimalware.	Administrador del sistema. M.C. Fabiola A. Velázquez Ayala

7.4. Acciones para la corrección y actualización de las medidas de seguridad

*(Llenar una tabla para cada sistema. Campos con * son obligatorios. Borrar instrucciones en cursivas)*

Secretaría Académica		
Identificador único*	***SIA01***	
(Nombre del sistema A1)*	**Sistema de Información Académica**	
Medida de seguridad*	**Acciones***	**Responsable***

Plan de migración del sistema operativo	Elaborar un plan de migración del sistema a otro sistema operativo en caso de necesidad de actualizaciones	Encargado de telecomunicaciones. M.T.I. Hugo Alejandro Zavala
Delegación Administrativa		
Identificador único*	***SSAD01***	
(Nombre del sistema A2)*	**Sistema de Solicitudes Administrativas**	
Medida de seguridad*	**Acciones***	**Responsable***
Plan de migración del sistema operativo	Elaborar un plan de migración del sistema a otro sistema operativo en caso de necesidad de actualizaciones	Encargado de telecomunicaciones. M.T.I. Hugo Alejandro Zavala
Plan de versionamiento	Verificar las nuevas versiones disponibles del sistema y realizar la actualización correspondiente previa evaluación de impacto al cambio de versión.	Administrador del Sistema M.C. Fabiola A. Velázquez Ayala
Secretaría Técnica		
Identificador único*	***WEBP01***	
(Nombre del sistema A3)*	**Perfiles de personal**	
Medida de seguridad*	**Acciones***	**Responsable***
Plan de migración del sistema operativo	Elaborar un plan de migración del sistema a otro sistema operativo en caso de necesidad de actualizaciones	Encargado de telecomunicaciones. M.T.I. Hugo Alejandro Zavala
Plan de versionamiento	Verificar las nuevas versiones disponibles del sistema y realizar la actualización correspondiente previa evaluación de impacto al cambio de versión.	Administrador del Sistema M.C. Fabiola A. Velázquez Ayala

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de seguridad de datos personales

*(Llenar una tabla para cada sistema. Campos con * son obligatorios. Borrar instrucciones en cursivas)*

Secretaría Académica			
Identificador único*	*SIA01*		
(Nombre del sistema A1)*	**Sistema de Información Académica**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Capacitación para el personal responsable de	Curso "Protección de Datos Personales" tomado en la institución	*10 horas, en línea, marzo 2022.*	*Personal responsable de protección de datos personales.*

seguridad de datos personales	Unidad de Transparencia, UNAM		
	Curso "Medidas de Seguridad Técnicas para la Protección de Datos Personales, DGTIC - UNAM	*25 horas, en línea, Abril-Mayo 2021*	
Delegación Administrativa			
Identificador único*	*SSAD01*		
(Nombre del sistema A2)*	**Sistema de Solicitudes Administrativas**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Capacitación para el personal responsable de seguridad de datos personales	Curso "Protección de Datos Personales" tomado en la institución Unidad de Transparencia, UNAM	*10 horas, en línea, marzo 2022.*	*Personal responsable de protección de datos personales.*
	Curso "Medidas de Seguridad Técnicas para la Protección de Datos Personales, DGTIC - UNAM	*25 horas, en línea, Abril-Mayo 2021*	
Secretaría Técnica			
Identificador único*	*WEBP01*		
(Nombre del sistema A3)*	**Sistema de Información Académica**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Capacitación para el personal responsable de seguridad de datos personales	Curso "Protección de Datos Personales" tomado en la institución Unidad de Transparencia, UNAM	*10 horas, en línea, marzo 2022.*	*Personal responsable de protección de datos personales.*
	Curso "Medidas de Seguridad Técnicas para la Protección de Datos Personales, DGTIC - UNAM	*25 horas, en línea, Abril-Mayo 2021*	

8.2. Programa de difusión de la protección a los datos personales

*(Llenar una tabla para cada sistema. Campos con * son obligatorios. Borrar instrucciones en cursivas)*

Secretaría Académica			
Identificador único*	*SIA01*		
(Nombre del sistema A1)*	**Sistema de Información Académica**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un Programa de Difusión de Protección de Datos Personales			
Delegación Administrativa			
Identificador único*	*SSAD01*		

(Nombre del sistema A2)*	**Sistema de Solicitudes Administrativas**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un Programa de Difusión de Protección de Datos Personales			
Secretaría Técnica			
Identificador único*	*WEBP01*		
(Nombre del sistema A3)*	**Sistema de Información Académica**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un Programa de Difusión de Protección de Datos Personales			

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

*(Llenar una tabla para cada sistema. Campos con * son obligatorios. Borrar instrucciones en cursivas)*

Secretaría Académica			
Identificador único*	**Secretaría Académica**		
(Nombre del sistema A1)*	***SIA01***		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualizar rubros académicos	Se realiza la actualización de los rubros académicos a incluir en el sistema.	Depende del tipo de actualización a realizar.	Parcial, dependiendo de si se agrega un nuevo rubro académico y la información correspondiente o se agrega más información a un rubro ya existente.
Migración del sistema	Dependiendo de las necesidades puede requerirse en algún momento la actualización completa del entorno de desarrollo del sistema.	24 meses (aprox.)	Total, migración a un nuevo sistema.
Sistema de Solicitudes Administrativas			

Identificador único*	**Delegación Administrativa**		
(Nombre del sistema A2)*	**SSAD01**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualizar solicitudes	Se realiza la actualización de la información contenida en cada solicitud.	Depende del tipo de actualización a realizar.	Parcial, dependiendo de si se agrega una nueva solicitud o se agrega más información a una solicitud ya existente.
Perfiles de personal			
Identificador único*	**Secretaría Técnica**		
(Nombre del sistema A3)*	**WEBP01**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización de información a mostrar.	Se realiza la actualización de la información a publicar.	Depende del tipo de actualización a realizar.	Total, sobre la información publicada del personal del centro.
Migración del sistema	Dependiendo de las necesidades puede requerirse en algún momento la actualización completa del entorno de desarrollo del sistema.	6 meses (aprox.)	Total, migración a un nuevo sistema.

9.2. Actualización y mantenimiento de equipo de cómputo

*(Llenar una tabla para cada sistema. Campos con * son obligatorios. Borrar instrucciones en cursivas)*

Secretaría Académica			
Identificador único*	**Secretaría Académica**		
(Nombre del sistema A1)*	*SIA01*		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización del sistema operativo	Actualización de los parches de seguridad del sistema operativo.	4 días	Total
Sistema de Solicitudes Administrativas			
Identificador único*	**Delegación Administrativa**		
(Nombre del sistema A2)*	SSAD01		
Actividad*	**Descripción***	**Duración***	**Cobertura***

Actualización del sistema operativo	Actualización de los parches de seguridad del sistema operativo.	4 días	Total
Perfiles de personal			
Identificador único*	**Secretaría Técnica**		
(Nombre del sistema A3)*	WEBP01		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización del sistema operativo	Actualización de los parches de seguridad del sistema operativo.	4 días	Total

9.3. Procesos para la conservación, preservación y respaldos de información

*(Llenar una tabla para cada sistema. Campos con * son obligatorios. Borrar instrucciones en cursivas)*

Secretaría Académica		
Identificador único*	**Secretaría Académica**	
(Nombre del sistema A1)*	*SIA01*	
Proceso*	**Descripción***	**Responsable***
Respaldo de información	Se realiza el proceso de respaldo completo del servidor y sus aplicaciones.	Encargado de telecomunicaciones. M.T.I. Hugo Zavala Vaca Un día hábil
Sistema de Solicitudes Administrativas		
Identificador único*	**Delegación Administrativa**	
(Nombre del sistema A2)*	SSAD01	
Proceso*	**Descripción***	**Responsable***
Respaldo de información	Se realiza el proceso de respaldo completo del servidor y sus aplicaciones.	Encargado de telecomunicaciones. M.T.I. Hugo Zavala Vaca Un día hábil
Perfiles de personal		
Identificador único*	**Secretaría Técnica**	
(Nombre del sistema A3)*	WEBP01	
Proceso*	**Descripción***	**Responsable***
Respaldo de información	Se realiza el proceso de respaldo completo del servidor y sus aplicaciones.	Encargado de telecomunicaciones. M.T.I. Hugo Zavala Vaca Un día hábil

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

*(Llenar una tabla para cada sistema. Campos con * son obligatorios. Borrar instrucciones en cursivas)*

Secretaría Académica		
Identificador único*	**Secretaría Académica**	
(Nombre del sistema A1)*	*SIA01*	
Proceso*	**Descripción***	**Responsable***
Formateo lógico de discos duros.	Uso de herramientas de software libre para realizar el borrado seguro de disco duro.	Encargado de telecomunicaciones. M.T.I. Hugo Zavala Vaca Duración: cuatro días.
Sistema de Solicitudes Administrativas		
Identificador único*	**Delegación Administrativa**	
(Nombre del sistema A2)*	SSAD01	
Proceso*	**Descripción***	**Responsable***
Formateo lógico de discos duros.	Uso de herramientas de software libre para realizar el borrado seguro de disco duro.	Encargado de telecomunicaciones. M.T.I. Hugo Zavala Vaca Duración: cuatro días.
Perfiles de personal		
Identificador único*	**Secretaría Técnica**	
(Nombre del sistema A3)*	WEBP01	
Proceso*	**Descripción***	**Responsable***
Formateo lógico de discos duros.	Uso de herramientas de software libre para realizar el borrado seguro de disco duro.	Encargado de telecomunicaciones. M.T.I. Hugo Zavala Vaca Duración: cuatro días.

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

(Informar y describir el procedimiento para la cancelación de un sistema de tratamiento de datos personales.)[14]

[14] La cancelación da lugar al bloqueo de los datos, esto es, el periodo en el que la autoridad conservará los datos para efectos de responsabilidades, el cual será equivalente al plazo de prescripción de las acciones derivadas de la relación jurídica que funda el tratamiento en términos de la normatividad de aplicable y, cumplido este plazo, deberá procederse a la supresión del dato que implica el borrado físico del mismo.
Bajo este contexto, la cancelación no supone automáticamente la supresión o borrado físico de los datos, sino que se debe determinar un período o fase previa de bloqueo de los datos, en el cual no se podrá disponer de tales datos en la misma medida en que la podría hacerse por el área universitaria de estar en operación el Sistema de tratamiento de datos personales.
La cancelación de sistema de tratamiento de datos personales debe considerar lo establecido en los Lineamientos Generales para la Organización, Administración y Conservación de los Archivos de la Universidad Nacional Autónoma de México, así como el Catálogo de disposición documental de la Universidad del año respectivo, a fin de atender al valor documental de la información contenida en el mismo.

A) DATOS DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES QUE SERÁ CANCELADO:

a) Denominación
b) Motivo de la cancelación

B) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:[15]

(Señalar el periodo de bloqueo, considerando los plazos de prescripción para el ejercicio de algún derecho por parte de los titulares de conformidad con la normatividad de cada área universitaria. Asimismo, se debe señalar las condiciones y el procedimiento que se seguirá para realizar el bloqueo)

A solicitud del área responsable se considera el periodo de bloqueo del sistema, aplicando técnicas informáticas para resguardar el acceso al mismo mediante IP o nombre de dominio.

C) MEDIDAS DE SEGURIDAD PARA EL BLOQUEO Y POSTERIOR SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:
(Describir las medidas de seguridad aplicables al periodo de bloqueo y la supresión del sistema, considerando el nivel de protección requerido en virtud del tipo de datos personales contenidos en el sistema)

Se considera el acceso permitido al personal autorizado por el área para fines estadísticos.

D) PROCEDIMIENTO PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

(Describir el procedimiento para suprimir el sistema, una vez cumplido el plazo de bloqueo)

Una vez concluido el periodo de bloqueo se procede a eliminar la información del servidor o máquina virtual con la información del servidor.

E) MECANISMOS PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

(Describir las técnicas para la eliminación física del sistema)

El Departamento de Cómputo y Telecomunicaciones realiza la implementación de técnicas de borrado seguro del sistema.

[15] Es el periodo por el que se conservará para efectos de responsabilidades, tomando en cuenta el plazo de su prescripción conforme la normatividad aplicable.

11. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

		Nombre y firma de quienes revisaron el presente documento:
Responsable del desarrollo:	M.T.I. Hugo Alejandro Zavala Vaca Encargado de la Unidad de Cómputo y Telecomunicaciones. hzavala@ciga.unam.mx Tel. 55 5623 7370 Ext. 37370	
	M.C. Fabiola Araceli Velázquez Ayala Responsable de Seguridad de Datos personales fvelaz@ciga.unam.mx Tel. 55 5623 7370 Ext. 37370	
Revisó:	Dr. Luis Miguel Morales Manilla Secretario Técnico moraman@ciga.unam.mx Tel. 55 5623 7370 Ext. 37370	
Autorizó:	Dr. José Antonio Vieyra Medrano Director avieyra@ciga.unam.mx Tel. 55 5623 7370 Ext. 37370	
Fecha de aprobación:	16 de agosto de 2022	
Fecha de actualización:	Versión 1.0: 16 agosto de 2022	