SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES.
DIRECCIÓN DE TEATRO

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 Teatro (DT), 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.

La misión de la DT de la UNAM, es la de apoyar, promover y difundir el arte dramático nacional - dentro y fuera del país- contribuyendo a la formación integral de los universitarios ofreciéndoles un

[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

amplio abanico de manifestaciones escénicas que les permitan relacionarse con el quehacer artístico de manera crítica y permanente.

La administración de la actual Dirección de Teatro está comprometida con el perfil de investigación escénica del teatro universitario y con la creación de nuevos caminos para la expresión teatral, así como la programación de montajes escénicos que representen a las diferentes tendencias artísticas en el campo de la creación teatral.

Avanzar en la consolidación del Teatro Universitario, conservando el prestigio que el mismo ha ganado a lo largo de su historia como un espacio de investigación escénica en el cual se revisen y discutan conceptos como la dramaturgia, la actoralidad, la expresión plástica en el escenario, la multidisciplina, entre otras. Producir, promover y difundir el arte teatral nacional, dentro y fuera del país, contribuyendo a la formación integral de los universitarios en particular y de la sociedad en general, ofreciéndoles un amplio abanico de manifestaciones escénicas que les permitan relacionarse con el quehacer artístico de manera crítica y permanente. Incidir en la formación cultural de la población en general y de los universitarios en particular, apoyando, promoviendo y difundiendo obras del arte teatral nacional e internacional. Resaltar la importancia del teatro universitario dentro del quehacer artístico nacional, a través de sus programas de Vinculación y Enlace con la comunidad universitaria y con la sociedad en general. Promover la reflexión sobre la naturaleza de los espectáculos programados por la Dirección, a través de conferencias, seminarios, programas de mano enriquecidos, etc. Profesionalizar todas las áreas que la integran, con el objeto de hacer más eficientes los procesos de producción y de difusión de las obras programadas. Así como promover la reflexión y el intercambio entre artistas nacionales y extranjeros.

ABREVIATURAS Y DENOMINACIONES

CCU – Centro Cultural Universitario

DT – Dirección de Teatro

EDPAC – Estímulos al Desempeño del Personal Administrativo y de Confianza

SCP – Sistema de Comprobantes de Pago

SCN – Sistema de Comprobación de Nómina

SIPH – Sistema Integral de Personal Honorarios

SIPFUE – Sistema Integral de Personal Formas Únicas

SGPP – Sistema General de Padrón de Profesionales

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

PPSP – Padrón de Prestadores de Servicios Profesionales

SGSDP – Sistema de Gestión de Seguridad de Datos Personales

SIAF – Sistema Integral de Administración Financiera

SIC – Sistema Institucional de Compras

SFDUNAM – Sistema de Factura Digital

UNAM – Universidad Nacional Autónoma de México

UPA – Unidad de Proceso Administrativo

SPPC – Sistema de Padrón de Proveedores y Contratistas

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 DT

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 DT.

   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

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:

ESTÍMULOS AL DESEMPEÑO DEL PERSONAL ADMINISTRATIVO DE CONFIANZA (EDPAC)
- Jefatura de la Unidad Administrativa
- Jefa del Área de Personal

SISTEMA DE COMPROBANTE DE PAGO (SCP)
- Jefatura de la Unidad Administrativa
- Jefa del Área de Personal

SISTEMA DE COMPROBACIÓN DE NÓMINA (SCN)
- Jefatura de la Unidad Administrativa
- Jefa del Área de Personal

SISTEMA DE COMPROBANTE DE PAGO (SCP)
- Jefatura de la Unidad Administrativa
- Jefa del Área de Personal

SISTEMA INTEGRAL DE PERSONAL HONORARIOS (SIPH)
- Jefatura de la Unidad Administrativa
- Jefa del Área de Personal

SISTEMA INTEGRAL DE PERSONAL FORMA ÚNICA ELECTRÓNICA (SIPFUE)
- Jefatura de la Unidad Administrativa
- Jefa del Área de Personal

SISTEMA GENERAL DE PADRÓN DE PROFESIONALES (SGPP)
- Jefatura de la Unidad Administrativa
- Jefa del Área de Personal

SISTEMA DE FACTURA DIGITAL (SFD)
- Jefatura de la Unidad Administrativa
- Jefatura del Departamento de Presupuesto

SISTEMA INSTITUCIONAL DE COMPRAS. (SIC)
- Jefatura de la Unidad Administrativa
- Jefatura del Departamento de Presupuesto
- Jefe de Área de Bienes y Suministros
- Jefe de Área de Servicios Generales
- Jefatura de Prensa y Relaciones Públicas
- Jefatura de Departamento de Teatro
- Jefatura de Departamento de Producción

SISTEMA INTEGRAN DE ADMINISTRACIÓN FINANCIERA (SIAF)

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

UNIDAD DE PROCESO ADMINISTRATIVO (UPA)

- Jefatura de la Unidad Administrativa
- Jefatura del Departamento de Presupuesto
- Jefa del Área de Personal

SISTEMA DE PADRÓN DE PROVEEDORES Y CONTRATISTAS (SPPC)

- Jefatura de la Unidad Administrativa
- Jefatura del Departamento de Presupuesto
- Jefa de Área de Personal

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

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

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

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

Usuarios. Utilizar el SGSDP en sus áreas específicas de acuerdo con el 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 pueden 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 DT.
- 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 DT.

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

2. Se medirá cualitativamente el grado en que la Dirección de Teatro 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:

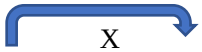
Valores de impacto	
Alto	3
Medio	2
Bajo	1

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 multiplicando

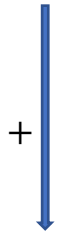
[2] Caralli, Richard A. *et al.* "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process", Software Engineering Intitute, Mayo 2007, *https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf* ,p. 53

[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:

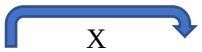


Área de Impacto	Prioridad	Valor de impacto	Puntaje
Reputación / Pérdida de confianza	7	Alto 3	21
Financiera	5	Alto 3	15
Productividad	6	Alto 3	18
Seguridad y salud	1	Alto 3	3
Multas y sanciones	2	Alto 3	6
Interrupción del servicio	4	Alto 3	12
Incumplimiento de obligaciones legales	3	Alto 3	9
	Puntaje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

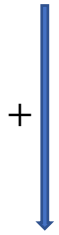


84/3 = 28

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



Área de Impacto	Prioridad	Valor de impacto	Puntaje
Reputación / Pérdida de confianza	7	3	21
Financiera	5	2	15
Productividad	6	3	18
Seguridad y salud	1	1	1
Multas y sanciones	2	2	4
Interrupción del servicio	4	3	12
Incumplimiento de obligaciones legales	3	3	9
		Puntaje total	80



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 reevalúan en algún momento futuro, generalmente estos no son una amenaza inminente ni afectan significativamente
   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 y vulnerabilidades

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

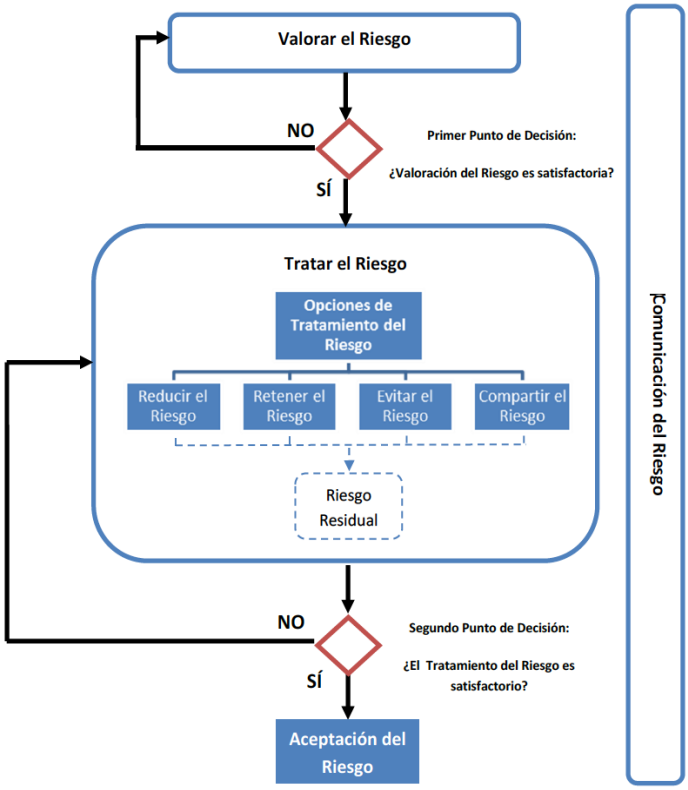
Se seleccionaron las medidas de seguridad administrativas, técnicas o físicas que permiten atender de mejor manera los riesgos identificados y minimizar las consecuencias de posibles vulneraciones. En particular se tomaron en cuenta los siguientes criterios para elegir las medidas de seguridad efectivas:

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 DT 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 reevalúan en algún momento futuro, generalmente estos no son una amenaza inminente ni afectan significativamente
- **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 pueden 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 amenazas potenciales. Deben atenderse considerando:
   i. El análisis y revisión de la amenaza;
   ii. Determinar las fallas o incidentes que podría desencadenarse con una amenaza;
   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 estableciendo:

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. Ejecución estimada 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:	Ana María Rodríguez Simental Jefa de la Unidad Administrativa de la Dirección de Teatro Tel. 55 5622 6843 Ext. 27185. simental@unam.mx	 Ana María Rodríguez Simental
Revisó:	José Antonio Valdez Cruz Jefe de Área de Servicios Generales Tel. 55 5622 6836 sgteatrounam@gmail.com	 José Antonio Valdez Cruz
Autorizó:	Juan Meliá Huerta Director de Teatro Tel. 55 5665 7248 ext. 27090 dirteatrounam@hotmail.com	 Juan Meliá Huerta
Fecha de aprobación:	(Incluir la fecha de liberación del documento)	
Fecha de actualización:	(Incluir la primer versión e ir agregando las subsiguientes del documento)	15/08/2022

ANEXO 1.

INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Dirección de Teatro			
Abreviatura del nombre del sistema	**DT/EDPAC**		
Nombre del sistema	Estímulos al Desempeño del Personal Administrativo y de Confianza		
Datos personales contenidos en el sistema:	- Nombre completo - RFC		
Responsable			
Nombre:	Ana María Rodríguez Simental		
Cargo:	Jefa de la Unidad Administrativa		
Funciones:	Obtención ( ) Uso (X) Registro (X) Organización ( ) Elaboración ( ) Conservación (X)	Utilización ( ) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	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.		
Encargado			
Nombre:	Silvia Araujo Esquivel		
Cargo:	Jefa del Área de Personal		
Funciones:	Obtención ( ) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación (X)	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	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.		
Dirección de Teatro			
Abreviatura del nombre del sistema	**DT/SCP**		
Nombre del sistema	**Sistema de Comprobantes de Pago**		
Datos personales contenidos en el sistema:	- Nombre completo - RFC - Correo Electrónico		
Responsable			
Nombre:	Ana María Rodríguez Simental		
Cargo:	Jefa de la Unidad Administrativa		
Funciones:	Obtención ( ) Uso (X) Registro (X) Organización ( ) Elaboración ( ) Conservación (X)	Utilización ( ) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	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.		
Encargado			
Nombre:	Silvia Araujo Esquivel		
Cargo:	Jefa del Área de Personal		
Funciones:	Obtención ( ) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación (X)	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	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.		
Dirección de Teatro			
Abreviatura del nombre del sistema	**DT/SCN**		
Nombre del sistema	**Sistema de Comprobación de Nómina**		
Datos personales contenidos en el sistema:	- Nombre completo - RFC - Curp - Correo electrónico		
Responsable			
Nombre:	Ana María Rodríguez Simental		
Cargo:	Jefa de la Unidad Administrativa		
Funciones:	Obtención ( ) Uso (X) Registro (X) Organización ( ) Elaboración ( ) Conservación (X)	Utilización ( ) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	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.		
Encargado			
Nombre:	Silvia Araujo Esquivel		
Cargo:	Jefa del Área de Personal		
Funciones:	Obtención ( ) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación (X)	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	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.		
Dirección de Teatro			
Abreviatura del nombre del sistema	**DT/SIPH**		
Nombre del sistema	Sistema Integral de Personal Honorarios		
Datos personales contenidos en el sistema:	- Nombre completo - RFC - Curp - Domicilio particular - Correo electrónico particular		
Responsable			
Nombre:	Ana María Rodríguez Simental		
Cargo:	Jefa de la Unidad Administrativa		
Funciones:	Obtención ( ) Uso (X) Registro (X) Organización ( ) Elaboración ( ) Conservación (X)	Utilización ( ) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	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.		
Encargado			
Nombre:	Silvia Araujo Esquivel		
Cargo:	Jefa del Área de Personal		
Funciones:	Obtención ( ) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación (X)	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	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.		
Dirección de Teatro			
Abreviatura del nombre del sistema	**DT/SIPFUE**		
Nombre del sistema	Sistema Integral de Personal Forma Única		
Datos personales contenidos en el sistema:	- Nombre completo - RFC - Curp - Domicilio particular - Correo electrónico particular		
Responsable			
Nombre:	Ana María Rodríguez Simental		
Cargo:	Jefa de la Unidad Administrativa		

Funciones:	Obtención ( ) Uso (X) Registro (X) Organización ( ) Elaboración ( ) Conservación (X)	Utilización ( ) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	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.		
Encargado			
Nombre:	Silvia Araujo Esquivel		
Cargo:	Jefa del Área de Personal		
Funciones:	Obtención ( ) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación (X)	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	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.		
Dirección de Teatro			
Abreviatura del nombre del sistema	**DT/SGPP**		
Nombre del sistema	Sistema General de Padrón de Profesionales		
Datos personales contenidos en el sistema:	- Nombre completo - RFC - Curp - Domicilio particular - Correo electrónico particular - Estado de cuenta bancario		
Responsable			
Nombre:	Ana María Rodríguez Simental		
Cargo:	Jefa de la Unidad Administrativa		
Funciones:	Obtención ( ) Uso (X) Registro (X) Organización ( ) Elaboración ( ) Conservación (X)	Utilización ( ) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	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.		
Encargado			

Nombre:	Silvia Araujo Esquivel		
Cargo:	Jefa del Área de Personal		
Funciones:	Obtención ( ) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación (X)	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	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.		
Dirección de Teatro			
Abreviatura del nombre del sistema	**DT/SFD**		
Nombre del sistema	**Sistema Factura Digital**		
Datos personales contenidos en el sistema:	- Nombre completo - RFC - Domicilio particular - Correo electrónico particular		
Responsable			
Nombre:	Ana María Rodríguez Simental		
Cargo:	Jefa de la Unidad Administrativa		
Funciones:	Obtención ( ) Uso (X) Registro (X) Organización ( ) Elaboración ( ) Conservación (X)	Utilización ( ) Comunicación ( ) Difusión ( ) Almacenamiento (X) Posesión ( ) Acceso (X)	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.		
Encargado			
Nombre:	Laura Tapia Guzmán		
Cargo:	Jefa del Departamento de Presupuesto		
Funciones:	Obtención ( ) Uso (X) Registro (X) Organización ( ) Elaboración ( ) Conservación (X)	Utilización ( ) Comunicación ( ) Difusión ( ) Almacenamiento (X) Posesión ( ) Acceso (X)	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.		
Encargado			

Nombre:	Gabriela Vázquez Jiménez		
Cargo:	Asistente de Procesos		
Funciones:	Obtención ( ) Uso (X) Registro (X) Organización ( ) Elaboración (X) Conservación (X)	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento (X) Posesión ( ) Acceso (X)	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.		
Dirección de Teatro			
Abreviatura del nombre del sistema	**DT/SIC**		
Nombre del sistema	**Sistema Institucional de Compras**		
Datos personales contenidos en el sistema:	- Nombre completo - RFC - Dirección - Número telefónico particular - Correo electrónico - Factura (en el caso de personas físicas: código postal y/o lugar de expedición)		
Responsable			
Nombre:	Ana María Rodríguez Simental		
Cargo:	Jefa de la Unidad Administrativa		
Funciones:	Obtención ( ) Uso (X) Registro (X) Organización ( ) Elaboración ( ) Conservación (X)	Utilización ( ) Comunicación ( ) Difusión ( ) Almacenamiento (X) Posesión ( ) Acceso (X)	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.		
Encargado			
Nombre encargado 1:	Laura Tapia Guzmán		
Cargo:	Jefa del Departamento de Presupuesto		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación (X)	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento (X) Posesión ( ) 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. -		
Nombre encargado 2:	Daniel Albarrán Oliveros		
Cargo:	Jefe del Área de Bienes y Suministros		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación (X)	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento (X) Posesión ( ) 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.		
Usuarios			
Nombre usuario 1:	Gabriela Vázquez Jiménez		
Cargo:	Asistente de Procesos		
Funciones:	Obtención (_) Uso ( ) Registro (X) Organización (_) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	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.		
Nombre usuario 1:	Angélica Moyfa García García		
Cargo:	Jefa del Departamento de Prensa y Relaciones Públicas		
Funciones:	Obtención (X) Uso ( ) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) 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.		
Nombre usuario 2:	Elizabeth Guadalupe Solís Reyes		
Cargo:	Jefa del Departamento de Teatro		
Funciones:	Obtención (X) Uso ( ) Registro (X) Organización (X) Elaboración ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( )	Manejo (X) Aprovechamiento ( ) Divulgación ( ) Transferencia ( ) Remisión ( )

	Conservación ( )	Acceso ( )	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:	Adán Ricardo de León Martínez		
Cargo:	Jefe del Departamento de Producción		
Funciones:	Obtención (X) Uso ( ) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) 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..		
Nombre usuario 4:	Juan Meliá Huerta		
Cargo:	Director de Teatro		
Funciones:	Obtención (X) Uso ( ) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) 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.		
Nombre usuario 5:	José Antonio Valdez Cruz		
Cargo:	Jefe de Área de Servicios Generales		
Funciones:	Obtención (X) Uso ( ) Registro ( ) Organización (X) Elaboración ( ) Conservación ( )	Utilización ( ) Comunicación ( ) Difusión ( ) Almacenamiento ( ) 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.		
Nombre usuario 6:	Silvia Araujo Esquivel		
Cargo:	Jefa del Área de Personal		

Funciones:	Obtención (X) Uso ( ) Registro ( ) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) 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.		
Dirección de Teatro			
Abreviatura del nombre del sistema	**DT/SIAF**		
Nombre del sistema	**Sistema Integral de Administración Financiera**		
Datos personales contenidos en el sistema:	- Nombre completo - RFC - Nacionalidad		
Responsable			
Nombre:	Ana María Rodríguez Simental		
Cargo:	Jefa de la Unidad Administrativa		
Funciones:	Obtención ( ) Uso (X) Registro (X) Organización (X) Elaboración (X) Conservación (X)	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento (X) Posesión (X) Acceso (X)	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.		
Encargado			
Nombre:	Laura Tapia Guzmán		
Cargo:	Jefa del Departamento de Presupuesto		
Funciones:	Obtención ( ) Uso (X) Registro (X) Organización (X) Elaboración (X) Conservación (X)	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento (X) Posesión (X) Acceso (X)	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.		

Dirección de Teatro			
Abreviatura del nombre del sistema	**DT/UPA**		
Nombre del sistema	**Unidad de Procesos Administrativos**		
Datos personales contenidos en el sistema:	- Factura - Comprobante de domicilio - INE - RFC - Correo electrónico particular - Teléfono particular		
Responsable			
Nombre:	Ana María Rodríguez Simental		
Cargo:	Jefa de la Unidad Administrativa		
Funciones:	Obtención ( ) 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 ( ) 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.		
Encargado			
Nombre Encargado 1:	Laura Tapia Guzmán		
Cargo:	Jefa de Departamento de Presupuesto		
Funciones:	Obtención ( ) 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 ( ) 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:	Silvia Araujo Esquivel		
Cargo:	Jefa del Área de Personal		
Funciones:	Obtención ( ) 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 ( )
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:	Juan Meliá Huerta		
Cargo:	Director de Teatro		
Funciones:	Obtención ( ) Uso (X) Registro ( ) Organización ( ) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) 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 Dirección General. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Dirección de Teatro			
Abreviatura del nombre del sistema	**DT/SPPC**		
Nombre del sistema	**Sistema de Padrón de Proveedores y Contratistas**		
Datos personales contenidos en el sistema:	- Estado de cuenta Bancario - Comprobante de domicilio - Constancia Fiscal - Correo electrónico particular - Teléfono particular		
Responsable			
Nombre:	Ana María Rodríguez Simental		
Cargo:	Jefa de la Unidad Administrativa		
Funciones:	Obtención ( ) 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 ( ) 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.		
Encargado			
Nombre:	Laura Tapia Guzmán		
Cargo:	Jefa de Departamento de Presupuesto		
Funciones:	Obtención ( ) Uso (X) Registro (X) Organización (X) Elaboración ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento (X) Posesión (X)	Manejo (X) Aprovechamiento ( ) Divulgación ( ) Transferencia ( ) Remisión ( )

	Conservación (X)	Acceso (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.		
Encargado			
Nombre:	Silvia Araujo Esquivel		
Cargo:	Jefa del Área de Personal		
Funciones:	Obtención ( ) 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 ( ) 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 Teatro		
Abreviatura del nombre del sistema	**DT/EDPAC**	
Nombre del sistema	**Estímulos al Desempeño del Personal Administrativo de Confianza**	
¿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 ( ) Otros:
	Descripción de la información que se resguarda	- Convocatorias - Acuses de registro - Cédula de evaluación
	Características del lugar donde se resguarda la información	- Archiveros tradicionales de metal, ubicados dentro de la oficina con iluminación artificial y natural. - Computadora ubicada en la oficina del encargado - Carpetas de control en equipo, se tiene cuenta de usuario para acceder.
Dirección de Teatro		
Abreviatura del nombre del sistema	**DT/SCP**	
Nombre del sistema	**Sistema de Comprobantes de Pago**	
¿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 ( ) Otros:
	Descripción de la información que se resguarda	- Complemento de pago
	Características del lugar donde se resguarda la información	- Archiveros tradicionales de metal, ubicados dentro de la oficina con iluminación artificial y natural. - Computadora ubicada en la oficina del encargado - Carpetas de control en equipo, se tiene cuenta de usuario para acceder.
Dirección de Teatro		
Abreviatura del nombre del sistema	**DT/SCN**	
Nombre del sistema	**Sistema de Comprobación de Nómina**	
¿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 ( ) Otros: - Expediente físicos en archiveros.

	Descripción de la información que se resguarda	- Comprobantes de pago (talón)
	Características del lugar donde se resguarda la información	- Archiveros tradicionales de metal, ubicados dentro de la oficina con iluminación artificial y natural. - Computadora ubicada en la oficina del encargado - Carpetas de control en equipo, se tiene cuenta de usuario para acceder.
Dirección de Teatro		
Abreviatura del nombre del sistema	**DT/SIPH**	
Nombre del sistema	**Sistema Integral de Personal 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 ( ) Otros:
	Descripción de la información que se resguarda	- Contratos - CFDI - Bóveda - Relación UPA - Complemento de pago - Recibo UNAM - Certificado de verificación
	Características del lugar donde se resguarda la información	- Computadora ubicada en la oficina del encargado
Dirección de Teatro		
Abreviatura del nombre del sistema	**DT/SIPFUE**	
Nombre del sistema	**Sistema Integral de Personal Forma Única Electrónica**	
¿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 ( ) Otros: Expedientes físicos en archiveros
	Descripción de la información que se resguarda	- Formas únicas - Contratos - Licencias - Procedimientos de investigación administrativa - Algún otro documento atribuible al trabajador

	Características del lugar donde se resguarda la información	- Archiveros tradicionales de metal, ubicados dentro de la oficina con iluminación artificial y natural. - Computadora ubicada en la oficina del encargado
Dirección de Teatro		
Abreviatura del nombre del sistema	**DT/SGPP**	
Nombre del sistema	**Sistema General de Padrón de Profesionales**	
¿Cómo se resguardan los datos personales?	Físico ( ) Digital ( ). Ambos (X)	
	Tipo de soporte	Físico ( ) Digital ( ) Ambos (X)
	¿Dónde se aloja?	Computadora ( ) Servidor (X) Nube ( ) Correo (X) Otros:
	Descripción de la información que se resguarda	- Documentos en PDF de Constancia de Situación Fiscal y Estado de Cuenta Bancario
	Características del lugar donde se resguarda la información	Computadora ubicada en la oficina del encargado

Dirección de Teatro		
Abreviatura del nombre del sistema	**DT/SFD**	
Nombre del sistema	**Sistema de Factura Digital**	
¿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 ( ) Otros:
	Descripción de la información que se resguarda	- Convocatorias - Acuses de registro - Cédula de evaluación
	Características del lugar donde se resguarda la información	- Archiveros tradicionales de metal, ubicados dentro de cada oficina con iluminación artificial y natural. - Computadoras ubicadas en las oficinas de cada usuario - Carpetas de control en equipo

Dirección de Teatro		
Abreviatura del nombre del sistema	**DT/SIC**	
Nombre del sistema	**Sistema Institucional de Compras**	
¿Cómo se resguardan los datos personales	Físico ( ) Digital ( ). Ambos (X)	
	Tipo de soporte	Físico ( ) Digital ( ) Ambos (X)
	¿Dónde se aloja?	Computadora (X) Servidor (X) Nube (X) Correo (X) Otros: - Expediente físicos en archiveros. - Sistema administrado por la Dirección General de Proveeduría
	Descripción de la información que se resguarda	- Solicitudes - Cotización - Factura - Bóveda fiscal - Forma múltiple - Órden de compra - Cheque - Poliza de cheque
	Características del lugar donde se resguarda la información	- Archiveros tradicionales de metal, ubicados dentro de cada oficina con iluminación artificial y natural. - Computadoras ubicadas en las oficinas de cada usuario - Carpetas de control en cada equipo, cada quien tiene su cuenta de usuario para acceder.
Dirección de Teatro		
Abreviatura del nombre del sistema	**DT/SIAF**	
Nombre del sistema	**Sistema Integral de Administración Financiera**	
¿Cómo se resguardan los datos personales?	Físico ( ) Digital ( ). Ambos (X)	
	Tipo de soporte	Físico ( ) Digital ( ) Ambos (X)
	¿Dónde se aloja?	Computadora (X) Servidor (X) Nube ( ) Correo ( ) Otros:
	Descripción de la información que se resguarda	- Tabla de contenido con datos del proveedor, trabajador, becario, etc.
	Características del lugar donde se resguarda la información	- Computadora ubicada en la oficina del responsable
Dirección de Teatro		
Abreviatura del nombre del sistema	**DT/UPA**	
Nombre del sistema	**Unidad de Procesos Administrativos**	
¿Cómo se resguardan los datos personales?	Físico ( ) Digital ( ). Ambos (X)	
	Tipo de soporte	Físico ( ) Digital ( ) Ambos (X)

	¿Dónde se aloja?	Computadora (X) Servidor (X) Nube (X) Correo (X) Otros: Expedientes físicos en archiveros
	Descripción de la información que se resguarda	- Formas múltiples - Factura - Contrarecibos - Comprobante de pago DGF - Convenio, contrato, datos bancarios en el caso de extranjeros (dependiendo la operación) - Contrarecibo complemento de pago
	Características del lugar donde se resguarda la información	- Archiveros tradicionales de metal, ubicados dentro de cada oficina con iluminación artificial y natural. - Computadoras ubicadas en las oficinas de cada responsable
Dirección de Teatro		
Abreviatura del nombre del sistema	**DT/SPPC**	
Nombre del sistema	**Sistema de Padrón de Proveedores y Contratistas**	
¿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 ( ) Otros: Expedientes físicos en archiveros
	Descripción de la información que se resguarda	- Factura - Contrarecibos - Comprobante de pago DGF
	Características del lugar donde se resguarda la información	- Archiveros tradicionales de metal, ubicados dentro de cada oficina con iluminación artificial y natural. - Computadoras ubicadas en las oficinas de cada encargado

ANEXO 3.

FUNCIONES Y OBLIGACIONES DE QUIENES TRATEN DATOS PERSONALES

Dirección de Teatro						
Abreviatura del nombre del sistema	**DT/EDPAC**					
Nombre del sistema	**Estímulos al Desempeño del Personal Administrativo de Confianza**					
ACTIVIDADES	**DG**	**JA**	**JD**	**UA**	**RDP**	**AP**
Guardar información de los documentos recibidos en el sistema de gestión					X	
Notificar la obtención de los documentos para iniciar el trámite de asignación de estímulos al personal administrativo de confianza		X	X			
Consultar la información de datos personales en el correo institucional		X	X	X		
Dar seguimiento al trámite de asignación del estímulo		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	
Guardar los documentos enviados por los titulares de los datos personales en el archivo físico y/o 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	
Mantener equipos de trabajo libres de documentos con datos personales	X	X	X	X	X	
Proteger los datos personales relativos al área universitaria contenidos en el sistema de accesos no autorizados	X	**X**	**X**	X	X	
Mantener actualizado el sistema de gestión					X	
Dictar políticas para el aseguramiento de los datos personales en la DT					X	
Dar capacitación en materia de protección de datos personales					X	
Proteger el archivo físico de la DT de accesos no autorizados	X	X	X	X	X	
Dirección de Teatro						
Abreviatura del nombre del sistema	**DT/SCP**					
Nombre del sistema	**Sistema de Comprobante de Pago**					
ACTIVIDADES	**DG**	**JA**	**JD**	**UA**	**RDP**	**AP**
Guardar información de los documentos recibidos en el sistema de gestión					X	
Notificar la obtención de los documentos para iniciar con los movimientos en personal		X	X	X		

Consultar la información de datos personales en el correo institucional		X	X	X		
Dar seguimiento a los trámites en el SIP		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	
Guardar los documentos enviados por los titulares de los datos personales en el archivo físico y/o 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	
Mantener equipos de trabajo libres de documentos con datos personales	X	X	X	X	X	
Proteger los datos personales relativos al área universitaria contenidos en el sistema de accesos no autorizados	X	X	X	X	X	
Mantener actualizado el sistema de gestión					X	
Dictar políticas para el aseguramiento de los datos personales en la DT					X	
Dar capacitación en materia de protección de datos personales					X	
Proteger el archivo físico de la DT de accesos no autorizados	X	X	X	X	X	
Dirección de Teatro						
Abreviatura del nombre del sistema	**DT/SCN**					
Nombre del sistema	**Sistema de Comprobación de Nómina**					
ACTIVIDADES	**DG**	**JA**	**JD**	**UA**	**RDP**	**AP**
Guardar información de los documentos recibidos en el sistema de gestión		X	X			
Notificar la obtención de los documentos para iniciar el trámite de pago		X	X			
Consultar la información de datos personales en el correo institucional		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	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/o digital		X	X	X		
Revisar los documentos entregados por los titulares de datos personales para detectar estos				X	X	
Hacer sugerencias al área universitaria para quitar, testar o clasificar la información de documentos entregados según sea el caso				X	X	
Mantener equipos de trabajo libres de documentos con datos personales	X	X	X	X	X	
Proteger los datos personales relativos al área universitaria contenidos en el sistema de accesos no autorizados				X	X	
Mantener actualizado el sistema de gestión				X	X	
Dictar políticas para el aseguramiento de los datos personales en la DT				X		
Dar capacitación en materia de protección de datos personales				X	X	
Proteger el archivo físico de la DT de accesos no autorizados	X	X	X	X	X	
Dirección de Teatro						
Abreviatura del nombre del sistema	**DT/SIPH**					
Nombre del sistema	**Sistema Integral de Personal**					
ACTIVIDADES	**DG**	**JA**	**JD**	**UA**	**RDP**	**AP**
Guardar información de los documentos recibidos en el sistema de gestión					X	
Notificar la obtención de los documentos para llevar el control del presupuesto		X	X	X		
Consultar la información de datos personales en el correo institucional		X	X	X		
Dar seguimiento a la gestión del presupuesto asignado		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	

Guardar los documentos enviados por los titulares de los datos personales en el archivo físico y/o 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	
Mantener equipos de trabajo libres de documentos con datos personales	X	X	X	X	X	
Proteger los datos personales relativos al área universitaria contenidos en el sistema de accesos no autorizados	X	X	X	X	X	
Mantener actualizado el sistema de gestión					X	
Dictar políticas para el aseguramiento de los datos personales en la DT		X	X	X		
Dar capacitación en materia de protección de datos personales					X	
Proteger el archivo físico de la DT de accesos no autorizados	X	X	X	X	X	
Dirección de Teatro						
Abreviatura del nombre del sistema	**DT/SIPFUE**					
Nombre del sistema	**Sistema Integral de Personal Forma Única Electrónica**					
ACTIVIDADES	**DG**	**JA**	**JD**	**UA**	**RDP**	**AP**
Guardar información de los documentos recibidos en el sistema de gestión					X	
Notificar la obtención de los documentos para iniciar con los movimientos en personal		X	X	X		
Consultar la información de datos personales en el correo institucional		X	X	X		
Dar seguimiento a los trámites en el SIP		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	
Guardar los documentos enviados por los titulares de los datos personales en el archivo físico y/o 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	
Mantener equipos de trabajo libres de documentos con datos personales	X	X	X	X	X	
Proteger los datos personales relativos al área universitaria contenidos en el sistema de accesos no autorizados	X	X	X	X	X	
Mantener actualizado el sistema de gestión					X	
Dictar políticas para el aseguramiento de los datos personales en la DT					X	
Dar capacitación en materia de protección de datos personales					X	
Proteger el archivo físico de la DT de accesos no autorizados	X	X	X	X	X	
Dirección de Teatro						
Abreviatura del nombre del sistema	**DT/SGPP**					
Nombre del sistema	**Sistema General de Padrón de Profesionales**					
ACTIVIDADES	**DG**	**JA**	**JD**	**UA**	**RDP**	**AP**
Guardar información de los documentos recibidos en el sistema de gestión					X	
Notificar la obtención de los documentos para dar de alta a un proveedor y pagarle		X	X			
Consultar la información de datos personales en el correo institucional		X	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	
Guardar los documentos enviados por los titulares de los datos personales en el archivo físico y/o 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	

Mantener equipos de trabajo libres de documentos con datos personales	X	X	X	X	X	
Proteger los datos personales relativos al área universitaria contenidos en el sistema de accesos no autorizados	X	X	X	X	X	
Mantener actualizado el sistema de gestión					X	
Dictar políticas para el aseguramiento de los datos personales en la DT					X	
Dar capacitación en materia de protección de datos personales					X	
Proteger el archivo físico de la DT de accesos no autorizados	X	X	X	X	X	
Dirección de Teatro						
Abreviatura del nombre del sistema	**DT/SFD**					
Nombre del sistema	Sistema de Factura Digital					
ACTIVIDADES	**DG**	**JA**	**JD**	**UA**	**RDP**	**AP**
Guardar información de los documentos recibidos en el sistema de gestión					X	
Notificar la obtención de los documentos para iniciar el trámite de pago		**X**	X			
Consultar la información de datos personales en el correo institucional		**X**	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	
Guardar los documentos enviados por los titulares de los datos personales en el archivo físico y/o 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	
Mantener equipos de trabajo libres de documentos con datos personales	X	**X**	X	X	X	X
Proteger los datos personales relativos al área universitaria contenidos en el sistema de accesos no autorizados	X	**X**	X	X	X	X
Mantener actualizado el sistema de gestión					X	
Dictar políticas para el aseguramiento de los datos personales en la DT					X	

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

Dirección de Teatro						
Abreviatura del nombre del sistema	**DT/SIC**					
Nombre del sistema	**Sistema Institucional de Compras**					
ACTIVIDADES	**DG**	**JA**	**JD**	**UA**	**RDP**	**AP**
Guardar información de los documentos recibidos en el sistema de gestión		X	X			
Notificar la obtención de los documentos para iniciar el trámite de pago		X	X			
Consultar la información de datos personales en el correo institucional		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	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/o digital		X	X	X		
Revisar los documentos entregados por los titulares de datos personales para detectar estos				X	X	
Hacer sugerencias al área universitaria para quitar, testar o clasificar la información de documentos entregados según sea el caso				X	X	
Mantener equipos de trabajo libres de documentos con datos personales	X	X	X	X	X	X
Proteger los datos personales relativos al área universitaria contenidos en el sistema de accesos no autorizados				X	X	
Mantener actualizado el sistema de gestión				X	X	

Dictar políticas para el aseguramiento de los datos personales en la DT				X		
Dar capacitación en materia de protección de datos personales				X	X	
Proteger el archivo físico de la DT de accesos no autorizados	X	X	X	X	X	X
Dirección de Teatro						
Abreviatura del nombre del sistema	**DT/SIAF**					
Nombre del sistema	**Sistema Integral de Administración Financiera**					
ACTIVIDADES	**DG**	**JA**	**JD**	**UA**	**RDP**	**AP**
Guardar información de los documentos recibidos en el sistema de gestión					X	
Notificar la obtención de los documentos para llevar el control del presupuesto		X	X	X		
Consultar la información de datos personales en el correo institucional		X	X	X		
Dar seguimiento a la gestión del presupuesto asignado		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	
Guardar los documentos enviados por los titulares de los datos personales en el archivo físico y/o 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	
Mantener equipos de trabajo libres de documentos con datos personales	X	X	X	X	X	
Proteger los datos personales relativos al área universitaria contenidos en el sistema de accesos no autorizados	X	X	X	X	X	
Mantener actualizado el sistema de gestión					X	
Dictar políticas para el aseguramiento de los datos personales en la DT		X	X	X		

Dar capacitación en materia de protección de datos personales					X	
Proteger el archivo físico de la DT de accesos no autorizados	X	X	X	X	X	
Dirección de Teatro						
Abreviatura del nombre del sistema	**DT/UPA**					
Nombre del sistema	**Unidad de Procesos Administrativos**					
ACTIVIDADES	**DG**	**JA**	**JD**	**UA**	**RDP**	**AP**
Guardar información de los documentos recibidos en el sistema de gestión					X	
Notificar la obtención de los documentos para iniciar el trámite de pago		**X**	X			
Consultar la información de datos personales en el correo institucional		**X**	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	
Guardar los documentos enviados por los titulares de los datos personales en el archivo físico y/o 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	
Mantener equipos de trabajo libres de documentos con datos personales	X	**X**	X	X	X	
Proteger los datos personales relativos al área universitaria contenidos en el sistema de accesos no autorizados	X	**X**	X	X	X	
Mantener actualizado el sistema de gestión					X	
Dictar políticas para el aseguramiento de los datos personales en la DT					X	
Dar capacitación en materia de protección de datos personales					X	
Proteger el archivo físico de la DT de accesos no autorizados	X	**X**	X	X	X	
Mantener actualizado el sistema de gestión					X	
Dictar políticas para el aseguramiento de los datos personales en la DT					X	
Dar capacitación en materia de protección de datos personales					X	
Proteger el archivo físico de la DT de accesos no autorizados	X	**X**	X	X	X	
Dirección de Teatro						

Abreviatura del nombre del sistema	**DT/SPPC**					
Nombre del sistema	**Sistema de Padrón de Proveedores y Contratistas**					
ACTIVIDADES	**DG**	**JA**	**JD**	**UA**	**RDP**	**AP**
Guardar información de los documentos recibidos en el sistema de gestión					X	
Consultar la información de datos personales en el correo institucional		**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	
Guardar los documentos enviados por los titulares de los datos personales en el archivo físico y/o 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	
Mantener equipos de trabajo libres de documentos con datos personales	X	**X**	X	X	X	
Proteger los datos personales relativos al área universitaria contenidos en el sistema de accesos no autorizados	X	**X**	X	X	X	
Mantener actualizado el sistema de gestión					X	
Dictar políticas para el aseguramiento de los datos personales en la DT					X	
Dar capacitación en materia de protección de datos personales					X	
Proteger el archivo físico de la DT de accesos no autorizados	X	**X**	X	X	X	
Mantener actualizado el sistema de gestión					X	
Dictar políticas para el aseguramiento de los datos personales en la DT					X	
Dar capacitación en materia de protección de datos personales					X	
Proteger el archivo físico de la DT de accesos no autorizados	X	**X**	X	X	X	

DG – Director General
JD – Jefaturas de departamento
UA – Unidad Administrativa
JA – Jefe de Área

SG – Servicios Generales
AP – Asistente de Procesos
RDP – Responsables de Datos Personales

Dirección de Teatro						
FUNCIONES DENTRO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES						
ACTIVIDADES	**DG**	**JA**	**JD**	**AP**	**UA**	**RDP**
Elaborar políticas y objetivos del SGSDP					X	
Aprobar políticas y objetivos del SGSDP	X					
Asignar funciones y obligaciones	X				X	
Elaborar inventario de datos personales	X	X	X	X	X	X
Realizar análisis de riesgos de los datos personales		X	X		X	X
Realizar análisis 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

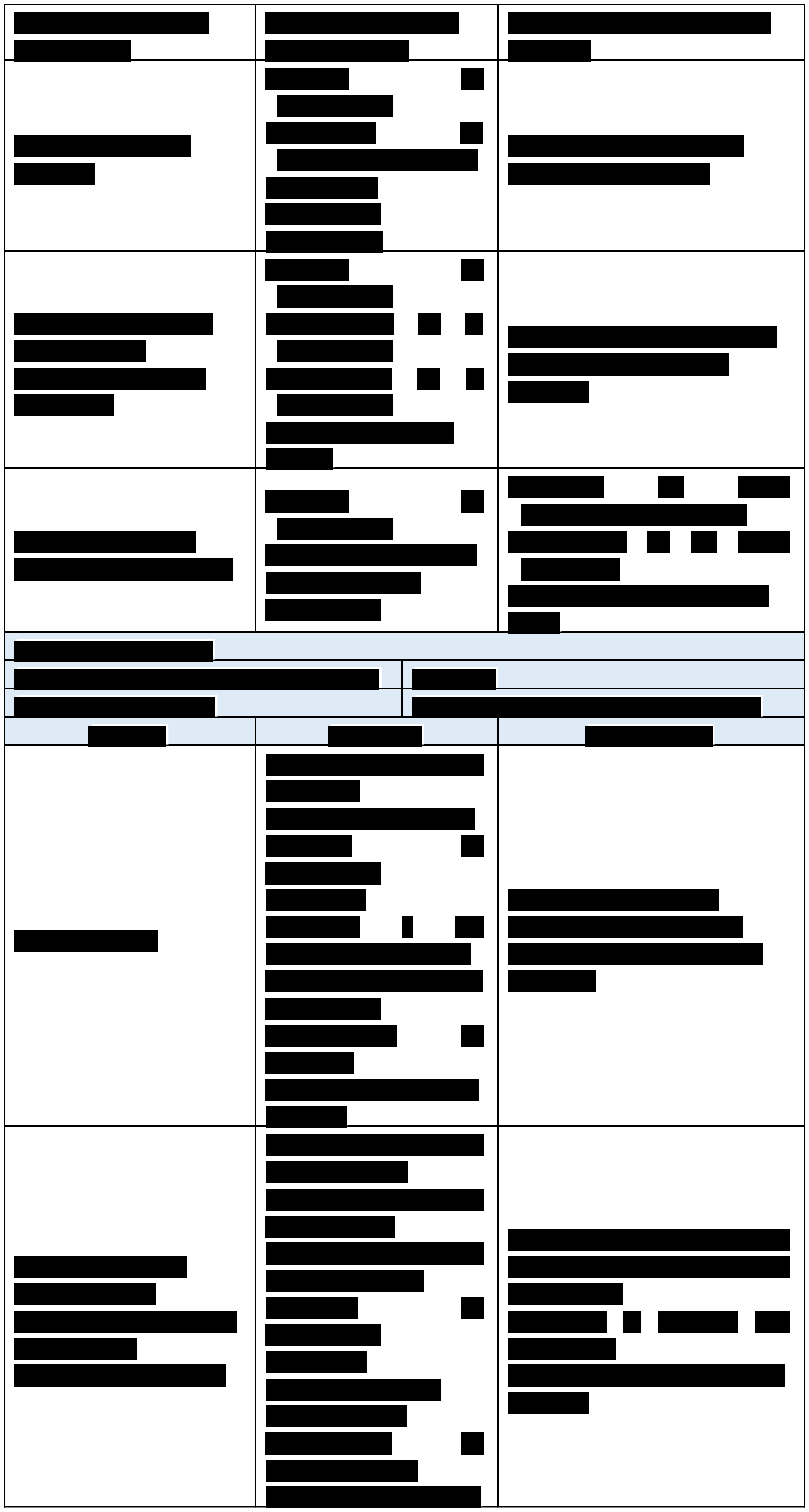
Dirección de Teatro						
MATRÍZ DE RENDICIÓN DE CUENTAS						
ÁREAS	**DG**	**JA**	**JD**	**AP**	**UA**	**SG**
Jefes de Departamento	X				X	
Asistente de Procesos	X				X	
Unidad Administrativa	X				X	
Jefe de Área	X				X	

DG – Director General
JD – Jefaturas de departamento
UA – Unidad Administrativa
JA – Jefe de Área
AP – Asistente de Procesos
RDP – Responsables de Datos Personales

ANEXO 4.

ANÁLISIS DE RIESGOS

[redacted]



[redacted]

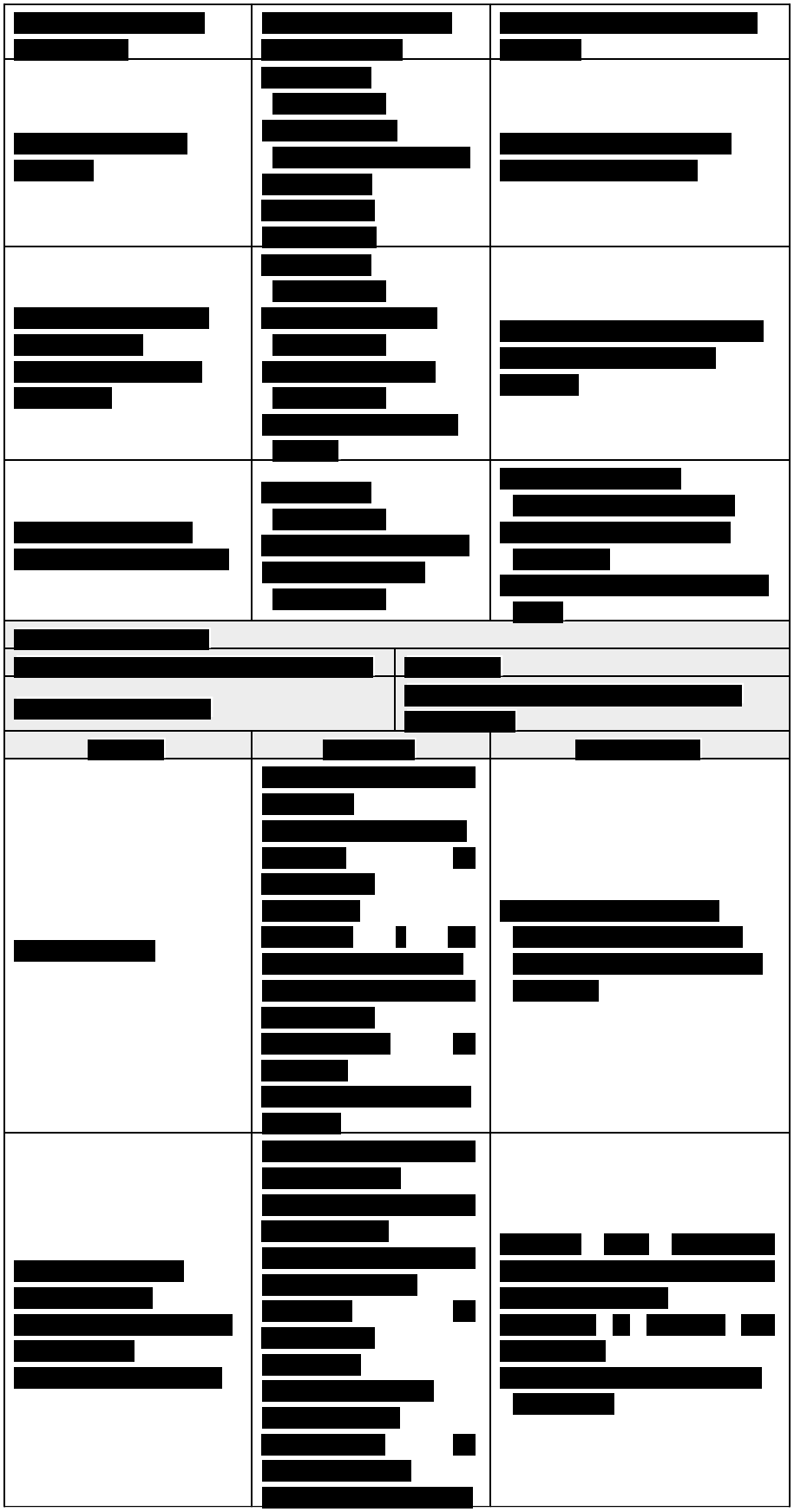
[redacted]

[redacted]

[redacted]

[redacted]

[redacted]



ANEXO 5.

ANÁLISIS DE BRECHA Y MEDIDAS DE SEGURIDAD

[redacted]

[redacted]		
[redacted]	[redacted]	
[redacted]	[redacted]	
[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

ANEXO 6.

PLAN DE TRABAJO

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

ANEXO 7.

Capacitación Administrativa Básica

CAPACITACIÓN ADMINISTRATIVA BÁSICA	
Dirección de Teatro	
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			DT	
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			

NO APLICA			DT	
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			

NO APLICA			DT	
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">EDPAC, SCP, SCN, SIPH, SIPFUE, SGPP, SFD, SIC, SIAF, UPA, SPPC</td><td colspan="2">DT</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="4">Ejecución</td><td>Fecha inicio</td></tr>
<tr><td colspan="4">José Antonio Valdez Cruz</td><td>15/08/2022</td></tr>
<tr><td colspan="4">Nombre y firma
Administrador del sistema de información o servidor</td><td>Fecha término</td></tr>
<tr><td colspan="4"></td><td></td></tr>
<tr><td>Observaciones / anotaciones</td><td colspan="4"></td></tr>
</table>

Acciones Realizadas
Se cuenta con un plan de respaldo de información para las diferentes áreas sustantivas, donde se ejecutan las siguientes actividades:

1. Respaldos periódicos de los equipos en donde se almacene datos personales.
2. Supervisar que se realicen adecuadamente los respaldos de información en todas las áreas.
3. Respaldos del correo institucional de los usuarios.
4. Respaldo periódicos de archivos y bases de datos del o los servidores.
5. Realizar procesos de restauración de respaldos, cuando así se requiera.
6. Desarrollar políticas de respaldos.

EDPAC, SCP, SCN, SIPH, SIPFUE, SGPP, SFD, SIC, SIAF, UPA, SPPC			DT	
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**	
José Antonio Valdez Cruz 			15/08/2022	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

Acciones Realizadas

1. Aplicar procedimientos de borrado seguro de documentos y respaldos.
2. Supervisar que se realicen adecuadamente los procedimientos de borrado.
3. Ocupar los medios y herramientas que garanticen el borrado seguro de información.
4. Aplicar los procesos efectivos para el borrado de información de los equipos que se disponen a dar de baja.

<table>
<tr><td colspan="3">NO APLICA</td><td colspan="2">DT</td></tr>
<tr><td>Formato:</td><td>6</td><td>Verificación anual</td><td>Acción concluida</td><td>( )</td></tr>
<tr><td>Medidas de seguridad técnicas:</td><td colspan="4">Artículo 18. II. a) Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM</td></tr>
<tr><td>Aplicable en:</td><td colspan="4">II. Sistemas operativos y servicios.</td></tr>
<tr><td>Tiempo estimado:</td><td colspan="4">Un día hábil.</td></tr>
<tr><td>Importancia de la acción:</td><td colspan="4">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>Proceso recomendado:</td><td colspan="4">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>Mejores prácticas, referencias:</td><td colspan="4">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>Conocimientos requeridos:</td><td colspan="4">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">NO APLICA</td></tr>
</table>

Equipos de la Dirección de Teatro			DT	
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**	
José Antonio Valdez Cruz 			15/08/2022	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

Acciones Realizadas

1. Se identifica los tipos de sistemas para aplicar la herramienta seguridad correspondiente.
2. Actualización de herramienta antimalware en los equipos.
3. Mantener bitácora de incidentes.
4. Se aplican las herramientas de antimalware para protección contra vulnerabilidades de los sistemas.
5. Se siguen las recomendaciones de DGTIC, para mejorar las protección en los equipos.
6. Se desarrollan estrategias de seguridad de redes multi capa, a partir de una defensa de profundidad.

Equipos de la Dirección de Teatro			DT	
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**	
José Antonio Valdez Cruz 			15/08/2022	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

Acciones Realizadas

1. Actualización de parches de seguridad en los sistemas.
2. Supervisión de las actualizaciones de sistema cada semana.
3. Mantener actualizados la versión de sistema.
4. Identificar aplicaciones no autorizadas, para mantener el buen funcionamiento del sistema.
5. Se siguen las recomendaciones de DGTIC.
6. Revisión de procesos para lograr un rendimiento optimo en los sistemas y equipo de cómputo.

EDPAC, SCP, SCN, SIPH, SIPFUE, SGPP, SFD, SIC, SIAF, UPA, SPPC			DT	
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**	
José Antonio Valdez Cruz 			15/08/2022	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

Acciones Realizadas

1. Los usuarios responsables y encargados, tienen los privilegios necesarios para realizar las actividades que les corresponde para cada aplicación que manejan.
2. Se tiene un control de accesos para cada usuario de los sistemas que se manejan.
3. Se revisa periódicamente los privilegios de acceso a los sistemas.

EDPAC, SCP, SCN, SIPH, SIPFUE, SGPP, SFD, SIC, SIAF, UPA, SPPC			DT	
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**	
José Antonio Valdez Cruz 			15/08/2022	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

Acciones Realizadas

1. Se revisa periódicamente los procesos, para identificar los de alto consumo.
2. Revisión periódica del administrador de programas, para identificar aquellos que puedan afectar el funcionamiento del sistema.
3. Desinstalar aplicaciones desconocidas que afecten el funcionamiento del sistema y equipo.
4. Aplicar privilegios de instalación de programas o aplicaciones.
5. Monitoreo de procesos de arranque e inicio.
6. Monitoreo de recursos en los equipos de cómputo.

EDPAC, SCP, SCN, SIPH, SIPFUE, SGPP, SFD, SIC, SIAF, UPA, SPPC			DT	
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 de la ubicación 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**	
José Antonio Valdez Cruz 			15/08/2022	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

Acciones Realizadas

1. Se tiene un circuito de cámaras, como medida de seguridad en el resguardo de los equipos de la Dirección de Teatro.
2. Se lleva un control de entrada y salida de equipo.
3. Los equipos de mayor impacto se tienen en oficinas.
4. Control de acceso al SAE.
5. Se atienden los incidentes de forma inmediata, relacionados con la seguridad física.
6. Se monitorean las condiciones y necesidades de seguridad física, para implementar las medidas que sean necesarias.

Equipos de la Dirección de Teatro			DT	
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**	
José Antonio Valdez Cruz			15/08/2022	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

Acciones Realizadas

1. Se controla en bitácora la entrada y salida de equipo de las instalaciones.
2. Se identifican los datos necesarios de los equipos en la entrada y salida.
3. Se cuenta con un control de salida del equipo que implique baja del inventario.
4. En el caso de baja del equipo, se realiza el borrado seguro de información, como medida de seguridad.

NO APLICA			DT	
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			

<table>
<tr><td colspan="3">EDPAC, SCP, SCN, SIPH, SIPFUE, SGPP, SFD, SIC, SIAF, UPA, SPPC</td><td colspan="2">DT</td></tr>
<tr><td>Formato:</td><td>14</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 20. Aplicar el procedimiento de borrado seguro que impida la recuperación en las bases de datos y todos sus respaldos.</td></tr>
<tr><td colspan="2">Aplicable en:</td><td colspan="3">Bases de datos y sistemas de tratamiento.</td></tr>
<tr><td colspan="2">Tiempo estimado:</td><td colspan="3">Tres días hábiles.</td></tr>
<tr><td colspan="2">Importancia de la acción:</td><td colspan="3">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).</td></tr>
<tr><td colspan="2">Proceso recomendado:</td><td colspan="3">A) Realizar una copia integral del sistema de información y colocarla en un servicio temporal. <u>Por ejemplo:</u> 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. <u>Por ejemplo</u>: 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.</td></tr>
<tr><td colspan="2">Mejores prácticas, referencias:</td><td colspan="3">1.- Se recomienda usar al menos un comando a nivel de sistema operativo para el borrado seguro de conformidad con el procedimiento establecido.</td></tr>
<tr><td colspan="2">Conocimientos requeridos:</td><td colspan="3">Administración de sistema operativo. Instalación de aplicaciones. Gestión de archivos.</td></tr>
<tr><td colspan="3">Ejecución</td><td colspan="2">Fecha inicio</td></tr>
<tr><td colspan="3">José Antonio Valdez Cruz</td><td colspan="2">15/08/2022</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>

Acciones Realizadas

1. Se aplican los procedimientos necesarios para un borrado seguro de información.
2. Se realizan copias de aquellas bases de datos, para realizar el borrado seguro que corresponde.
3. Las recomendaciones de DGTIC de borrado seguro, se toman en cuenta como apoyo y buenas prácticas de estos procedimientos.
4. Para el método de borrado seguro, se aplican herramientas para una eliminación permanente de información.

POLÍTICAS

POLÍTICAS PARA LA PROTECCIÓN DE DATOS PERSONALES

En todo tratamiento de datos personales que se realice en la DT, 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.

---

[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*

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.

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 DT 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 DT, 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 DT.

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 DT 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 DT 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 DT 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 DT 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 DT 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 DT 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 DT 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 DT 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 DT.

Al respecto, de conformidad con los artículos 59 a 62 de la Ley General y 108 a 110 de los Lineamientos Generales, la DT 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 DT 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 DT 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 DT, 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 DT 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 DT 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 DT 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 DT 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 DT 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 DT 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 DT 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 DT 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 DT 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 DT.

En ningún caso, la DT 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 DT deberá verificar el cumplimiento de lo estipulado en las "Políticas para la Remisión de Datos Personales"; es decir, además de observar las obligaciones señaladas, deberá

[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.

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 DT 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 DT 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 DT 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 DT, 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 DT así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
- Permitir y colaborar con la DT 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 DT, 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 DT 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 DT. 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 DT deberá contar con una cuenta de correo electrónico institucional.

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 a la Jefa de Unidad Administrativa de la DT y no a través de terceros.

6. El Director de Teatro, será quien podrá solicitar a la Jefa de Unidad Administrativa el alta de un usuario en el servicio de correo electrónico institucional.

7. El nombre de usuario es asignado por la Jefa de Unidad administrativa, 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 DT, a través de la Unidad Administrativa 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 la Jefa de Unidad Administrativa.

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 del 19 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, en relación con los artículos 247 y 248 de los 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. Las Reglas 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.