SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES.
DIRECCIÓN DE LITERATURA Y FOMENTO A LA LECTURA

PRESENTACIÓN.

El artículo 34 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), establece que las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales deberán estar documentadas y contenidas en un *sistema de gestión*.

Por sistema de gestión debemos entender el conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, de conformidad con lo previsto en dicha legislación y las disposiciones que resulten aplicables en la materia.

En este mismo sentido, el artículo 65 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público[1] (LGPDPSP), estipula que el sistema de gestión deberá permitir planificar, establecer, implementar, operar, monitorear, mantener, revisar y mejorar las medidas de seguridad de carácter administrativo, físico y técnico aplicadas a los datos personales; tomando en consideración los estándares nacionales e internacionales en materia de protección de datos personales y seguridad.

Es así que dando cumplimiento a lo establecido en el capítulo II de la LGPDPPSO, donde se 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, 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, se busca la creación del presente Sistema de Seguridad de Gestión de Datos Personales (SGSDP), así como del Documento Seguridad respectivo.

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 encuentra 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”.

El presente documento de seguridad tiene como finalidad señalar las medidas de seguridad administrativas, físicas y técnicas aplicables a los sistemas de tratamiento de datos personales de la Dirección de Literatura y Fomento a la Lectura (DLFL); así como identificar los sistemas de datos personales que posee, el tipo de datos que contiene cada uno, los responsables, encargados, usuarios de cada sistema y las medidas de seguridad implementadas.

---

[1] Publicados en el Diario Oficial de la Federación el 26 de enero de 2018, consultables a través de la liga: http://www.dof.gob.mx/nota_detalle.php?codigo=5511540&fecha=26/01/2018#gsc.tab=0

La DLFL se encarga de fomentar la lectura y la cultura escrita a través de convocatorias, eventos, programas, congresos, encuentros y actividades públicas de corto y largo alcance, así como de diversos proyectos de difusión en medios de comunicación y plataformas electrónicas, entre la comunidad universitaria y el público en general, para contribuir a la difusión de la cultura en México. Su misión es conseguir ser un punto de referencia para el intercambio literario entre autores y lectore a través del fomento a la lectura y la cultura escrita, con perspectiva de género, incluyente y de derechos humanos que permee en los universitarios e impacte en la sociedad. La Dirección de literatura está conformada por el sistema de Universo de Letras que trabaja en programas de mediadores de lectura y en ofrecer cursos y talleres para la formación de lectores de todas las edades, las cátedras Carlos Fuentes y José Emilio Pacheco, la publicación impresa bimestral Punto de partida, así como las publicaciones digitales Periódico de poesía y Punto en línea la Escuela de Escritura que ofrece diplomados y talleres de escritura.

ABREVIATURAS Y DENOMINACIONES

CCU – Centro Cultural Universitario

DLFL – Dirección de Literatura y Fomento a la Lectura

EDPAC – Estímulos al Desempeño del Personal Administrativo y de Confianza

INAI – Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

LGPDPPSO o Ley General – Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados

LGPDPSP o Lineamientos Generales – Lineamientos Generales de Protección de Datos Personales para el Sector Público

LPDPPUNAM – Lineamientos para la protección de datos personales en posesión de la Universidad Nacional Autónoma de México

MP – Ministerio Público

SGSDP – Sistema de Gestión de Seguridad de Datos Personales

SIC – Sistema Institucional de Compras

SICD – Sistema de Inscripción a cursos, talleres y diplomados

SPH – Sistema de Pago por honorarios

UNAM – Universidad Nacional Autónoma de México

UPA – Unidad de Proceso Administrativo

ALCANCES Y OBJETIVOS

Los objetivos del presente SGSDP son los siguientes:

1. Establecer las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales en la DLFL.

2. Definir el conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales en la DLFL.

   Para esto se puntualizarán las políticas generales y específicas que deberán regir en el tratamiento de los datos personales.

   Asimismo, en el presente documento se desarrollarán los siguientes aspectos:
   - Las atribuciones y obligaciones relacionadas con la protección de los datos personales.
   - Las actuaciones que deben ser consideradas al realizar una transferencia de los datos personales.
   - Las actuaciones que deben ser consideradas al realizar una remisión de los datos personales.
   - Las actuaciones que deben ser consideradas al utilizar el cómputo en la nube.
   - Lo relacionado con la capacitación en materia de protección de datos personales.
   - Acciones para la mejora continua
   - Sanciones aplicables.

ROLES Y RESPONSABILIDADES DE LOS INVOLUCRADOS EN EL TRATAMIENTO DE DATOS PERSONALES

Se busca definir los roles, responsabilidades, cadena de rendición de cuentas y estructura organizacional, para así poder asegurar que todo aquel que trate datos personales tenga claros sus roles y funciones, así como su contribución para el logro de los objetivos del SGSDP y las consecuencias de su incumplimiento.

Quienes participan en el tratamiento de datos personales son:

SPH – Sistema de Pago por honorarios

SIC – Sistema Institucional de Compras

SDP- Sistema de difusión y promoción

SICD – Sistema de Inscripción a convocatorias, cursos, talleres y diplomados

SISTEMA DE PAGO POR HONORARIOS

- Jefatura de la Unidad Administrativa
- Jefatura del Departamento de Presupuesto y Personal

SISTEMA INTEGRAL DE COMPRAS

- Jefatura de la Unidad Administrativa
- Jefatura del Departamento de Bienes y Suministros y Servicios Generales
- Jefatura del Departamento de Presupuesto y Personal
- Jefatura del Área de Vinculación
- Jefatura del Área de Publicaciones
- Subdirección de Literatura y Fomento a la lectura
- Jefatura de Difusión y Comunicación
- Jefatura del Área de Proyectos y Ediciones Digitales
- Coordinación de Cátedras Extraordinarias en Fomento a la lectura Carlos Fuentes y José emilio Pacheco

SISTEMA DE INSCRIPCIÓN A CONVOCATORIAS, CURSOS, TALLERES Y DIPLOMADOS

- Subdirección de Literatura y Fomento a la lectura
- Coordinación de Cátedras Extraordinarias en Fomento a la lectura Carlos Fuentes y José Emilio Pacheco
- Jefatura de Publicaciones

Las funciones y responsabilidades en general de los integrantes del SGSDP son las siguientes:

Director. Supervisar que el SGSDP se cumpla de acuerdo al documento de seguridad.

Responsables. Verificar que el SGSDP se cumpla en sus áreas específicas de acuerdo al documento de seguridad.

Encargados. Mantener el SGSDP en sus áreas específicas de acuerdo al documento de seguridad.

Usuarios. Utilizar el SGSDP en sus áreas específicas de acuerdo al documento de seguridad.

Anexo 1. Inventario de sistemas de tratamiento de datos personales

Anexo 2. Estructura y descripción de los sistemas de datos personales

Anexo 3. Funciones y obligaciones de quienes traten datos personales

ANÁLISIS DE RIESGO DE LOS DATOS PERSONALES

Se determinan las características del riesgo que mayor impacto puden tener sobre los datos personales que se tratan, con el fin de priorizar y tomar la mejor decisión respecto a los controles de seguridad más relevantes e inmediatos a implementar. Entendiendo como riesgo a una situación en la que una persona podría hacer algo no deseado o una ocurrencia natural que puede causar un resultado indeseable, lo que resultaría en un impacto o consecuencia negativa. Un riesgo se compone de un evento, una consecuencia y una incertidumbre.[2]

Para esto se definen los posibles daños y perjuicios que pudieran causarle al titular de los datos personales en caso de un evento que atente contra estos, considerando:

- El valor de los datos para la DLFL.
- El incumplimiento de las obligaciones legales y contractuales relacionadas con el titular.
- Vulneraciones de seguridad. La presencia de éstas no causan un daño por sí mismas, se requiere de una amenaza que las explote.
- Daño a la integridad de los titulares de datos personales.
- Daño a la reputación de la DLFL.

Lo anterior se realiza tomando como base el OCTAVE Allegro Method[3], como se indica a continuación:

1. Se establecieron y priorizaron áreas de impacto que se utilizarán para evaluar el efecto de un riesgo en los diversos sistemas. Para lo anterior se asignó la puntuación más alta a la categoría más importante y la más baja a la menos importante.

Priorización del área de impacto	
Prioridad	Área de Impacto
4	Reputación / Pérdida de confianza
6	Financiera
5	Productividad
1	Seguridad y salud
3	Multas y sanciones
7	Interrupción del servicio
2	Incumplimiento de obligaciones legales

2. Se medirá cualitativamente el grado en que la Dirección de Literatura y Fomento a la Lectura se ve afectada por una amenaza calculando una puntuación de riesgo relativo para cada uno de ellos, asignando para esto los siguientes valores de impacto:

Valores de impacto	
Alto	3
Medio	2
Bajo	1

El puntaje total que se obtendrá, es un valor cuantitativo que puede ir de 0 a 84, el cual es directamente proporcional al impacto sobre los activos. El intervalo del valor cuantitativo se obtiene mulplicando

---

[2] Caralli, Richard A. *et al.* "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process", Software Engineering Intitute, Mayo 2007, *https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf* ,p. 53

[3] *op. cit.*

la prioridad por 3 que corresponde al valor de impacto “alto”, posteriormente se suma el puntaje, obteniendo un puntaje total máximo y se divide esto entre 3 para poder tener tres grupos en que clasificarlos:

X

Área de Impacto	Prioridad	Valor de impacto	Puntaje
Reputación / Pérdida de confianza	4	Alto 3	12
Financiera	6	Alto 3	18
Productividad	5	Alto 3	15
Seguridad y salud	1	Alto 3	3
Multas y sanciones	3	Alto 3	9
Interrupción del servicio	7	Alto 3	21
Incumplimiento de obligaciones legales	2	Alto 3	6
	Puntaje total máximo		84

+

84/3 = 28

3. Para calcular la puntuación de riesgo relativo de cada área de impacto se multiplicará la prioridad del área de impacto por el valor de impacto, registrando el resultado en la columna “puntaje”. Se sumará la columna de puntaje, el resultado obtenido indica el riesgo relativo

X

Área de Impacto	Prioridad	Valor de impacto	Puntaje
Reputación / Pérdida de confianza	4	3	12
Financiera	6	2	12
Productividad	5	3	15
Seguridad y salud	1	1	1
Multas y sanciones	3	2	6
Interrupción del servicio	7	3	21
Incumplimiento de obligaciones legales	2	3	6
		Puntaje total	73

+

4. El puntaje de cada área de impacto se utilizará para definir el tratamiento a realizar una vez identificados los riesgos y su prioridad, el cual puede ser:
   i) **Aceptar:** no tomar acción alguna sobre el riesgo y aceptar las consecuencias establecidas. Los riesgos que se acepten deben tener poco o bajo impacto.
   ii) **Mitigar:** desarrollar e implementar controles para contrarrestar la amenaza y/o minimizar el impacto. Los riesgos que se mitigan normalmente tienen un impacto medio a alto.
   iii) **Aplazar:** una situación en la que un riesgo no se acepta ni mitiga en función del deseo de recopilar información adicional y realizar análisis adicionales. Los riesgos aplazados se monitorean y reevaluán en algún momento futuro, generalmente estos no son una amenaza inminente ni afectan siginificativamente
   iv) **Transferir:** acciones que dirigen el riesgo a un tercero. Suele ocurrir cuando no se tiene un control total sobre la situación.

5. Se ordena cada uno de los riesgos que se han identificado por su puntaje de riesgo de mayor a menor. A continuación se separarán los riesgos en cuatro grupos, los cuales se identificarán en el intervalo correspondiente según el puntaje total obtenido.

Matríz de riesgo relativo			
Prioridad	Puntuación de riesgo		
	57 – 84	29 – 56	0 – 28
Alta	Grupo 1: Mitigar	Grupo 2: Mitigar o Aplazar	Grupo 2: Mitigar o Aplazar
Media	Grupo 2: Mitigar o Aplazar	Grupo 2: Mitigar o Aplazar	Grupo 3: Aplazar o Aceptar
Baja	Grupo 3: Aplazar o Aceptar	Grupo 3: Aplazar o Aceptar	Grupo 4: Aceptar

6. Identificado cómo se tratará el riesgo, se plantearán acciones para mitigar, aplazar, transferir o aceptar el riesgo, considerando los controles de seguridad física, administrativa y técnica para la protección de datos personales.
7. Registrar el riesgo identificado en el SGSDP-

Anexo 4. Análisis de riesgos

ANÁLISIS DE BRECHA Y MEDIDAS DE SEGURIDAD

Una vez identificados los activos y procesos, se procede a realizar el análisis de brecha, consistente en identificar:

- Las medidas de seguridad existentes que operan correctamente;
- Las medidas de seguridad faltantes; y
- Las medidas de seguridad nuevas que puedan remplazar a las existentes

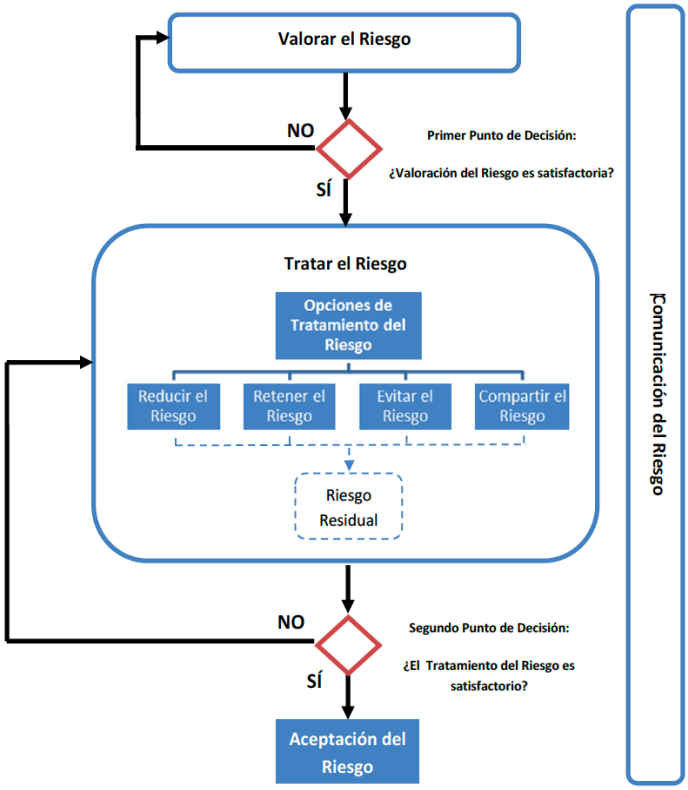
Se seleccionaron las medidas de seguridad administrativas, técnicas o físicas que permiten atender de mejor manera los riesgos identificados y minimizar las consecuencias de posibles vulneraciones. En particular se tomaron en cuenta los siguientes criterios para elegir las medidas de seguridad efectivas:

1. Proteger los datos personales contra daño, pérdida, destrucción o alteración.
2. Evitar el uso, acceso o tratamiento no autorizado.
3. Impedir la divulgación no autorizada de los datos personales.

Anexo 5. Análisis de brecha y Medidas de Seguridad

PLAN DE TRABAJO

La DLFL seleccionó los controles de seguridad faltantes o necesarios de reforzar identificados del análisis de riesgos y análisis de brecha realizados, tomando en cuenta la ponderación hecha en la valoración propuesta por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), además se han considerado los recursos asignados, el personal con el que se cuenta y los tiempos establecidos para la implementación de los controles de seguridad nuevos o a reforzar.



Además, se indica el grado de cobertura de cada control de seguridad con base en las opciones de tratamiento del riesgo, de la siguiente manera:

- **Aceptar:** no tomar acción alguna sobre el riesgo y aceptar las consecuencias establecidas. Los riesgos que se acepten deben tener poco o bajo impacto.
- **Mitigar:** desarrollar e implementar controles para contrarrestar la amenaza y/o minimizar el impacto. Los riesgos que se mitigan normalmente tienen un impacto medio a alto .
- **Aplazar:** una situación en la que un riesgo no se acepta ni mitiga en función del deseo de recopilar información adicional y realizar análisis adicionales. Los riesgos aplazados se monitorean y reevaluán en algún momento futuro, generalmente estos no son una amenaza inminente ni afectan siginificativamente
- **Transferir:** acciones que dirigen el riesgo a un tercero. Suele ocurrir cuando no se tiene un control total sobre la situación.

Anexo 6. Plan de trabajo

MEJORA CONTINUA Y CAPACITACIÓN

Mejora Continua.

El monitoreo de los factores de riesgo así como del Sistema de Gestión de Seguridad de Datos Personales, permitirán que éste pueda ser mejorado. Los puntos de mejora del SGSDP puden corresponder a dos tipos:

a) **Acciones correctivas:** encaminadas a eliminar las causas de fallas o incidentes ocurridos en el SGSDP, con el objeto de prevenir que vuelvan a ocurrir, dichas acciones deben ser proporcionales a la gravedad del incidente. Deben atenderse considerando:
   i. El análisis y revisión de la falla o incidente;
   ii. Determinar las causas que dieron origen a la falla o incidente;
   iii. Evaluar las acciones necesarias para evitar que la falla o incidente vuelva a ocurrir;
   iv. Determinar e implementar las acciones necesarias;
   v. Registrar los resultados de las acciones tomadas;
   vi. Revisar la eficacia de las acciones correctivas tomadas.

b) **Acciones preventivas:** acciones encaminadas a eliminar las causas de fallas o incidentes posibles en el SGSDP, dichas acciones deben ser proporcionales a las amenzas potenciales. Deben atenderse considerando:
   i. El análisis y revisión de la amenaza;
   ii. Determinar las fallas o incidentes que podría desencadenarse con una amenza;
   iii. Evaluar las acciones necesarias para evitar que la falla o incidente ocurra;
   iv. Determinar e implementar las acciones necesarias;
   v. Registrar los resultados de las acciones tomadas;
   vi. Revisar la eficacia de las acciones preventivas tomadas.

La implementación de las acciones antes mencionadas pueden establecerse en un periodo inmediato a la detección y análisis del punto de mejora o calendarizarse para una futura revisión del SGSDP en función de la importancia de la mejora de los recursos disponibles. Su eficacia se evaluará considerando la reducción de los niveles de riesgo en los resultados del monitorio del SGSDP.

Capacitación.

La mejor medida de seguridad contra posibles vulneraciones es contar con personal consciente de sus responsabilidades y deberes respecto a la protección de datos personales y que identifiquen cuál es su contribución para el logro de los objetivos del SGSDP.

Para lo anterior se estarán establenciendo:

1. Platicas informativas para la difusión en general de la protección de datos personales.
2. Capacitación al personal de manera específica respecto a sus funciones y responsabilidades en el tratamiento y seguridad de los datos personales.
3. Infografía mediante correo electrónico para generar una cultura sobre la seguridad en el tratamiento de los datos personales.

Tomando en cuenta elementos como:

a) Los requerimientos y actualizaciones al contexto del SGSDP;
b) La legislación vigente en materia de protección de datos personales y mejores prácticas relacionadas al tratamiento de datos personales;

c) Las consecuencias del incumplimiento de los requerimientos legales o requisitos organizacionales;
d) Las herramientas tecnológicas relacionadas o utilizadas para el tratamiento de datos personales y para la implementación de medidas de seguridad.

Anexo 7. Capacitación Administrativa Básica

RUTA CRÍTICA PARA EL CUMPLIMIENTO DE LAS MEDIDAS DE SEGURIDAD TÉCNICAS (MST)

Dada la complejidad de diversos sistemas en la UNAM, se ha dispuesto la ruta crítica para el cumplimiento de las MST en tres etapas para los sistemas de información que a la fecha de publicación de este SGSDP estén en producción o funcionamiento. Todo sistema de información deberá satisfacer a cabalidad el 100% de las MST en un tiempo máximo de un año contado a partir de la publicación de las MST para conservar su registro y publicación dentro del dominio institucional ***.unam.mx.***

a) Etapa 1. Corto plazo. Requisitos de misión crítica y mínimos indispensables para la protección de datos personales y datos personales sensibles. Cumplimiento obligatorio en menos de treinta días hábiles.
b) Etapa 2. Mediano plazo. Requisitos importantes para garantizar la protección de datos personales y datos personales sensibles. Ejecuciónestimada entre un mes y seis meses.
c) Etapa 3. Largo plazo. Requisitos necesarios para reforzar la seguridad en la protección de datos personales y datos personales sensibles. Ejecución estimada entre seis y doce meses.

Anexo 8. Formatos para el cumplimiento de las MST (Etapa 1)

APROBACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES

		Nombre y firma de quienes revisaron el presente documento:
Responsable del desarrollo:	Gabriela Rasso Figueroa Jefa de difusión y comunicación Tel- 5622-6241 literatura.difusion@gmail.com	 Gabriela Rasso Figueroa
Revisó:	Julieta García Subdirectora de Literatura y Fomento a la Lectura Tel. 5622-6245 subdireccion.literatura@gmail.com	 Julieta García M
Autorizó:	Ana Elsa Pérez Martínez Directora de Literatura y Fomento a la Lectura Tel. 5665-0419 anaelsaperez@gmail.com	 Ana Elsa Pérez Martínez
Fecha de aprobación:	12 de agosto de 2022	
Fecha de actualización:	12 de agosto de 2022	

ANEXO 1.

INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Dirección de Literatura y fomento a la Lectura			
Abreviatura del nombre del sistema	**DLFL/SIC**		
Nombre del sistema	Sistema Integral de Compras		
Datos personales contenidos en el sistema:	- Nombre completo - Correo electrónico - Número de teléfono particular - Constancia de situación fiscal del SAT (últimos 2 meses) - CURP - Carátula del estado de cuenta bancaria (últimos 2 meses)		
Responsable del sistema			
Nombre:	Lic. Silvestre Bernardo Zamacona Esquivel		
Cargo:	Jefe de la Unidad Administrativa		
Funciones:	Obtención (|X) Uso (X) Registro (X) Organización ( ) Elaboración ( ) Conservación (X)	Utilización (X) Comunicación (X) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento ( ) Divulgación ( ) Transferencia ( ) Remisión (X) Disposición (X)
Obligaciones:	- Guardar la confidencialidad de los datos personales. - Proteger los datos personales recibidos. - No modificar la información de datos personales contenidos en los documentos recibidos. - No difundir la información de datos personales contenidos en los documentos recibidos. - Mantener la información de datos personales en el archivo de la Unidad Administrativa. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Encargados del sistema			
Nombre encargado 1:	Genaro Gutiérrez Soto		
Cargo:	Jefe del Departamento de Bienes y Suministros y Servicios Generales		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización ( ) Elaboración ( ) Conservación (X)	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento ( ) Divulgación ( ) Transferencia ( ) Remisión (X) Disposición (X)
Obligaciones:	- Guardar la confidencialidad de los datos personales. - Proteger los datos personales recibidos. - No modificar la información de datos personales contenidos en los documentos recibidos. - No difundir la información de datos personales contenidos en los documentos recibidos. - Mantener la información de datos personales en el archivo de la Unidad Administrativa. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre encargado 2:	Brenda María Saldaña Hernández		
Cargo:	Jefa del Departamento de Presupuesto y Personal		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación (X)	Utilización (X) Comunicación (X) Difusión ( ) Almacenamiento (X) Posesión (X) Acceso (X)	Manejo (X) Aprovechamiento ( ) Divulgación ( ) Transferencia (X) Remisión (X) Disposición (X)
Obligaciones:	- Guardar la confidencialidad de los datos personales. - Proteger los datos personales recibidos. - No modificar la información de datos personales contenidos en los documentos recibidos.		

	- No difundir la información de datos personales contenidos en los documentos recibidos. - Mantener la información de datos personales en el archivo de la Unidad Administrativa. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Usuarios			
Nombre usuario 1:	María Imelda Martorell Nieto		
Cargo:	Funcionario		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración (X) Conservación (X)	Utilización (X) Comunicación (X) Difusión ( ) Almacenamiento (X) Posesión (X) Acceso (X)	Manejo (X) Aprovechamiento ( ) Divulgación ( ) Transferencia (X) Remisión (X) Disposición (X)
Obligaciones:	- Guardar la confidencialidad de los datos personales. - Proteger los datos personales recibidos. - No modificar la información de datos personales contenidos en los documentos recibidos. - No difundir la información de datos personales contenidos en los documentos recibidos. - Mantener la información de datos personales en el archivo de la Unidad Administrativa. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre usuario 2:	María Guadalupe Llamas Uribe		
Cargo:	Personal de Honorarios		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración (X) Conservación (X)	Utilización (X) Comunicación (X) Difusión ( ) Almacenamiento (X) Posesión (X) Acceso (X)	Manejo (X) Aprovechamiento ( ) Divulgación ( ) Transferencia (X) Remisión (X) Disposición (X)
Obligaciones:	- Guardar la confidencialidad de los datos personales. - Proteger los datos personales recibidos. - No modificar la información de datos personales contenidos en los documentos recibidos. - No difundir la información de datos personales contenidos en los documentos recibidos. - Mantener la información de datos personales en el archivo de la Unidad Administrativa. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados..		
Nombre usuario 3:	Carmina Vicenta Estrada Castillo		
Cargo:	Funcionario		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración (X) Conservación (X)	Utilización (X) Comunicación (X) Difusión ( ) Almacenamiento (X) Posesión (X) Acceso (X)	Manejo (X) Aprovechamiento ( ) Divulgación ( ) Transferencia (X) Remisión (X) Disposición (X)
Obligaciones:	- Guardar la confidencialidad de los datos personales. - Proteger los datos personales recibidos. - No modificar la información de datos personales contenidos en los documentos recibidos. - No difundir la información de datos personales contenidos en los documentos recibidos. - Mantener la información de datos personales en el archivo de la Unidad Administrativa. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre usuario 4:	Carolina Domínguez Hidalgo		
Cargo:	Funcionaria		
Funciones:	Obtención (X) Uso (X) Registro (X)	Utilización (X) Comunicación (X) Difusión ( )	Manejo (X) Aprovechamiento ( ) Divulgación ( )

	Organización (X) Elaboración ( ) Conservación ( )	Almacenamiento ( ) Posesión (X) Acceso (X)	Transferencia ( ) Remisión (X) Disposición (X)
Obligaciones:	- Guardar la confidencialidad de los datos personales. - Proteger los datos personales recibidos. - No modificar la información de datos personales contenidos en los documentos recibidos. - No difundir la información de datos personales contenidos en los documentos recibidos. - Mantener la información de datos personales en el archivo de la Unidad Administrativa. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados..		
Nombre usuario 5:	Julieta García González		
Cargo:	Funcionaria		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración (X) Conservación (X)	Utilización (X) Comunicación (X) Difusión ( ) Almacenamiento (X) Posesión (X) Acceso (X)	Manejo (X) Aprovechamiento ( ) Divulgación ( ) Transferencia (X) Remisión ( ) Disposición ( )
Obligaciones:	- Guardar la confidencialidad de los datos personales. - Proteger los datos personales recibidos. - No modificar la información de datos personales contenidos en los documentos recibidos. - No difundir la información de datos personales contenidos en los documentos recibidos. - Mantener la información de datos personales en el archivo de la Unidad Administrativa. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre usuario 6:	Gabriela Rasso Figueroa		
Cargo:	Funcionaria		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración (X) Conservación (X)	Utilización (X) Comunicación (X) Difusión ( ) Almacenamiento (X) Posesión (X) Acceso (X)	Manejo (X) Aprovechamiento ( ) Divulgación ( ) Transferencia (X) Remisión ( ) Disposición ( )
Obligaciones:	- Guardar la confidencialidad de los datos personales. - Proteger los datos personales recibidos. - No modificar la información de datos personales contenidos en los documentos recibidos. - No difundir la información de datos personales contenidos en los documentos recibidos. - Mantener la información de datos personales en el archivo de la Unidad Administrativa. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados..		
Nombre usuario 7:	Silvia Elisa Aguilar Funes		
Cargo:	Jefe de Area		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración (X) Conservación (X)	Utilización (X) Comunicación (X) Difusión (X) Almacenamiento (X) Posesión (X) Acceso (X)	Manejo (X) Aprovechamiento (X) Divulgación (X) Transferencia (X) Remisión (X) Disposición (X)
Obligaciones:	- Guardar la confidencialidad de los datos personales. - Proteger los datos personales recibidos. - No modificar la información de datos personales contenidos en los documentos recibidos. - No difundir la información de datos personales contenidos en los documentos recibidos. - Mantener la información de datos personales en el archivo de la Unidad Administrativa. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		

Dirección de Literatura y fomento a la Lectura			
Abreviatura del nombre del sistema	**DLFL/SPH**		
Nombre del sistema	**Sistema de Pagos de Honorarios**		
Datos personales contenidos en el sistema:	- Nombre completo - Correo electrónico - Número de teléfono particular - Constancia de situación fiscal del SAT (últimos 2 meses) - CURP - Carátula del estado de cuenta bancaria (últimos 2 meses) - Identificación oficial (INE o Pasaporte) - Comprobante de Estudios o cédula profesional - Comprobante de Domicilio (últimos 2 meses) - Recibo de honorarios en PDF y XML -Carta de naturalización (extranjeros naturalizados) - Permiso migratorio (extranjeros)		
Responsable del sistema			
Nombre:	Lic. Silvestre Bernardo Zamacona Esquivel		
Cargo:	Jefe de la Unidad Administrativa		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización ( ) Elaboración ( ) Conservación (x)	Utilización ( ) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo ( ) Aprovechamiento (X) Divulgación ( ) Transferencia ( ) Remisión (X) Disposición ( )
Obligaciones:	- Guardar la confidencialidad de los datos personales. - Proteger los datos personales recibidos. - No modificar la información de datos personales contenidos en los documentos recibidos. - No difundir la información de datos personales contenidos en los documentos recibidos. - Mantener la información de datos personales en el archivo de la Unidad Administrativa. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Encargados del Sistema			
Nombre:	Brenda Saldaña Hernández		
Cargo:	Jefe de departamento de personal y presupuesto		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración (X) Conservación (X)	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento (X) Posesión (X) Acceso (X)	Manejo (X) Aprovechamiento (X) Divulgación ( ) Transferencia ( ) Remisión (X) Disposición ( )
Obligaciones:	- Guardar la confidencialidad de los datos personales. - Proteger los datos personales recibidos. - No modificar la información de datos personales contenidos en los documentos recibidos. - No difundir la información de datos personales contenidos en los documentos recibidos. - Mantener la información de datos personales en el archivo de la Unidad Administrativa. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Usuarios			
Nombre usuario 1:	Miriam Gudiño García		
Cargo:	Asistente de procesos		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X)	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento (X)	Manejo (X) Aprovechamiento ( ) Divulgación ( ) Transferencia ( )

	Elaboración (X) Conservación (X)	Posesión ( ) Acceso (X)	Remisión ( ) Disposición ( )
Obligaciones:	- Guardar la confidencialidad de los datos personales. - Proteger los datos personales recibidos. - No modificar la información de datos personales contenidos en los documentos recibidos. - No difundir la información de datos personales contenidos en los documentos recibidos. - Mantener la información de datos personales en el archivo de la Unidad Administrativa. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre usuario 2:	Atzimba González		
Cargo:	Secretaria de base		
Funciones:	Obtención ( ) Uso ( ) Registro ( ) Organización (X) Elaboración ( ) Conservación (X)	Utilización ( ) Comunicación ( ) Difusión ( ) Almacenamiento (X) Posesión ( ) Acceso ( )	Manejo ( ) Aprovechamiento ( ) Divulgación ( ) Transferencia ( ) Remisión ( ) Disposición ( )
Obligaciones:	- Guardar la confidencialidad de los datos personales. - Proteger los datos personales recibidos. - No modificar la información de datos personales contenidos en los documentos recibidos. - No difundir la información de datos personales contenidos en los documentos recibidos. - Mantener la información de datos personales en el archivo de la Unidad Administrativa. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre Usuario 3:	Genaro Gutiérrez Soto		
Cargo:	Jefe de Departamento de Bienes y Suministros y Servicios Generales		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación (X)	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento (X) Posesión (X) Acceso (X)	Manejo (X) Aprovechamiento ( ) Divulgación ( ) Transferencia ( ) Remisión (X) Disposición ( )
Obligaciones:	- Guardar la confidencialidad de los datos personales. - Proteger los datos personales recibidos. - No modificar la información de datos personales contenidos en los documentos recibidos. - No difundir la información de datos personales contenidos en los documentos recibidos. - Mantener la información de datos personales en el archivo de la Unidad Administrativa. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		

Dirección de Literatura y Fomento a la Lectura	
Abreviatura del nombre del sistema	**DLFL/SICD**
Nombre del sistema	**Sistema de Inscripción a Convocatorias, Cursos, Talleres y Diplomados**
Datos personales contenidos en el sistema:	- Nombre completo - Correo - Teléfono - Edad - Género - Escolaridad

Responsable del sistema			
Nombre:	Julieta García González		
Cargo:	Subdirectora de Liteatura y Fomento a la Lectrura		
Funciones:	Obtención ( ) Uso ( ) Registro ( )	Utilización ( ) Comunicación ( ) Difusión ( )	Manejo ( ) Aprovechamiento ( ) Divulgación ( )

	Organización ( ) Elaboración ( ) Conservación ( )	Almacenamiento ( ) Posesión ( ) Acceso ( )	Transferencia ( ) Remisión ( ) Disposición ( )
Obligaciones:	- Guardar la confidencialidad de los datos personales. - Proteger los datos personales recibidos. - No modificar la información de datos personales contenidos en los documentos recibidos. - No difundir la información de datos personales contenidos en los documentos recibidos. - Mantener la información de datos personales en el archivo de la Unidad Administrativa. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Encargados del sistema			
Nombre encargado 1:	Gloria Ávila Álvarez		
Cargo:	Enlace de vinculación Universo de Letras		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación (X)	Utilización (X) Comunicación ( ) Difusión (X) Almacenamiento (X) Posesión ( ) Acceso (X)	Manejo ( ) Aprovechamiento ( ) Divulgación ( ) Transferencia ( ) Remisión ( ) Disposición ( )
Obligaciones:	- Guardar la confidencialidad de los datos personales. - Proteger los datos personales recibidos. - No modificar la información de datos personales contenidos en los documentos recibidos. - No difundir la información de datos personales contenidos en los documentos recibidos. - Mantener la información de datos personales en el archivo de la Unidad Administrativa. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre encargado 2:	Carmina Estrada Castillo		
Cargo:	Jefe de la Unidad de Revistas y Publicaciones		
Funciones:	Obtención ( ) Uso (X) Registro ( ) Organización (X) Elaboración ( ) Conservación ( )	Utilización ( ) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso ( )	Manejo ( ) Aprovechamiento ( ) Divulgación ( ) Transferencia ( ) Remisión ( ) Disposición ( )
Obligaciones:	- Guardar la confidencialidad de los datos personales. - Proteger los datos personales recibidos. - No modificar la información de datos personales contenidos en los documentos recibidos. - No difundir la información de datos personales contenidos en los documentos recibidos. - Mantener la información de datos personales en el archivo de la Unidad Administrativa. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre encargado 3:	Eduardo Cerdán		
Cargo:	Escuela de Escritura		
Funciones:	Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación (X)	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento (X) Posesión ( ) Acceso ( )	Manejo (X) Aprovechamiento ( ) Divulgación ( ) Transferencia ( ) Remisión ( ) Disposición ( )
Obligacione:	- Guardar la confidencialidad de los datos personales. - Proteger los datos personales recibidos. - No modificar la información de datos personales contenidos en los documentos recibidos. - No difundir la información de datos personales contenidos en los documentos recibidos. - Mantener la información de datos personales en el archivo de la Unidad Administrativa. - No generar copias de los documentos en los equipos de trabajo.		

	Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre encargado 4:	Julia Antivillo		
Cargo:	Coordinadora Cátedra Extraordinaria Carlos Fuente		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación (X)	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento (X) Posesión ( ) Acceso ( )	Manejo (X) Aprovechamiento ( ) Divulgación ( ) Transferencia ( ) Remisión ( ) Disposición ( )
Obligaciones:	- Guardar la confidencialidad de los datos personales. - Proteger los datos personales recibidos. - No modificar la información de datos personales contenidos en los documentos recibidos. - No difundir la información de datos personales contenidos en los documentos recibidos. - Mantener la información de datos personales en el archivo de la Unidad Administrativa. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Usuarios			
Nombre usuario 1:	Aranzazú Blazquez Menes		
Cargo:	Editora Revista Punto de partida		
Funciones:	Obtención (X) Uso (X) Registro ( ) Organización (X) Elaboración ( ) Conservación (X)	Utilización ( ) Comunicación ( ) Difusión ( ) Almacenamiento (X) Posesión ( ) Acceso (X)	Manejo ( ) Aprovechamiento ( ) Divulgación ( ) Transferencia ( ) Remisión ( ) Disposición ( )
Obligaciones:	- Guardar la confidencialidad de los datos personales. - Proteger los datos personales recibidos. - No modificar la información de datos personales contenidos en los documentos recibidos. - No difundir la información de datos personales contenidos en los documentos recibidos. - Mantener la información de datos personales en el archivo de la Unidad Administrativa. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre usuario 2:	Karla Elisa Morales Vargas		
Cargo:	Productora de Programación Cátredra Extraordinaria Carlos Fuentes		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación (X)	Utilización ( ) Comunicación ( ) Difusión ( ) Almacenamiento (X) Posesión (X) Acceso ( )	Manejo ( ) Aprovechamiento ( ) Divulgación ( ) Transferencia ( ) Remisión ( ) Disposición ( )
Obligaciones:	- Guardar la confidencialidad de los datos personales. - Proteger los datos personales recibidos. - No modificar la información de datos personales contenidos en los documentos recibidos. - No difundir la información de datos personales contenidos en los documentos recibidos. - Mantener la información de datos personales en el archivo de la Unidad Administrativa. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados..		

ANEXO 2.

ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE DATOS PERSONALES

Dirección de de Literatura y Fomento a la Lectura		
Abreviatura del nombre del sistema	**DLFL/SIC**	
Nombre del sistema	Sistema Integral de Compras	
¿Cómo se resguardan los datos personales?	Físico ( ) Digital (X). Ambos ( )	
	Tipo de soporte	Físico ( ) Digital (X) Ambos ( )
	¿Dónde se aloja?	Computadora (X) Servidor ( ) Nube ( ) Correo (X) Otros:
	Descripción de la información que se resguarda	- Archivo digital general con los documentos en formato pdf de los proveedores. Estos están resguardados por nombre junto a contrato en caso de haberse genrado.
	Características del lugar donde se resguarda la información	- Computadora ubicada en la oficina de cada usuario/responsable. - Correo electrónico de cada usuario/encargado
Dirección de Literatura y Fomento a la Lectura		
Abreviatura del nombre del sistema	**DLFL/SPH**	
Nombre del sistema	**Sistema de Pagos a Honorarios**	
¿Cómo se resguardan los datos personales	Físico ( ) Digital ( ). Ambos (X)	
	Tipo de soporte	Físico ( ) Digital ( ) Ambos (X)
	¿Dónde se aloja?	Computadora (X) Servidor ( ) Nube ( ) Correo (X) Otros: - Expediente físicos en archiveros.
	Descripción de la información que se resguarda	- Expedientes físicos en papel. - Carpetas en computadoras personales.
	Características del lugar donde se resguarda la información	- Archiveros tradicionales de madera y de metal, ubicados dentro de cada oficina con iluminación artificial y natural. - Computadoras ubicadas en las oficinas de cada usuario
Dirección de de Literatura y Fomento a la Lectura		
Abreviatura del nombre del sistema	**DLFL/SICD**	
Nombre del sistema	**Sistema de Inscripción a Convocatorias, Cursos, Talleres y Diplomados**	
¿Cómo se resguardan los datos personales?	Físico ( ) Digital (X). Ambos ( )	
	Tipo de soporte	Físico ( ) Digital (X) Ambos ( )

	¿Dónde se aloja?	Computadora (X) Servidor ( ) Nube (X) Correo (X) Otros:
	Descripción de la información que se resguarda	- Hojas de cálculo en Excel - Archivo digital en forma de lista donde se indican los nombres de las persons interesadas en asisitir al evento especial
	Características del lugar donde se resguarda la información	- Computadora ubicada en la oficina de cada usuario/responsable. - Nube.

ANEXO 3.

FUNCIONES Y OBLIGACIONES DE QUIENES TRATEN DATOS PERSONALES

Dirección de Literatura y fomento a la Lectura						
Abreviatura del nombre del sistema	**DLFL/SPH**					
Nombre del sistema	**Sistema de pago de honorarios**					
ACTIVIDADES	**D**	**SB**	**UA**	**JD**	**AP**	**PB**
Guardar información de los documentos recibidos en el sistema de gestión			X	X	X	
Notificar la obtención de los documentos para iniciar el trámite de pago			X	X	X	
Consultar la información de datos personales en el correo insitucional				X	X	
Dar seguimiento al trámite de pago				X	X	
Dar seguimiento a solicitudes de acceso a la información y ejercicio de derechos ARCO				X		
Consulta información de datos personales en los documentos recibidos en el sistema de gestión			X	X	X	
Guardar los documentos enviados por los titulares de los datos personales en el archivo físico y digital			X	X		X

Revisar los documentos entregados por los titulares de datos personales para detectar estos				X		
Hacer sugerencias al área universitaria para quitar, testar o clasificar la información de documentos entregados según sea el caso		X	X			
Registrar respuesta en la PNT				X		
Mantener equipos de trabajo libres de documentos con datos personales		X	X	X	X	X
Generar respaldos de sistemas			X	X	X	X
Proteger los datos personales contenidos en el sistema de accesos no autorizados			X	X	X	
Mantener actualizado el sistema de gestión				X		
Dictar políticas para el aseguramiento de los datos personales en la DLFL		X	X	X		
Dar capacitación en materia de protección de datos personales			X	X		
Proteger el archivo físico de la DGM de accesos no autorizados				X		X

D – Director
SB – Subdirector
JD – Jefes de departamento
UA- Unidad administrativa
AP- Asistente de procesos
PB – Personal de Base

Dirección de Literatura y fomento a la Lectura							
Abreviatura del nombre del sistema	**DLFL/SIC**						
Nombre del sistema	Sistema Integral de Compras						
ACTIVIDADES	**DL**	**SL**	**JD**	**CC**	**EV**	**UA**	**CA**
Guardar información de los documentos recibidos en el sistema de gestión			X	X	X	X	X
Notificar la obtención de los documentos para iniciar el trámite de pago						X	
Consultar la información de datos personales en el correo insitucional			X	X	X	X	X
Dar seguimiento al trámite de pago			X	X	X	X	
Dar seguimiento a solicitudes de acceso a la información y ejercicio de derechos ARCO		X	X				
Consulta información de datos personales en los documentos recibidos en el sistema de gestión			X	X	X	X	
Guardar los documentos enviados por los titulares de los datos personales en el archivo digital						X	
Revisar los documentos entregados por los titulares de datos personales para detectar estos			X				
Hacer sugerencias al área universitaria para quitar, testar o clasificar la información de documentos entregados según sea el caso		X				X	
Registrar respuesta en la PNT			X				
Mantener equipos de trabajo libres de documentos con datos personales			X	X	X	X	X
Generar respaldos de sistemas		X	X	X	X	X	X

Proteger los datos personales contenidos en el sistema de accesos no autorizados		X	X	X	X	X	X
Mantener actualizado el sistema de gestión			X			X	
Dictar políticas para el aseguramiento de los datos personales en la DLFL		X	X			X	
Dar capacitación en materia de protección de datos personales			X			X	

Dirección de Literatura y Fomento a la Lectura							
Abreviatura del nombre del sistema	**DLFL/SICD**						
Nombre del sistema	**Sistema de Inscripción a Convocatorias, Cursos, Talleres y Diplomados**						
ACTIVIDADES	**DL**	**SL**	**JD**	**CC**	**EV**	**UA**	**CA**
Guardar información de los documentos recibidos en el sistema de gestión			X		X		X
Consultar la información de datos personales en el correo insitucional			X	X	X		X
Dar seguimiento a solicitudes de acceso a la información y ejercicio de derechos ARCO			X				
Consulta información de datos personales en los documentos recibidos en el sistema de gestión					X		X
Guardar los documentos enviados por los titulares de los datos personales en el archivo físico y digital					X		X
Revisar los documentos entregados por los titulares de datos personales para detectar estos					X		X
Registrar respuesta en la PNT			X				
Mantener equipos de trabajo libres de documentos con datos personales			X	X	X		X
Generar respaldos de sistemas					X		X
Proteger los datos personales contenidos en el sistema de accesos no autorizados					X		X
Mantener actualizado el sistema de gestión			X		X		X
Dictar políticas para el aseguramiento de los datos personales en la DLFL		X	X				
Dar capacitación en materia de protección de datos personales			X				

DL – Director Literatura
SB – Subdirector Literatura
JD – Jefes de departamento
CC- Coordinadores de Cátedras
EV- Enlace de Vinculación
UA – Personal de la Unidad Administrativa
CA- Colaborador de área

Dirección de Literatura y Fomento a la Lectura							
FUNCIONES DENTRO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES							
ACTIVIDADES	D	SB	JD	CA	CC	UA	EV
Elaborar políticas y objetivos del SGSDP		X	X			X	
Aprobar políticas y objetivos del SGSDP	X						
Asignar funciones y obligaciones	X	X				X	
Elaborar inventario de datos personales	X	X	X	X	X	X	X
Realizar análisis de riesgos de los datos personales			X	X		X	X
Realizar análsis de brecha de las medidas de seguridad			X	X		X	X
Implementar las medidas de seguridad			X	X		X	X
Capacitación			X			X	
Revisiones y auditoría			X			X	

Dirección de Literatura y Fomento a la Lectura							
MATRÍZ DE RENDICIÓN DE CUENTAS							
AREAS	D	SB	JD	CA	CC	UA	EV
Coordinador Ejecutivo	X					X	
Subdirectores		X				X	
Jefes de Departamento		X	X			X	
Asistente Ejecutiva	X					X	
Personal de la Unidad Administrativa	X	X				X	
Jefe de Cómputo	X	X	X			X	

D – Director
SB – Subdireccion
JD – Jefatura de Deparpartamento
CA– Colaborador de área
UA – Unidad Administrativa
CC- Coordinadores de Cátedras
EV- Enlace de vinculación

ANEXO 7.

Capacitación Administrativa Básica

CAPACITACIÓN ADMINISTRATIVA BÁSICA	
DIRECCIÓN DE LITERATURA Y FOMENTO A LA LECTURA	
TEMA	**IMPARTE**
1. Introducción a la Protección de Datos Personales. - Conceptos y figuras claves en la LGPDPPSO. - Principios y deberes de la protección de datos personales. - Principios de protección de datos personales. - Deberes de seguridad y confidencialidad. - Obligaciones específicas: encargados, régimen de transferencias y evaluaciones de impacto. - Responsabilidades administrativas en caso de incumplimiento.	Unidad de Transparencia UNAM
2. Elaboración de Avisos de Privacidad Integral y Simplificado de las áreas administrativas.	
3. Derechos ARCOP, medios de impugnación y facultad de verificación. - Derechos de acceso, rectificación, cancelación, oposición y portabilidad. - Formas y plazos señalados por la LGPDPPSO para el ejercicio de estos derechos. - Recursos de revisión y de inconformidad. Etapas de sustanciación. - Facultades que el INAI tiene para verificar el incumplimiento de la LGPDPPSO. - Medidas cautelares y de apremio para cumplir resoluciones de la LGPDPPSO.	
4. Elaboración del Documento de Seguridad y Sistema de Gestión de Seguridad de Datos Personales.	

ANEXO 8.

Formatos para el cumplimiento de las MST (Etapa 1)

NO APLICA

Sistema de pagos			DLFL/SP	
Formato	**1**	**Verificación anual**	**Acción concluida**	( )
Medida de seguridad técnica:		**Artículo 18. I. c) Utilizar datos no personales durante el desarrollo y pruebas de los sistemas.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Un día hábil.		
Importancia de la acción:		Evitar usar datos personales mientras se está desarrollando, actualizando o modificando el código fuente de un sistema de información.		
Proceso recomendado:		**A)** Realizar respaldo completo de la base de datos. **B)** Ejecutar consulta en el sistema de información, por medio de formato o comandos. **C)** Verificar que los datos usados en el desarrollo no correspondan a personas identificables. **D)** Si se usan datos de personas identificables, cambiar por datos genéricos o datos ficticios y regresar al punto B. **E)** Si no se usan datos de personas identificables, llenar formato con nombre y firma de quien realizó la acción, fecha de inicio y de conclusión.		
Mejores prácticas, referencias:		**1.-** Se recomienda al desarrollar un sistema de información no usar datos personales sino ficticios. **2.-** Se sugiere incluir en la documentación del desarrollo de un sistema de información el inventario de datos y el tipo de información de prueba.		
Conocimientos requeridos:		Administración de bases de datos. Consulta y actualización de tablas.		
Ejecución			**Fecha inicio**	
Nombre y firma Programador, desarrollador o diseñador del sistema de información			**Fecha término**	
Observaciones / anotaciones				

NO APLICA

Sistema de pagos			DLFL/SP	
Formato:	**2**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 18. I. e) Asignar o revocar los privilegios de acceso para los usuarios teniendo como base el principio del menor privilegio.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Un día hábil.		
Importancia de la acción:		No se deben asignar privilegios de acceso a los usuarios en niveles que no estén relacionados con su responsabilidad en el tratamiento de datos.		
Proceso recomendado:		**A)** Realizar respaldo completo de la base de datos. **B)** Ejecutar consulta en el sistema de información de la lista de usuarios y sus niveles o privilegios de acceso. **C)** Validar que los niveles de acceso son acordes a la relación del usuario con el tratamiento de datos personales. **D)** Si hay usuarios con privilegios mayores a los que les son necesarios, cambiar al mínimo indispensable e informarlo al usuario. Regresar al punto B. **E)** Si los privilegios de acceso son correctos para los usuarios, llenar formato con nombre y firma de quien realizó la acción, fecha de inicio y de conclusión.		
Mejores prácticas, referencias:		**1.-** Definir niveles de acceso adecuados para cada perfil o tipo de usuario. **2.-** Tener un mínimo de administradores o usuarios con altos privilegios en el sistema.		
Conocimientos requeridos:		Administración de bases de datos. Consulta y actualización de usuarios.		
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información			**Fecha término**	
Observaciones / anotaciones				

NO APLICA

Sistema de pagos			DLFL/SP	
Formato:	**3**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 18. I. g) Instalar y mantener vigentes certificados de comunicación segura SSL en el caso de servicios basados en Web.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Tres días hábiles.		
Importancia de la acción:		El instalar un certificado SSL en servidores web incrementa la seguridad al encriptar la transferencia de datos y la unicidad del sitio para los usuarios.		
Proceso recomendado:		**A)** En caso de no tener un certificado SSL vigente, enviar correo electrónico al Departamento de Firma Electrónica de DGTIC a firma.tic@unam.mx solicitando la asignación. **B)** El Departamento de Firma Electrónica Avanzada envía procedimiento para obtención de CSR del servidor, formato de la solicitud y costos de recuperación en función del tipo de certificado requerido (organizacional, comodín o corporativo). **C)** Completar documentación, proceso y pago de costo de recuperación. Enviar comprobantes a firma.tic@unam.mx. **D)** Al recibir el certificado SSL, instalarlo en el servidor de acuerdo con las instrucciones recibidas junto con el certificado.		
Mejores prácticas, referencias:		**1.-** Los certificados SSL deben tener una vigencia de al menos un año. **2.-** En caso de tener varios sistemas de información bajo un mismo dominio, se recomienda obtener un certificado SSL del tipo comodín (*wildcard*). **3.-** Se debe realizar el proceso de renovación del certificado al menos 10 días hábiles antes de su vencimiento.		
Conocimientos requeridos:		Administración de sistema operativo. Administración de servicios Web.		
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

NO APLICA

<table>
<tr><td colspan="3">Sistema de pagos</td><td colspan="2">DLFL/SP</td></tr>
<tr><td>Formato:</td><td>4</td><td>Verificación anual</td><td>Acción concluida</td><td>( )</td></tr>
<tr><td colspan="2">Medidas de seguridad técnicas:</td><td colspan="3">Artículo 18. I. h) Definir el plan de respaldos de la información, incluyendo periodicidad y alcance.</td></tr>
<tr><td colspan="2">Aplicable en:</td><td colspan="3">I. Bases de datos y sistemas de tratamiento.</td></tr>
<tr><td colspan="2">Tiempo estimado:</td><td colspan="3">Dos días hábiles.</td></tr>
<tr><td colspan="2">Importancia de la acción:</td><td colspan="3">En todo sistema de información es indispensable contar con un plan de respaldos periódicos, y especialmente en aquellos que contienen datos personales.</td></tr>
<tr><td colspan="2">Proceso recomendado:</td><td colspan="3">A) Elaborar documento con la secuencia de respaldos al menos con el siguiente orden:
- Diario – incremental.
- Semanal – incremental.
- Mensual – total.
B) Establecer en el plan los medios para resguardo del respaldo y su forma de identificación:
- En línea: mismo equipo donde se ejecuta el sistema.
- Respaldo como servicio: otro equipo de almacenamiento.
- Fuera de línea: medios magnéticos (cintas, discos) y/u ópticos.
C) Incluir en el plan:
- Responsables de cada tipo y medio de respaldo.
- Rotación de respaldos y medios.
- Áreas de resguardo.
- Métodos de cifrado.
- RTO: Recovery Time Objective. Tiempo objetivo de recuperación.
- RPO: Recovery Point Objective: Punto objetivo de recuperación.
D) Concluir este documento, adjuntarlo a SGPDP, llenar y firmar formato.</td></tr>
<tr><td colspan="2">Mejores prácticas, referencias:</td><td colspan="3">1.- Se deben tener al menos 3 respaldos del sistema y sus bases de datos en distintos medios.</td></tr>
<tr><td colspan="2">Conocimientos requeridos:</td><td colspan="3">Administración de sistema operativo. Gestión y programación de respaldos.</td></tr>
<tr><td colspan="3">Ejecución</td><td colspan="2">Fecha inicio</td></tr>
<tr><td colspan="3"></td><td colspan="2"></td></tr>
<tr><td colspan="3">Nombre y firma
Administrador del sistema de información o servidor</td><td colspan="2">Fecha término</td></tr>
<tr><td colspan="3"></td><td colspan="2"></td></tr>
<tr><td colspan="2">Observaciones / anotaciones</td><td colspan="3"></td></tr>
</table>

NO APLICA

Sistema de pagos			DLFL/SP	
Formato:	**5**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 18. I. i) Definir el procedimiento para el borrado seguro.**			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Un día hábil.			
Importancia de la acción:	Al igual que el procedimiento de respaldo, el borrado seguro de la información debe estar definido en cualquier sistema de información.			
Proceso recomendado:	**A)** Elaborar documento con el procedimiento y la herramienta para borrado seguro en función del tipo de base de datos para registros, tablas y base de datos. **B)** Incluir en el documento de borrado seguro el proceso de verificación de la no existencia del dato, generalmente por medio de consultas y de copias de respaldo. **C)** El borrado seguro debe incluirse en los respaldos incrementales y totales y en cualquiera de los medios de respaldo, así como máquinas virtuales o contenedores. **D)** Concluir este documento, adjuntarlo a SGPDP, llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** Para el caso de baja de equipo, se debe llenar el formato con la declaración de borrado seguro del Patronato Universitario, disponible en: http://www.patrimonio.unam.mx/patrimonio/descargas/formato_responsiva_borrado_datos.pdf **2.-** Se recomienda utilizar herramientas de borrado seguro por medio de sobre escritura aleatoria, llenado de ceros (0x00), llenado de unos o protocolos de borrado del estándar *DOD-5220.22-M*.			
Conocimientos requeridos:	Administración de sistema operativo. Comandos de borrado.			
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

NO APLICA

<table>
<tr><td colspan="3">Sistema de pagos</td><td colspan="2">DLFL/SP</td></tr>
<tr><td>Formato:</td><td>6</td><td>Verificación anual</td><td>Acción concluida</td><td>( )</td></tr>
<tr><td colspan="2">Medidas de seguridad técnicas:</td><td colspan="3">Artículo 18. II. a) Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM</td></tr>
<tr><td colspan="2">Aplicable en:</td><td colspan="3">II. Sistemas operativos y servicios.</td></tr>
<tr><td colspan="2">Tiempo estimado:</td><td colspan="3">Un día hábil.</td></tr>
<tr><td colspan="2">Importancia de la acción:</td><td colspan="3">A fin de poseer información consistente, los sistemas de información deben estar sincronizados con una instancia central de tiempo, en este caso el servidor NTP de la UNAM.</td></tr>
<tr><td colspan="2">Proceso recomendado:</td><td colspan="3">A) Realizar la verificación y configuración con privilegio de administrador del sistema operativo.
B) En función del sistema operativo, acceder a la configuración de servidor de tiempo (NTP) en interfaz gráfica o por medio de línea de comandos. <u>Por ejemplo</u>, en el caso del sistema operativo Linux:
- Verificar la existencia del archivo /etc/ntp.conf
- Editar el archivo ntp.conf incluyendo en la primera línea:
server ntpdgtic.redunam.unam.mx ó
server 132.247.169.17
- Reiniciar el demonio del cliente NTP con el comando sudo service ntp reload.
C) En caso de no tener el cliente NTP instalado, descargarlo del repositorio de aplicaciones del sistema operativo, instalarlo y regresar al punto B.
D) Llenar y firmar formato.</td></tr>
<tr><td colspan="2">Mejores prácticas, referencias:</td><td colspan="3">1.- Los servidores virtuales y contenedores hospedados en el Centro de Datos en DGTIC son configurados de origen con sincronización al servidor NTP de la UNAM.
2.- No se deben usar otros servidores de NTP distintos al de UNAM.</td></tr>
<tr><td colspan="2">Conocimientos requeridos:</td><td colspan="3">Administración de sistema operativo.</td></tr>
<tr><td colspan="3">Ejecución</td><td colspan="2">Fecha inicio</td></tr>
<tr><td colspan="3"></td><td colspan="2"></td></tr>
<tr><td colspan="3">Nombre y firma
Administrador del sistema de información o servidor</td><td colspan="2">Fecha término</td></tr>
<tr><td colspan="3"></td><td colspan="2"></td></tr>
<tr><td>Observaciones / anotaciones</td><td colspan="4"></td></tr>
</table>

NO APLICA

Sistema de pagos			DLFL/SP	
Formato:	**7**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 18. II. b) Instalar y mantener actualizado el software antimalware.**		
Aplicable en:		II. Sistemas operativos y servicios.		
Tiempo estimado:		Dos días hábiles.		
Importancia de la acción:		El servidor que hospede el sistema de información debe tener protecciones instaladas para mitigar la inserción de *malware* (*rootkits, backdoors o* códigos maliciosos) que pueda alterar su operación o la integridad y seguridad de los datos.		
Proceso recomendado:		**A)** En función del sistema operativo, instalar uno o varios programas para la contención de malware. *Por ejemplo*, para el caso del sistema operativo Linux existen herramientas de código abierto y uso libre como *chkrootkit, rootkit hunter, bothunter, clamAV, avast*, entre otros, que se pueden instalar desde el repositorio correspondiente a la distribución de Linux en uso. **B)** Disponer de comandos para la localización de amenazas. *Por ejemplo*, para el caso de Linux, se recomienda usar el comando *grep* para la detección de cadenas regulares de texto en las invocaciones al *shell*. **C)** Una vez instalada la solución, verificar periódicamente su actualización **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** UNAM-CERT puede asesorar en la selección de las herramientas *anti malware* más adecuadas para el servidor donde se aloje el sistema de información. Contactar al correo seguridad.tic@unam.mx.		
Conocimientos requeridos:		Administración de sistema operativo. Instalación de aplicaciones.		
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

NO APLICA

Sistema de pagos			DLFL/SP	
Formato:	**8**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 18. II. c) Instalar las actualizaciones de seguridad más recientes disponibles.**		
Aplicable en:		II. Sistemas operativos y servicios.		
Tiempo estimado:		Cuatro días hábiles.		
Importancia de la acción:		El servidor que hospede el sistema de información debe tener vigentes todas las actualizaciones de seguridad proporcionadas por el fabricante o desarrollador del sistema operativo.		
Proceso recomendado:		**A)** En función del sistema operativo, se debe revisar la vigencia y actualización de las herramientas de seguridad de la información. *Por ejemplo*, en el sistema operativo Linux ejecutar *apt-get update* para obtener la lista de actualizaciones, especialmente en el repositorio *security* de la respectiva distribución. **B)** Realizar un respaldo del sistema para garantizar retorno a versión anterior en caso de incompatibilidad con alguna aplicación de las actualizaciones de seguridad. **C)** Instalar las actualizaciones en el sistema operativo. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Debe verificarse la actualización de seguridad del sistema operativo al menos una vez a la semana y configurar la actualización o notificación inmediata en caso de complementos de seguridad urgentes.		
Conocimientos requeridos:		Administración de sistema operativo. Instalación de aplicaciones.		
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

NO APLICA

Sistema de pagos			DLFL/SP	
Formato:	**9**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 19. I. a) Aplicar un mecanismo de autenticación para las personas autorizadas con base en el principio del menor privilegio.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Cuatro días hábiles.		
Importancia de la acción:		Partiendo de la asignación o niveles de acceso a la información con el principio del menor privilegio, debe haber en operación en el sistema al menos un mecanismo para la validación de los usuarios autorizados.		
Proceso recomendado:		**A)** Verificar el tipo de control de acceso al sistema, esto es: a través de contraseñas, claves, identificadores, nombres de usuario, nombres de dominio, entre otros. Según sea aplicable al sistema de información en lo particular. En caso de no tener un control de acceso establecer al menos uno como: usuarios de sistema operativo, cuenta y contraseña de sistema. **B)** Revisar que los privilegios de acceso sean los adecuados en función del rol del usuario. *Por ejemplo:* el usuario de conexión a la base de datos no debe estar asignado a alguna cuenta del personal que tiene acceso al sistema. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Se recomienda usar un esquema estándar de acceso a sistemas que están vinculados, por ejemplo: por medio de Directorio Activo (*Active Directory*), *LDAP* u *OpenAIM.* **2.-** Las contraseñas deben ser de 12 caracteres o más con uso de signos, letras mayúsculas y minúsculas y números.		
Conocimientos requeridos:		Administración de bases de datos. Consulta y actualización de usuarios.		
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

NO APLICA

Sistema de pagos			DLFL/SP	
Formato:	**10**	**Verificación anual**	**Acción concluida**	( )
Medida de seguridad técnica:		**Artículo 19. II. b) Evitar la instalación de cualquier elemento de software que implique algún riesgo para el tratamiento de datos personales.**		
Aplicable en:		II. Sistemas operativos.		
Tiempo estimado:		Dos días hábiles.		
Importancia de la acción:		Por la relevancia de los sistemas de información con datos personales se debe minimizar o erradicar el riesgo de seguridad que implica instalar aplicaciones no verificadas.		
Proceso recomendado:		**A)** Dependiendo del sistema operativo, configurar las actualizaciones solamente para versiones maduras o revisiones certificadas de las aplicaciones. *Por ejemplo*: en sistemas Linux desactivar la instalación de versiones *beta, test, debug, non-official.* **B)** De la lista de software instalado, verificar el consumo de recursos de aplicaciones *TSR (Terminal and Stay Resident)*. Identificar demonios que ocupen excesiva RAM o tiempo de ejecución en el procesador. *Por ejemplo*: En sistemas Windows usar el Administrador de Tareas para identificar programas de alto consumo. **C)** Desinstalar toda aquella aplicación, librería, programa, paquetería o servicio que no sea estrictamente necesario para la operación del sistema. *Por ejemplo*, si el servidor Linux no proporcionará direcciones IP, el demonio o servicio *dchpd* no debe estar instalado. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** En ningún caso puede instalarse software de procedencia desconocida. Se debe impedir a los usuarios en sus privilegios de acceso instalar software o inyectar código a la aplicación del sistema de información. y se debe realizar un control estricto de los puertos de comunicación (USB, Red, etc) para evitar la extracción no autorizada de datos.		
Conocimientos requeridos:		Administración de sistema operativo. Instalación de aplicaciones.		
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

NO APLICA

Sistema de pagos			DLFL/SP	
Formato:	**11**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 19. III. a) Establecer las medidas físicas de seguridad que controlen el acceso a los equipos.**		
Aplicable en:		III. Equipo de cómputo.		
Tiempo estimado:		Dos días hábiles.		
Importancia de la acción:		Además de las protecciones de tipo lógico, deben implementarse medidas de seguridad para reducir el riesgo al sistema de información por accesos físicos no autorizados.		
Proceso recomendado:		**A)** Identificar las medidas físicas que restrinjan el acceso físico a equipos, tales como chapas, puertas, biométricos. **B)** En función del equipo de cómputo, hacer una relación de las condiciones más adecuadas para su protección que aún sean necesarias implementar. **C)** Establecer y seguir un plan de mejoramiento de la protección física de equipos. *Por ejemplo*; cámaras de videovigilancia, bitácoras, vigilantes, cuartos cerrados, racks con puerta y chapa, candados en equipos, bloqueo o desconexión física de puertos USB, alarmas y sensores, según sea lo más conveniente como mínimo para la protección de los datos. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Las medidas físicas de seguridad deben revisarse regularmente y formar parte de plan de continuidad de operaciones, así como ser del conocimiento de la Comisión local de seguridad.		
Conocimientos requeridos:		Administración de bases de datos. Consulta y actualización de usuarios.		
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

NO APLICA

Sistema de pagos			DLFL/SP	
Formato:	**12**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 19. III. b) Restringir la salida de equipos de las instalaciones de cada área universitaria.**		
Aplicable en:		III. Equipo de cómputo.		
Tiempo estimado:		Un día hábil.		
Importancia de la acción:		Se debe tener un mecanismo de control para la entrada y salida de equipos de cómputo y eliminar extracciones no autorizadas.		
Proceso recomendado:		**A)** Diseñar una bitácora o formato para el registro de entrada y salida de equipos de cómputo y periféricos asociados como discos duros, cintas, unidades *flash*, discos ópticos, monitores, teclados, ratones y en lo general todo componente de un equipo. **B)** La bitácora de entrada y salida debe incluir el registro de número de serie e inventario UNAM. responsable de ingreso o egreso del componente y firma autorizada del responsable del área. **C)** Incluir en el procedimiento la revisión periódica (al menos una vez al mes) de la consistencia del inventario registrado contra la bitácora de entrada y salida. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Se recomienda usar un formato estándar de control de entrada y salida de bienes proporcionado por las áreas administrativas de las entidades y dependencias y conservar una copia en el área responsable del equipo de cómputo. **2.-** En la bitácora se debe incluir la razón de la entrada o salida del equipo. En el caso de baja, se deberá firmar la declaración de borrado seguro de Patrimonio Universitario.		
Conocimientos requeridos:		Gestión de Tecnología de información, control de entrada y salida de equipo y materiales.		
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

NO APLICA

Sistema de pagos			DLFL/SP	
Formato:	**13**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 19. IV. a) Realizar la transmisión de datos personales a través de un canal cifrado.**		
Aplicable en:		IV. Red de datos.		
Tiempo estimado:		Tres días hábiles.		
Importancia de la acción:		La comunicación del sistema de información con otros sistemas o servicios, así como el acceso de administración para ejecución de procesos por comandos, debe estar encriptada para evitar el envío o recepción de datos susceptibles de ser interceptados en tránsito.		
Proceso recomendado:		**A)** Identificar, mediante el administrador de aplicaciones que corresponda al sistema operativo, los protocolos y aplicaciones instalados para comunicación cifrada. *Por ejemplo*: *SFTP (Secure File Transfer Protocol), SSH (Secure Shell), SCP (Secure Copy*). **B)** Instalar con el administrador de aplicaciones o comando similar los protocolos de comunicación cifrada que sean necesarios para el tipo de transacciones y accesos del sistema. *Por ejemplo*, en el caso de requerir ejecutar comandos de forma remota en un servidor Linux, instalarlo con el comando *apt-get install openssh-server.* **C)** Activar los protocolos de comunicación encriptada en el servidor. *Por ejemplo*: en Linux con el comando *sudo systemctl enable ssh*. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Se deben mantener actualizados los protocolos de comunicación por canal cifrado al igual que las utilerías de seguridad. 2.- El protocolo de comunicación cifrada requiere puertos específicos TCP, los cuales deberán estar permitidos en la configuración del equipo activo de red.		
Conocimientos requeridos:		Administración de sistema operativo. Instalación de aplicaciones. Administración de red.		
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

NO APLICA

Sistema de pagos			DLFL/SP	
Formato:	**14**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 20. Aplicar el procedimiento de borrado seguro que impida la recuperación en las bases de datos y todos sus respaldos.**		
Aplicable en:		Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Tres días hábiles.		
Importancia de la acción:		Se debe verificar que el procedimiento de borrado seguro es funcional y que el dato no persiste en función del tipo de borrado (registro, tabla, base, sistema).		
Proceso recomendado:		**A)** Realizar una copia integral del sistema de información y colocarla en un servicio temporal. *Por ejemplo:* máquina virtual directorio temporal en el servidor. **B)** Ingresar a la copia del sistema de información y realizar el borrado de un registro. Verificar que el dato no persiste en la base de datos por medio de forma de consulta o comando. **C)** Realizar el mismo proceso del punto B para una tabla y finalmente para la base de datos completa. D) En caso de persistencia del dato, instalar y ejecutar herramientas para borrado seguro. *Por ejemplo*: en Linux se dispone *de shred, wipe, secure-delete, srm, sfill, sswap, sdmem,* que se pueden instalar desde el administrador de aplicaciones. **D)** Llenar y firmar este formato.		
Mejores prácticas, referencias:		**1.-** Se recomienda usar al menos un comando a nivel de sistema operativo para el borrado seguro de conformidad con el procedimiento establecido.		
Conocimientos requeridos:		Administración de sistema operativo. Instalación de aplicaciones. Gestión de archivos.		
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

POLÍTICAS

POLÍTICAS PARA LA PROTECCIÓN DE DATOS PERSONALES

En todo tratamiento de datos personales que se realice en la DLFL, se deberán respetar los principios y deberes dispuestos en la LGPDPPSO, de conformidad con lo dispuesto para ello en los LGPDPSP y en los LPDPPUNAM, considerando el ciclo de vida de los datos personales conforme al "Catalogo de Disposición documental"[4].

Lo anterior, en los términos que a continuación se presentan:

a) Principios que rigen la protección de los datos personales.

Licitud: el tratamiento de datos personales por parte del responsable deberá sujetarse a las facultades o atribuciones que la normatividad aplicable le confiera.

Finalidad: todo tratamiento de datos personales que efectúe el responsable deberá estar justificado por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable le confiera.

Lealtad: el responsable no deberá obtener y tratar datos personales, a través de medios engañosos o fraudulentos, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad.

Consentimiento: cuando no se actualicen algunas de las causales de excepción previstas en el artículo 22 de la LGPDPPSO, el responsable deberá contar con el consentimiento previo del titular para el tratamiento de los datos personales.

Calidad: El responsable deberá adoptar las medidas necesarias para mantener exactos, completos, pertinentes, correctos y actualizados los datos personales en su posesión, a fin de que no se altere su veracidad.

Se presume que se cumple con la calidad en los datos personales cuando estos son proporcionados directamente por su titular y hasta que éste no manifieste y acredite lo contrario.

Cuando los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento, deberán ser suprimidos, previo bloqueo en su caso, y una vez que concluya el plazo de conservación de los mismos.

Proporcionalidad: el responsable sólo deberá tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento.

Información: el responsable deberá informar al titular, a través del aviso de privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto.

---

[4] Instrumentos de Control y Consulta Archivística de la Universidad Nacional Autónoma de México 2022. Publicados en el Portal de Transparencia Universitaria el 1 de enero de 2022, consultables a través de la liga: *https://www.repositoriotransparencia.unam.mx/DocumentosDigitales/descargar/JOHE_1650676046*

Responsabilidad: el responsable deberá adoptar políticas e implementar mecanismos para asegurar y acreditar el cumplimiento de los principios, deberes y demás obligaciones establecidas en la LGPDPPSO.

b) Deberes que rigen la protección de los datos personales.

Seguridad: implica que la DLFL deberá establecer y mantener medidas de carácter administrativo, físico y técnico para la protección de datos personales en su posesión.

Confidencialidad: se deben definir controles o mecanismos que tengan por objeto que todas aquellas personas que intervengan en cualquier fase del tratamiento de los datos personales guarden confidencialidad respecto de estos, obligación que subsistirá aún después de finalizar sus relaciones con el mismo.

c) Generalidades del ciclo de vida de los datos personales.

En el respeto de los principios y el cumplimiento de los deberes previstos para el tratamiento de los datos personales, se deberán considerar las etapas que integran el ciclo de vida de los datos personales, los cuales son:

1. Obtención;
2. Uso (registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición); y
3. Eliminación.

Las etapas del ciclo de vida de los datos personales se relacionan con los principios y deberes de la siguiente forma:

Por tanto, las áreas deberán alinear cada etapa del ciclo de vida de acuerdo al principio y deber respectivo.

d) Prohibición de tratamientos que tengan como efecto cualquier tipo de discriminación.

Queda prohibido el tratamiento de datos personales que tengan como efecto la discriminación de sus titulares por su origen étnico o racial, su estado de salud presente, futuro o pasado, su información genética, sus opiniones políticas, religiosas o creencias filosóficas o morales o su preferencia sexual.

POLÍTICAS DE BORRADO SEGURO DE DATOS PERSONALES

Cuando los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, es decir, borrados, suprimidos, eliminados o destruidos.

La destrucción de los datos personales debe hacerse bajo procedimientos seguros que garanticen que los datos fueron borrados o eliminados de la base de datos en su totalidad y que los mismos no pueden ser recuperados, y utilizarse de manera indebida.

Para la protección de los datos personales a lo largo de su ciclo de vida, así como en general de cualquier información que represente un activo para la DLFL, es importante contar con una medida de seguridad que permita minimizar el efecto de cualquier tipo de recuperación de información no autorizada, sobre los medios de almacenamiento físicos y electrónicos, relacionados con el tratamiento de datos personales que se desechan. Por lo tanto, el borrado seguro es la medida de seguridad mediante la cual se establecen métodos y técnicas para la eliminación definitiva de los datos personales, de modo que la probabilidad de recuperarlos sea mínima.

Cuando los datos personales hayan dejado de ser necesarios para las finalidades por las que se obtuvieron, deben ser eliminados, tomando en cuenta lo dispuesto en el "Catalogo de Disposición Documental"[5] aplicable para los plazos de conservación.

Con independencia de que el titular de los datos personales ejerza su derecho de cancelación, el responsable del tratamiento está obligado a eliminar, de oficio, los datos personales cuando hayan dejado de ser necesarios para la finalidad para la cual se obtuvieron.

Para definir los métodos de borrado, es necesario establecer la naturaleza de los activos, los cuales pueden ser:

1. **Medios de almacenamiento físico.** Todo recurso inteligible a simple vista y con el que se puede interactuar sin la necesidad de ningún aparato que procese su contenido para examinar, modificar o almacenar datos personales.
2. **Medios de almacenamiento electrónico.** Todo recurso al que se puede acceder sólo mediante el uso de un equipo de cómputo que procese su contenido para examinar, modificar o almacenar los datos personales

¿CÓMO BORRAR DE MANERA SEGURA LOS DATOS PERSONALES?

a) Destrucción de los medios de almacenamiento físico:
   1. Trituración - para la adquisición de una trituradora se debe considerar el tipo y tamaño del corte o "partícula", así como la capacidad de la trituradora.

b) Destrucción de los medios de almacenamiento electrónicos:
   1. Desintegración – separación completa o pérdida de la unión de los elementos que conforman algo, de modo que deje de existir.

MÉTODOS LÓGICOS DE BORRADO

Son aquellos que implican la sobre-escritura o modificación del contenido del medio de almacenamiento electrónico.

---

[5] *Op. cit.*

a) **Desmagnetización:** expone a los dispositivos de almacenamiento a un campo magnético a través de un dispositivo denominado desmagnetizador.
b) **Sobre-escritura:** escribir información nueva en la superficie de almacenamiento, en el mismo lugar que los datos existentes, utilizando herramientas de software.
c) **Cifrado de medios:** cuando un archivo electrónico o medio de almacenamiento se encuentra cifrado, es posible aplicar el denominado "borrado criptográfico". Para borrar únicamente las claves que se utilizaron para cifrar el medio de almacenamiento o archivo.

MEDIOS DE ALMACENAMIENTO Y SUS RESPECTIVOS MÉTODOS DE BORRADO SEGURO

Medios de almacenamiento	Tipo de medio	Método de borrado seguro
Medio de almacenamiento físico	- Archiveros - Gavetas - Bodegas - Estantes - Oficinas	- Trituración
Magnéticos	- Disco duro - Disco duro externo o portátil - Cintas magnéticas	- Sobre-escritura - Desmagnetización - Destrucción física
Óptico (dispositivos re-grabables)	- CD-RW/DVD-RW - Blu-Ray re-grabable (BD-RE)	- Sobre-escritura - Destrucción física
Magneto-óptico	- Disco magneto-óptico - MiniDisc - HI-MD	- Sobre-escritura - Destrucción física
Estado sólido	- Pendrive/USB - Tarjetas de memoria (Flash drive) - Dispositivo de estado sólido	- Sobre-escritura - Destrucción física

Nota: En caso de realizar una subcontratación, es necesario tomar en cuenta las siguientes consideraciones:

1. Si el borrado seguro se realiza en las instalaciones de un tercero, esto implica posibles gastos de transporte, así como la necesidad de establecer medidas para el resguardo, registro y vigilancia de los medios de almacenamiento. Por lo que se debe ser cuidadoso con este proceso a fin de que no existan fugas de información o pérdidas de activos.
2. Se requiere establecer un contrato donde se defina de forma detallada el servicio que prestará el tercero, así como las responsabilidades de ambas partes.
3. Se debe verificar si el proveedor cuenta con credenciales, certificaciones, o cualquier prueba de que el borrado seguro se realiza en un ambiente controlado.
4. Es importante atestiguar el borrado y solicitar al prestador de servicio un certificado o acta del proceso de borrado realizado.

Sin importar si el borrado seguro se hace dentro del área universitaria, o bien a través de una subcontratación, se debe administrar la generación de evidencia de dicho proceso. Por ejemplo, con certificados, actas, fotografías y bitácoras de la destrucción, a fin de que ante un procedimiento del INAI se pueda demostrar el cumplimiento de esta medida de seguridad.

CÓMPUTO EN LA NUBE

En caso de contar con un servicio de nube particular, y que la información se encuentre almacenada en la infraestructura de un tercero. La mejor herramienta con la que se cuenta es el contrato de servicio.

Además de las cláusulas de borrado, se deben revisar las políticas del proveedor respecto a las copias de seguridad y respaldos que realiza de la información. De ser posible, se debe solicitar al proveedor evidencia del proceso de borrado que realiza.

POLÍTICAS PARA LA TRANSFERENCIA DE DATOS PERSONALES

Por transferencia[6] debe entenderse todo traslado de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta de su titular, la UNAM o la DLFL.

De los artículos 65 y 66 de la LGDPPSO se desprenden dos reglas:

1. Toda transferencia de datos personales sea nacional o internacional, se encuentra sujeta al consentimiento de su titular, salvo las excepciones previstas en los artículos 22, 66 y 70 de la Ley General.
2. Toda transferencia debe encontrarse formalizada mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, de conformidad con la normatividad aplicable a la UNAM, con excepción de los supuestos previstos en el artículo 66 de la Ley General.

Reglas generales y excepciones:

a) El consentimiento del titular de los datos personales

Toda transferencia de datos personales sea nacional o internacional, se encuentra sujeta al consentimiento de su titular, salvo las excepciones previstas en los artículos 22, 66 y 70 de la LGPDPPSO.

Lo anterior implica que, las instancias deben contar con el consentimiento del titular de los datos personales para realizar transferencias. Con excepción de los supuestos siguientes:

- Cuando la transferencia esté prevista en la Ley General u otras leyes, convenios o tratados internacionales suscritos y ratificados por México.
- Cuando la transferencia se realice entre la UNAM y/o la DLFL y otro responsable, siempre y cuando los datos personales se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales.
- Cuando la transferencia sea legalmente exigida para la investigación y persecución de los delitos, así como la procuración o administración de justicia.
- Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho ante autoridad competente, siempre y cuando medie el requerimiento de esta última.
- Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios, siempre y cuando dichos fines sean acreditados.
- Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre la UNAM y/o la DLFL y el titular de los datos personales.
- Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por la UNAM y/o un tercero.
- Cuando se trate de los casos en los que la DLFL no está obligada a recabar el consentimiento del titular para el tratamiento y transmisión de sus datos personales, conforme a lo dispuesto en el artículo 22 de la Ley General.
- Cuando la transferencia sea necesaria por razones de seguridad nacional.

Bajo el esquema expuesto, si la transferencia a realizar se encuentra sujeta al consentimiento del titular de los datos personales, las instancias deberán realizar las gestiones necesarias para recabarlo.

---

[6] Artículo 3, fracc. XXXII - **Transferencia**: Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado

Al respecto, de conformidad con el artículo 113 de los Lineamientos Generales, por regla general el consentimiento a que se refiere el punto anterior será tácito, salvo que una ley exija a la DLFL recabar el consentimiento expreso para la transferencia de sus datos personales.

En términos de lo previsto en el artículo 114 de los citados Lineamientos, cuando se requiera el consentimiento expreso, la instancia podrá establecer cualquier medio lícito que le permita obtenerlo de manera previa a la transferencia de los datos personales.

En todos los casos, las instancias deberán verificar que en el aviso de privacidad correspondiente al tratamiento en que los datos personales fueron recabados, se realice lo siguiente:

i. Se informe al titular de la transferencia a realizar.
ii. Los mecanismos y medios disponibles para que el titular, en su caso, pueda manifestar su negativa para el tratamiento de sus datos personales para finalidades y transferencias de datos personales que requieren su consentimiento, de conformidad con el artículo 27, fracción IV, de la Ley General.

En términos del artículo 113 de los Lineamientos Generales, la DLFL deberá comunicar al destinatario o receptor de los datos personales el aviso de privacidad conforme al cual se obligó a tratar los datos personales frente al titular.

b) Formalización de la transferencia

De conformidad con el artículo 66 de la Ley General, toda transferencia deberá formalizarse mediante alguno de los medios siguientes:

- Suscripción de cláusulas contractuales.
- Convenios de colaboración.
- Instrumentos jurídicos que de conformidad con la normatividad que resulte aplicable, permitan demostrar el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes.

Dicha formalización no será aplicable en los siguientes casos:

- Cuando la transferencia sea nacional y se realice entre responsables en virtud del cumplimiento de una disposición legal o en el ejercicio de atribuciones expresamente conferidas a éstos.
- Cuando la transferencia sea internacional y se encuentre prevista en una ley o tratado suscrito y ratificado por México, o bien, se realice a petición de una autoridad extranjera u organismo internacional competente en su carácter de receptor, siempre y cuando las facultades entre el responsable transferente y receptor sean homólogas, o bien, las finalidades que motivan la transferencia sean análogas o compatibles respecto de aquéllas que dieron origen al tratamiento del responsable transferente.

Por lo que, si la transferencia no se ubica en ninguno de las excepciones antes mencionadas, previo a la realización de una transferencia de datos personales, la DLFL deberá realizar lo siguiente:

1. Identificar las cláusulas contractuales, convenios de colaboración o instrumentos jurídicos existentes en que se encuentren previstas las transferencias de los datos personales.
2. Verificar que, en dichas cláusulas contractuales, convenios o instrumentos, se refleje el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes.
3. Comunicar al tercero receptor el aviso de privacidad correspondiente al tratamiento en que se obtuvieron los datos personales.

4. Solicitar al tercero receptor que manifieste por escrito que se obliga a proteger los datos personales conforme a los principios y deberes que establece la LGPDPPSO y las disposiciones que resulten aplicables en la materia.

Respecto del punto anterior, es importante considerar que en términos del artículo 116 de los Lineamientos Generales, la DLFL sólo podrá transferir datos personales fuera del territorio nacional cuando el receptor o destinatario se obligue a proteger los datos personales conforme a los principios, deberes y demás obligaciones similares o equiparables a las previstas en la Ley General y demás normatividad mexicana en la materia, así como a los términos previstos en el aviso de privacidad que le será comunicado por el responsable transferente.

En caso de considerarlo necesario, las instancias podrán solicitar a través de la Unidad de Transparencia la gestión ante el INAI de una opinión respecto de la logística de la realización de aquellas transferencias internacionales de datos personales que se pretenda efectuar; por lo que deberá de cumplirse con el procedimiento estipulado en el artículo 117 de los Lineamientos Generales.

Fundamento: Artículos 65 a 71 de la Ley General y 113 a 118 de los Lineamientos Generales.

POLÍTICAS PARA LA REMISIÓN DE DATOS PERSONALES

La remisión[7] se refiere a toda comunicación de datos personales realizada exclusivamente entre la DLFL y una persona ajena a ésta que sola o conjuntamente con otras, efectuará el tratamiento de datos personales a nombre y por cuenta de la DLFL.

Al respecto, de conformidad con los artículos 59 a 62 de la Ley General y 108 a 110 de los Lineamientos Generales, la DLFL deberá formalizar su relación con los encargados[8] mediante un contrato o instrumento jurídico que permita acreditar su existencia, alcance y contenido.

Dicho contrato o instrumento deberá considerar con carga al encargado, al menos, las obligaciones siguientes:

- Realizar el tratamiento de los datos personales conforme a la normativa de la UNAM y la DLFL y a las instrucciones que, en su caso, se indiquen en el contrato o instrumento jurídico respectivo.
- Abstenerse de tratar los datos personales para finalidades distintas a las establecidas en la normativa de la DLFL o de lo instruido en el contrato o instrumento jurídico respectivo.
- Implementar medidas de seguridad conforme a la LGPDPPSO. LGPSPSP, LPDPPUNAM, y los instrumentos jurídicos aplicables.
- Informar inmediatamente sobre la vulneración de datos personales a la instancia de la UNAM con quien se haya realizado la remisión de estos.
- Durante y después de la transmisión de los datos personales, deberán guardar la confidencialidad respecto de los mismos.
- Suprimir o devolver los datos personales objeto de tratamiento una vez cumplida la relación jurídica con la DLFL, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales.
- Abstenerse de transferir los datos personales salvo en el caso de que la DLFL así lo determine, o la comunicación derive de una subcontratación, o bien, se realice por mandato expreso de la autoridad competente.
- Permitir y colaborar con la DLFL o con el INAI, para realizar verificaciones en el lugar o establecimiento donde se lleva a cabo el tratamiento de los datos personales, o en su caso, proporcionar la documentación o información que se estime necesaria.
- Generar, actualizar y conservar la documentación necesaria que le permita acreditar el cumplimiento de todas las obligaciones.

En relación con lo anterior todas las instancias que, en el ámbito de su competencia, realicen contrataciones que impliquen el tratamiento de datos personales por parte de encargados, deberán formalizar tales relaciones mediante un contrato o instrumento jurídico que contenga las obligaciones y cláusulas antes señaladas, incluyendo aquella que regule lo que procederá en caso de que el encargado desee subcontratar servicios que involucren el tratamiento de datos personales.

En términos de lo previsto en el artículo 60 de la Ley General, cuando el encargado incumpla las instrucciones de la DLFL y decida por sí mismo sobre el tratamiento de los datos personales, asumirá el carácter de responsable conforme a la legislación de la materia que le resulte aplicable.

---

[7] Artículo 3, fracc. XXVII - **Remisión**: Toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado, dentro o fuera del territorio mexicano.

[8] Artículo 3, fracc. XV - **Encargado**: La persona física i jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable.

a) Regulación de subcontrataciones en la remisión de datos personales

Como se indicó, el contrato o instrumento jurídico en que se convenga la remisión, deberá incluir la regulación procedente en caso de que el encargado desee subcontratar servicios que involucren el tratamiento de los datos personales.

En todos los casos, las instancias competentes deberán conocer y autorizar las subcontrataciones que el encargado realice.

Las autorizaciones se podrán otorgar desde el contrato original, cuando el encargado ya prevea subcontrataciones específicas y garantice que las mismas se realizarán en las condiciones precisadas. En caso contrario, la autorización se podrá realizar de manera posterior.

Para ello, el contrato o instrumento jurídico deberá establecer que las subcontrataciones que no se establezcan de manera expresa en dicho contrato o instrumento deberán ser autorizadas por la DLFL previo a su ejecución.

Asimismo, se deberá comunicar al encargado que el contrato o el instrumento jurídico mediante el cual se formalice la subcontratación deberá incluir cláusulas con las obligaciones indicadas.

POLÍTICAS PARA CÓMPUTO EN LA NUBE

Se referirán a los aspectos que se deberán observar al contratar servicios de cómputo en la nube[9] en caso de no utilizar el servicio de "centro de datos UNAM".

En términos de los artículos 63 y 64 de la Ley General, la DLFL podrá contratar o adherirse a servicios, aplicaciones e infraestructura de cómputo en la nube, y otras materias que impliquen el tratamiento de datos personales, siempre y cuando el proveedor externo garantice las políticas de protección de datos personales equivalentes a los principios, deberes, obligaciones y responsabilidades establecidas en la LGPDPPSO, los LGPSPSP, los LPDPPUNAM y demás disposiciones que resulten aplicables en la materia.

En caso de que la DLFL contrate dichos servicios, deberá delimitar el tratamiento de los datos personales por parte del proveedor externo a través de cláusulas contractuales u otros instrumentos jurídicos.

Por otro lado, en el supuesto de que la DLFL se adhiera a dichos servicios mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente:

- Tener y aplicar políticas de protección de datos personales afines a los principios y deberes que establecen la LGPDPPSO, los LGPSPSP, los LPDPPUNAM y demás disposiciones que resulten aplicables en la materia.
- Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio.
- Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que preste el servicio.
- Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.

Además, se deberá verificar que el proveedor cuente con mecanismos, al menos, para:

- Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta.
- Permitir a la DLFL limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio.
- Establecer y mantener medidas de seguridad para la protección de los datos personales sobre los que se preste el servicio.
- Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado a la DLFL y que este último haya podido recuperarlos.
- Impedir el acceso a los datos personales a personas que no cuenten con permisos de acceso, o bien, en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho a la DLFL.

En ningún caso, la DLFL podrá adherirse a servicios que no garanticen la debida protección de los datos personales, conforme a la LGPDPPSO, los LGPSPSP, los LPDPPUNAM y demás disposiciones que resulten aplicables en la materia.

De conformidad con lo estipulado en el artículo 111 de los Lineamientos Generales, los proveedores de servicios de cómputo en la nube tendrán el carácter de encargados, por lo que si se pretende contratar sus servicios, la DLFL deberá verificar el cumplimiento de lo estipulado en las "Políticas

[9] Artículo 3, fracc. VI – **Cómputo en la nube**: Modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente.

para la Remisión de Datos Personales"; es decir, además de observar las obligaciones señaladas, deberá incluir en el contrato o instrumento jurídico las obligaciones generales de cualquier encargado, las cuales son:

- Realizar el tratamiento de los datos personales conforme a la normativa de la DLFL y a las instrucciones que, en su caso, se indiquen en el contrato o instrumento jurídico respectivo.
- Abstenerse de tratar los datos personales para finalidades distintas a las establecidas en la normativa de la DLFL y de lo instruido en el contrato o instrumento jurídico respectivo.
- Implementar medidas de seguridad conforme a la LGPDPPSO, los LGPSPSP, los LPDPPUNAM y demás disposiciones que resulten aplicables en la materia.
- Informar a la DLFL con quien se haya realizado la remisión de los datos personales cuando ocurra una vulneración a estos.
- Guardar confidencialidad respecto de los datos personales tratados.
- Suprimir o devolver los datos personales objeto de tratamiento una vez cumplida la relación con la DLFL, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales.
- Abstenerse de transferir los datos personales salvo en el caso de que la DLFL así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
- Permitir y colaborar con la DLFL o con el INAI, para realizar verificaciones en el lugar o establecimiento donde se lleva a cabo el tratamiento de los datos personales, o en su caso, proporcionar la documentación o información que se estime necesaria.
- Generar, actualizar y conservar la documentación necesaria que le permita acreditar y verificar el cumplimiento de todas las obligaciones.

POLÍTICAS DE USO DEL CORREO ELECTRÓNICO INSTITUCIONAL

Los mecanismos informáticos se han consolidado como un elemento de primera importancia para la DLFL, en virtud de que apoyan al fortalecimiento y modernización agrupando integralmente la información generada por y para sus actividades, con la finalidad de producir, recolectar, procesar, trasladar y difundir la información de la DLFL con seguridad, precisión y rapidez.

En este contexto, la seguridad de la información es un aspecto de fundamental importancia para los sistemas y bases de datos con las que cuenta la DLFL. Por tal motivo, se deben establecer los mecanismos que habiliten la confiabilidad, disponibilidad y veracidad de la información.

GENERALES:

1. Todo colaborador(a) de la DLFL deberá contar con una cuenta de correo electrónico inscitucional.

2. La cuenta de correo electrónico es personal e intransferible, por lo que queda estrictamente prohibido compartirla, prestarla, traspasarla o cualquier otro acto que implique dar a otros la posibilidad de uso.

3. Toda actividad derivada del uso de la cuenta del correo institucional será responsabilidad del propietario de la misma.

4. El uso de la cuenta de correo electrónico institucional debe limitarse exclusivamente para fines laborales.

5. En caso de presentarse alguna problemática relacionada con el servicio de correo electrónico institucional, el titular de la cuenta deberá comunicarlo de manera directo al Jefe del Departamento de Bienes y Suministros y Servicios Generales de la DLFL y no a través de terceros.

6. La Directora de Literatura y Fomento a la Lectura será quien podrá solicitar al Jefe del Departamento de Bienes y Suministros y Servicios Generales el alta de un usuario en el servicio de correo electrónico institucional.

7. El nombre de usuario es asignado por el Jefe del Departamento de Bienes y Suministros y Servicios Generales, tomando como base el nombre completo del colaborador(a). El nombre de usuario no es modificable.

8. Una vez que el usuario haya recibido los datos de su cuenta de correo electrónico, deberá proceder a cambiar inmediatamente la contraseña por motivos de seguridad.

9. La contraseña deberá cambiarse periódicamente para remplazarla por una nueva.

DE LAS RESTRICCIONES:

1. Queda prohibido el envío o reenvío de correos electrónicos que incluyan: cartas cadena, software pirata, juegos, mensajes con virus o gusanos informáticos, material obsceno, amenazante, invitaciones para integrarse a esquemas de pirámide con intención de hacer propaganda, mensajes con motivos publicitarios con fines lucrativos, políticos, comerciales o para negocio particular, mensajes con intención de intimidar, insultar o acosar, racismo,

envío masivo de mensajes, cambiar o intentar cambiar su identidad en el envío de correos y cualquier otro tipo de correos no solicitados (SPAM). Ninguno de estos u otros mensajes deberá utilizarse en contra de los intereses de individuos o instituciones.

DE LAS SANCIONES:

1. Todo mal uso de la cuenta de correo electrónico institucional ocasionará la cancelación inmediata de la misma.

ADMINISTRACIÓN DE LA CUENTA:

1. La DLFL, a través de la Jefatura de Cómputo es la encargada de asignar el nombre de usuario y una contraseña inicial.

2. El nombre de usuario de la cuenta de acceso que se asigne es definitivo.

RESPONSABILIDADES DEL USUARIO

1. La cuenta de acceso institucional es personal e intransferible. Queda prohibido compartirla, prestarla, traspasarla o cualquier otro acto que implique dar a otros la posibilidad de uso.

2. El usuario titular de la cuenta institucional será responsable de las acciones llevadas a cabo con el acceso otorgado.

3. La contraseña asociada a la cuenta institucional, debe contar con las siguientes características:
   - Longitud mínima de ocho caracteres.

   Contar con al menos:
   - Una letra mayúscula.
   - Una letra minúscula.
   - Un número.
   - Un carácter especial: ! @ , # $ % ^ & * □ ? _ ~ - + . : ; = " [ ] ( ) / \ | { } >

4. La contraseña no debe estar basada en información que pueda inferirse u obtenerse usando datos relacionados a la persona. Por ejemplo: nombres, números telefónicos, fechas de cumpleaños.

5. La contraseña no debe estar basada o contener palabras registradas en diccionarios de cualquier lengua.

6. La contraseña no debe contener caracteres idénticos (numéricos o alfabéticos) de forma consecutiva.

7. La contraseña debe cambiarse al menos una vez cada 4 meses.

Los usuarios que hagan uso de la cuenta institucional deben asegurarse que:

1. Las sesiones en sus equipos personales tengan una protección adecuada, en caso de que los equipos queden desatendidos, se debe configurar el protector de pantalla con contraseña.

2. El equipo personal de cómputo cuente con la protección de un programa antivirus instalado y actualizado.

3. Las sesiones iniciadas por los usuarios del sistema se originen exclusivamente en áreas de trabajo, excluyendo sitios de acceso público a Internet, donde pueda verse comprometido su información de acceso.

4. Todo evento relacionado con el extravió, pérdida o robo de la cuenta institucional debe ser notificado a la brevedad a Genaro Gutiérrez Soto, Jefe del Departamento de Bienes y Suministros y Servicios Generales.

Se testan los anexos titulados “Análisis de Riesgos”, “Análisis de Brecha” y “Plan de Trabajo” por tratarse de información reservada, por un periodo de cinco años, que se computarán a partir del19 de agosto de 2022, fecha de la resolución CTUNAM/525/2022 del Comité de Transparencia de la Universidad Nacional Autónoma de México, 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.

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		