Dirección General de Publicaciones y Fomento Editorial

Oficio DGPYFE/DG/487/2022

Asunto: Reserva de Documento de seguridad para la Verificación del INAI relativo al *Apartado Virtual de datos personales de la UNAM*

Dr. Alfredo Sánchez Castañeda
Presidente del Comité de Transparencia de la UNAM

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

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

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

A efecto de cumplir con lo señalado, se realiza la siguiente prueba de daño relativa al documento de seguridad de datos personales que obran en el Sistema de Gestión de Seguridad de Datos Personales de esta área universitaria. El documento de seguridad contiene los siguientes apartados cuya autorización de reserva total se solicita a ese Comité:

Anexos o Políticas	Contenido y su afectación	Páginas
a) Análisis de riesgos	El análisis de riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica de esta área universitaria, y otorga herramientas a las personas para implementar un ataque informático a los activos críticos y no críticos.	**De la 71 a la 75**

[1] DOF: 26 de noviembre de 2021.

b) Análisis de brecha	El análisis de brecha integra información relativa a la seguridad de la infraestructura tecnológica; enlistan los controles de seguridad con los que cuenta esta área; y menciona las herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información.	**De la 76 a la95**
c) Plan de Trabajo	El plan de trabajo define los controles de seguridad a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes con base en el riesgo real detectado. El uso de esta información permite inferir nuestros riesgos, por cuánto tiempo seguirán así hasta el momento en que se implementen nuevos controles.	**De la 96 a la 101**

Los fundamentos y motivos se exponen a continuación:

- Existe un *riesgo real, demostrable e identificable* en perjuicio del nexo causal que prevé la hipótesis de reserva ahora analizada contemplada en los artículos 113, fracción VII, y 110, fracción VII, de las Leyes General y Federal de Transparencia y Acceso a la Información Pública, respectivamente, pues los documentos consistentes en análisis de riesgo, el análisis de brecha, las políticas de respaldo y el plan de trabajo de esta dependencia contienen información de cómo se protegen los datos personales de los titulares que nos confiaron su información personal y que es nuestra responsabilidad garantizar. Es un riesgo real el hecho de que toda persona que quiera ocasionar la pérdida, destrucción, robo, copia, uso, acceso o tratamiento no autorizado, daño, alteración o modificación no autorizada de datos personales, puede hacerlo si cuenta con la información exacta de las vulnerabilidades de un área universitaria, lo que esta serie de documentos les otorga directamente si se difundiera la información.

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

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

La prueba de daño precitada, además de colmar los extremos establecidos en los numerales 97 y 111 de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con el 104 de la Ley General de Transparencia y Acceso a la Información Pública; también se realiza de conformidad con el Vigésimo Sexto de *los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información así como para la elaboración de versiones públicas,* donde se prevé que podrá considerarse como información reservada, aquélla que obstruya la prevención de delitos al obstaculizar las acciones implementadas por las autoridades para evitar su comisión, o menoscabar o limitar la capacidad de las autoridades para evitar la comisión de delitos.

En esa inteligencia, el dar a conocer el análisis de riesgo, el análisis de brecha y el plan de trabajo de esta área universitaria, no podrían prevenirse actos ilícitos que pudieran realizarse en contra de los sistemas de información y tratamiento de datos personales, así como en contra de los activos e infraestructura crítica de esta dependencia; por lo que es posible advertir que algunas de las posibles

consecuencias de divulgar dicha información podrían derivar en la comisión de diversos delitos tipificados en el Código Penal Federal, como accesos no autorizados a los sistemas, robos de información, suplantación de identidades, entre otros. Es decir, se advierte que la negativa de acceso a la información se motiva en evitar o prevenir la comisión del delito al vulnerar las medidas de seguridad establecidas por esta Área Universitaria, con relación al cumplimiento de los principios de protección de datos personales previsto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

En tal sentido, proteger la información de los documentos relativos al análisis de riesgo, al análisis de brecha y al plan de trabajo de esta área se adecua al principio de proporcionalidad porque se justifica negar su divulgación, toda vez que la pretensión de fondo que persigue la reserva de la información consiste en prevenir las conductas antijurídicas tipificadas, aunado a que la restricción es temporal, hasta en tanto las medidas tomadas caduquen; de igual manera, con la no divulgación de la información se contribuye a garantizar la protección de los datos personales de no solo la comunidad universitaria sino de cualquiera que ponga la confianza en esta Universidad para resguardar sus datos personales.

Por tales motivos, respetuosamente, se propone la reserva total de cada uno de esos documentos, que obran como anexos y políticas del documento de seguridad de esta área universitaria, por un periodo de 5 años, de conformidad con los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

En virtud de lo anterior, le solicito de la manera más atenta que ese Cuerpo Colegiado tenga a bien emitir la resolución que en derecho corresponda, para lo cual se adjunta la documentación completa.

Sin otro particular, reciba un cordial saludo.

A t e n t a m e n t e
"Por Mi Raza Hablará el Espíritu"
Ciudad Universitaria, a 16 de agosto de 2022
La Directora

Mtra. Socorro Venegas

c.c.p. Lic. Jorge Barrera Gutiérrez. Secretario Técnico del Comité. Presente.
Mtro. David Gómez Gaytán. Jefe de Unidad Administrativa de la DGPYFE
Mtra. Karen Hernández Negrete. Coordinadora de Sistemas de la DGPYFE

SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES

DIRECCIÓN GENERAL DE PUBLICACIONES Y FOMENTO EDITORIAL

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 Público1 (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 General de Publicaciones y Fomento Editorial (DGPyFE), así como, identificar los sistemas de datos personales que posee, el tipo de datos que contiene cada uno, los responsables, encargados, usuarios de cada sistema y las medidas de seguridad implementadas.

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

La Dirección General de Publicaciones y Fomento Editorial (DGPyFE), adscrita a la Coordinación de Difusión Cultural, tiene como principales objetivos promover y difundir el sello editorial universitario, perfeccionar la actividad editorial de la institución, así como distribuir y comercializar la producción editorial de nuestra casa de estudios. Forma parte del sistema editorial universitario al ser la distribuidora central de la UNAM, la representante en ferias nacionales e internacionales y la encargada de impulsar la profesionalización de los agentes que intervienen en la producción y distribución de las publicaciones universitarias. Es una dependencia de apoyo y de servicio para las diversas instancias editoras universitarias, la editora de la administración central y, además, la Secretaría Técnica del Consejo Editorial de la UNAM.

Misión
Difundir, distribuir y comercializar la producción editorial de la UNAM y contribuir con la extensión de la cultura a la comunidad universitaria y la sociedad en general.

Visión
Agrupar con eficiencia la producción editorial de la UNAM mediante sistemas de información que garanticen la transparencia y la operación de esta dependencia. Difundir y comercializar dentro y fuera del territorio nacional nuestra producción editorial y convertirnos en referente por la calidad editorial de nuestras publicaciones y de nuestras librerías; propiciar la permanente evaluación y procurar una mejora constante y sostenida.

Objetivo
Publicar, distribuir y comercializar la producción editorial de la UNAM, así como concentrar la información del ramo para difundirla entre la comunidad universitaria y la sociedad en general, con el fin de generar acercamientos entre autores, editores, libreros, bibliotecas, lectores, estudiosos e investigadores.

ABREVIATURAS Y DENOMINACIONES

UNAM – Universidad Nacional Autónoma de México

DGPyFE – Dirección General de Publicaciones y Fomento Editorial

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

SGSDP – Sistema de Gestión de Seguridad de Datos Personales

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

MP – Ministerio Público

TE – Tienda electrónica

FD – Factura Digital

SIC – Sistema Institucional de Compras

PPC – Padrón de Proveedores y Contratistas

SIAF – Sistema Integral de Administración Financiera

SGA - Papyrus

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 DGPyFE

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 DGPyFE.

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

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

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

Se pretende 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.

Dentro de la DGPyFE, quienes participan en el tratamiento de datos personales son los siguientes:

SISTEMA DE TIENDA ELECTRÓNICA (TE)

- Jefatura de cómputo
- Jefatura de comercialización
- Jefatura de la unidad administrativa
- Jefatura de revistas académicas y publicaciones digitales

SISTEMA DE FACTURACIÓN DIGITAL (FD)

- Jefatura de la unidad administrativa
- Jefatura del área de presupuesto
- Jefatura del área de contabilidad
- Jefatura de sistemas
- Jefatura de comercialización

SISTEMA INSTITUCIONAL DE COMPRAS (SIC)

- Dirección
- Jefatura de la unidad administrativa
- Jefatura del área de presupuesto
- Jefatura del área de contabilidad
- Jefatura de revistas académicas y publicaciones digitales
- Jefatura de comercialización
- Jefatura de sistemas
- Jefatura de editorial

PADRÓN DE PROVEEDORES Y CONTRATISTAS (PPC)

- Jefatura de la unidad administrativa

SISTEMA INTEGRAL DE ADMINISTRACIÓN FINANCIERA (SIAF)

- Jefatura de la unidad administrativa
- Jefatura del área de presupuesto

INTELISIS - PAPYRUS(SGA)

- Dirección
- Jefatura de la unidad administrativa
- Jefatura del área de presupuesto
- Jefatura del área de contabilidad
- Jefatura del departamento de personal
- Jefatura de comercialización
- Jefatura de sistemas
- Jefatura de editorial

- Jefatura de revistas académicas y publicaciones digitales
- Jefatura de almacén

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

Director. Supervisar que el SGSDP se cumpla de acuerdo al documento de seguridad.
Responsables. Verificar que el SGSDP se cumpla en sus áreas específicas de acuerdo al documento de seguridad.
Encargados. Mantener el SGSDP en sus áreas específicas de acuerdo al documento de seguridad.
Usuarios. Utilizar el SGSDP en sus áreas específicas de acuerdo al documento de seguridad.

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 DGPyFE.
- 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 DGPyFE.

Lo anterior se realiza tomando como base el OCTAVE Allegro Method3, 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 DGPyFE 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

[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.*

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

X

Área de Impacto	Prioridad	Valor de impacto	Puntaje
Reputación / Pérdida de confianza	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

X

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

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:

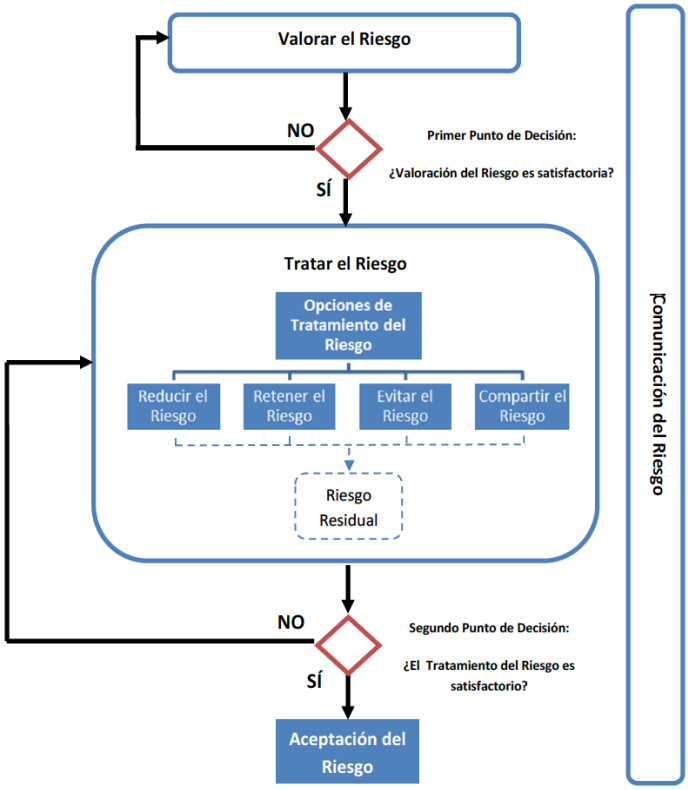
- Las medidas de seguridad existentes que operan correctamente;
- Las medidas de seguridad faltantes; y
- Las medidas de seguridad nuevas que puedan remplazar a las existentes

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.

PLAN DE TRABAJO

La DGPyFE 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.

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 período 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;

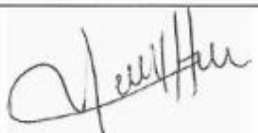
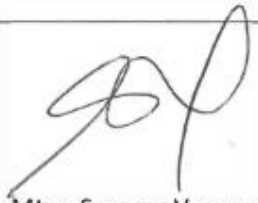
b) La legislación vigente en materia de protección de datos personales y mejores prácticas relacionadas al tratamiento de datos personales;
c) Las consecuencias del incumplimiento de los requerimientos legales o requisitos organizacionales;
d) Las herramientas tecnológicas relacionadas o utilizadas para el tratamiento de datos personales y para la implementación de medidas de seguridad.

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.

APROBACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES

		Nombre y firma de quienes revisaron el presente documento:
Responsable del desarrollo:	Mtro. David Gómez Gaytán Jefe de Unidad Administrativa de la DGPyFE Tel. 55 5622 6580 david.gomez@libros.unam.mx	 Mtro. David Gómez
Revisó:	Mtra. Karen Hernández Negrete Coordinadora de sistemas de la DGPyFE Tel. 55 5622 6575 karen.hernandez@libros.unam.mx	 Mtra. Karen Hernández Negrete
Autorizó:	Mtra. Socorro Venegas Directora General de la DGPyFE Tel. 55 5622 6570 svenegas@libros.unam.mx	 Mtra. Socorro Venegas
Fecha de aprobación:	(Incluir la fecha de liberación del documento)	CDMX, 16 de agosto de 2022
Fecha de actualización:	(Incluir la primer versión e ir agregando las subsiguientes del documento)	1.0

ANEXO 1

INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Dirección General de Publicaciones y Fomento Editorial			
Abreviatura del nombre del sistema	**TE**		
Nombre del sistema	**Tienda electrónica libros UNAM**		
Datos personales contenidos en el sistema	- Nombre completo del usuario - Correo electrónico - Domicilio particular - RFC - Teléfono particular - Datos bancarios		
Responsable del sistema			
Nombre:	Karen Hernández Negrete		
Cargo:	Coordinación de sistemas / DGPyFE UNAM		
Funciones:	Obtención (X) Uso (X) Registro ( ) Organización (X) Elaboración ( ) Conservación (X)	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento (X) Posesión (X) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 tienda electrónica de acuerdo a los permisos otorgados.		
Encargados del sistema			
Nombre encargado 1:	Marlene Fernández Martínez		
Cargo:	Asistente de procesos / DGPyFE UNAM		
Funciones:	Obtención (X) Uso (X) Registro () Organización (X) Elaboración ( ) Conservación (X)	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento (X) Posesión (X) Acceso (X)	Manejo (X) Aprovechamiento (X) Divulgación ( ) Transferencia ( ) Remisión ( ) Disposición ( )
Obligaciones:	- Guardar la confidencialidad de los datos personales. - Proteger los datos personales recibidos. - No modificar la información de datos personales contenidos en los documentos recibidos. - No difundir la información de datos personales contenidos en los documentos recibidos. - Mantener la información de datos personales en el archivo de la Unidad Administrativa. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Usuarios			
Nombre de usuario 1:	Alejandro Villaseñor Valerio		
Cargo:	Subdirector Comercial		
Funciones:	Obtención (X) Uso (X) Registro ( ) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 de usuario 2:	Laura Mariana Orozco		
Cargo:	Comercialización		
Funciones:	Obtención (X) Uso (X) Registro ( ) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 3:	Beatriz Vallarta Jiménez		
Cargo:	Jefa del Departamento de Catálogos		
Funciones:	Obtención (X) Uso (X) Registro ( ) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 4:	César Arturo Silva Castro		
Cargo:	Comercial		
Funciones:	Obtención (X) Uso (X) Registro ( ) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		

Nombre de usuario 5:	Magali Arámbula Morales		
Cargo:	Librería Palacio de Minería		
Funciones:	Obtención (X) Uso (X) Registro ( ) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 6:	Marisol Martínez		
Cargo:	Coordinadora de comunicación		
Funciones:	Obtención (X) Uso (X) Registro ( ) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Dirección General de Publicaciones y Fomento Editorial			
Abreviatura del nombre del sistema	**FD**		
Nombre del sistema	**Facturación digital**		
Datos personales contenidos en el sistema	- Nombre completo del usuario - Correo electrónico - Domicilio particular - RFC - Datos bancarios - País		
Responsable del sistema			
Nombre:	Karen Hernández Negrete		
Cargo:	Coordinación de sistemas / DGPyFE UNAM		
Funciones:	Obtención (X) Uso (X) Registro ( ) Organización (X) Elaboración ( ) Conservación (X)	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento (X) Posesión (X) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 mesa de ayuda de acuerdo a los permisos otorgados.		
Nombre:	David Gómez		
Cargo:	Unidad administrativa / DGPyFE UNAM		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación (X)	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento (X) Posesión (X) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 mesa de ayuda de acuerdo a los permisos otorgados.		
Encargados del sistema			
Nombre encargado 1:	Karen Hernández Negrete		
Cargo:	Coordinación de sistemas / DGPyFE UNAM		
Funciones:	Obtención (X) Uso (X) Registro ( ) Organización (X) Elaboración ( ) Conservación (X)	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento (X) Posesión (X) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 mesa de ayuda de acuerdo a los permisos otorgados.		
Nombre de usuario 1:	Alejandro Hernández Carmona		
Cargo:	Asistente de procesos		
Funciones:	Obtención (X) Uso (X) Registro ( ) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Usuarios			
Nombre de usuario 1:	Benjamín Villanueva Elías		
Cargo:	Administrador técnico		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración (X) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 2:	Ignacio Medina Leyva		
Cargo:	Responsable de Un Paseo por los Libros		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración (X) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 3:	Jorge Abrego Ugalde		
Cargo:	Jefe de ventas		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación (X)	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 4:	Luis Antonio Reyes Quezada		
Cargo:	Jefe de departamento de operación y control CxC		

Funciones:	Obtención (X) Uso (X) Registro ( ) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 5:	Ma. del Socorro Nava Martínez		
Cargo:	Encargada de la librería Palacio de Minería		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 6:	Ma. de la Luz Nazario Morales		
Cargo:	Coordinadora de comercialización		
Funciones:	Obtención (X) Uso (X) Registro ( ) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 7:	Norma Angelica Salazar Enciso		
Cargo:	Jefa departamento contabilidad		
Funciones:	Obtención (X) Uso (X) Registro ( ) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 8:	Oscar Santamaria González		
Cargo:	Jefe de desarrollo tecnológico		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración (X) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 9:	Víctor Manuel Sánchez Trejo		
Cargo:	Jefe de librería Jaime García Terrés		
Funciones:	Obtención (X) Uso (X) Registro ( ) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 10:	César Arturo Silva Castro		
Cargo:	Jefe del departamento de promoción y distribución de publicaciones		
Funciones:	Obtención (X) Uso (X) Registro ( ) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		

Nombre de usuario 11:	María Guadalupe Sánchez Hernández		
Cargo:	Jefa del departamento de operación y control		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración (X) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 12:	Virginia Palma Cortes		
Cargo:	Jefe administrativo		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración (X) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 13:	Leticia Pérez Ramírez		
Cargo:	Asistente de procesos		
Funciones:	Obtención (X) Uso (X) Registro ( ) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 14:	Magali Arámbula Morales		
Cargo:	Jefa de la librería Palacio de Minería		
Funciones:	Obtención (X) Uso (X) Registro ( ) Organización (X)	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( )	Manejo (X) Aprovechamiento (X) Divulgación ( ) Transferencia ( )

	Elaboración ( ) Conservación ( )	Posesión ( ) Acceso (X)	Remisión ( ) Disposición ( )
Obligaciones:	- Guardar la confidencialidad de los datos personales. - Proteger los datos personales recibidos. - No modificar la información de datos personales contenidos en los documentos recibidos. - No difundir la información de datos personales contenidos en los documentos recibidos. - Mantener la información de datos personales en el archivo de su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 15:	Manuel Mendoza Tirado		
Cargo:	Asistente de procesos		
Funciones:	Obtención (X) Uso (X) Registro ( ) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 16:	Pablo Javier Quezada García		
Cargo:	Jefe de departamento		
Funciones:	Obtención (X) Uso (X) Registro ( ) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 17:	Silvia Natalia Pérez Monrroy		
Cargo:	Asistente de procesos		
Funciones:	Obtención (X) Uso (X) Registro ( ) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área.		

	- No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 18:	Luz Elena Silva Guerrero		
Cargo:	Jefe de departamento		
Funciones:	Obtención (X) Uso (X) Registro ( ) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 19:	Marcos Mancera Reyes		
Cargo:	Jefe de presupuesto		
Funciones:	Obtención (X) Uso (X) Registro ( ) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Dirección General de Publicaciones y Fomento Editorial			
Abreviatura del nombre del sistema	**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 del sistema			
Nombre:	Karen Hernández Negrete		
Cargo:	Coordinación de sistemas / DGPyFE UNAM		
Funciones:	Obtención (X) Uso (X) Registro ( ) Organización (X) Elaboración ( ) Conservación (X)	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento (X) Posesión (X) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 tienda electrónica de acuerdo a los permisos otorgados.		
Nombre:	David Gómez		
Cargo:	Unidad administrativa / DGPyFE UNAM		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración (X) Conservación (X)	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento (X) Posesión (X) Acceso (X)	Manejo (X) Aprovechamiento (X) Divulgación ( ) Transferencia ( ) Remisión ( ) 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 mesa de ayuda de acuerdo a los permisos otorgados.		
Encargados del sistema			
Nombre encargado 1:	Karen Hernández Negrete		
Cargo:	Coordinación de sistemas / DGPyFE UNAM		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación (X)	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento (X) Posesión (X) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 mesa de ayuda de acuerdo a los permisos otorgados.		
Usuarios			
Nombre de usuario 1:	Araceli Hernández Alvarado		
Cargo:	Jefa del departamento de personal		
Funciones:	Obtención (X) Uso (X) Registro ( ) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 de usuario 2:	María de Jesús cadena Sandoval		
Cargo:	Administrativa		
Funciones:	Obtención (X) Uso (X) Registro ( ) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 3:	David Gómez Gaytán		
Cargo:	Unidad Administrativa		
Funciones:	Obtención (X) Uso (X) Registro ( ) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 4:	Elsa Concepción Botello López		
Cargo:	Editorial		
Funciones:	Obtención (X) Uso (X) Registro ( ) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 5:	Elsa Nava Velázquez		
Cargo:	Administrativa		
Funciones:	Obtención (X) Uso (X) Registro ( )	Utilización (X) Comunicación ( ) Difusión ( )	Manejo (X) Aprovechamiento (X) Divulgación ( )

	Organización (X) Elaboración ( ) Conservación ( )	Almacenamiento ( ) Posesión ( ) Acceso (X)	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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 6:	Guillermo Chávez Sánchez		
Cargo:	Revistas académicas y publicaciones		
Funciones:	Obtención (X) Uso (X) Registro ( ) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 7:	Gerardo Israel López García de León		
Cargo:	Administrativa		
Funciones:	Obtención (X) Uso (X) Registro ( ) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 8:	Jorge Alejandro Abrego Ugalde		
Cargo:	Comercialización		
Funciones:	Obtención (X) Uso (X) Registro ( ) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 9:	Claudia Tome González		
Cargo:	Administrativa		
Funciones:	Obtención (X) Uso (X) Registro ( ) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 10:	Lilia Juana Cruz Sánchez		
Cargo:	Editorial		
Funciones:	Obtención (X) Uso (X) Registro ( ) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 11:	Luis Antonio Reyes Quezada		
Cargo:	Administrativa		
Funciones:	Obtención (X) Uso (X) Registro ( ) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 12:	Luz Elena Silva Guerrero		
Cargo:	Comercialización		
Funciones:	Obtención (X)	Utilización (X)	Manejo (X)

	Uso (X) Registro ( ) Organización (X) Elaboración ( ) Conservación ( )	Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 13:	Juana María de la Luz Nazario Morales		
Cargo:	Comercialización		
Funciones:	Obtención (X) Uso (X) Registro ( ) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 14:	María Guadalupe Sánchez Hernández		
Cargo:	Comercialización		
Funciones:	Obtención (X) Uso (X) Registro ( ) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 15:	Marcos Mancera Reyes		
Cargo:	Administrativa		
Funciones:	Obtención (X) Uso (X) Registro ( ) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 16:	Miguel Julián Noé Murillo		
Cargo:	Administrativa		
Funciones:	Obtención (X) Uso (X) Registro ( ) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 17:	Nayely Karen Hernández Negrete		
Cargo:	Coordinación de sistemas		
Funciones:	Obtención (X) Uso (X) Registro ( ) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 18:	Norma Angélica Salazar Enciso		
Cargo:	Administrativa		
Funciones:	Obtención (X) Uso (X) Registro ( ) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 19:	Pablo Javier Quezada García		

Cargo:	Comercialización		
Funciones:	Obtención (X) Uso (X) Registro ( ) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 20:	Silvia Juana Paredes Jiménez		
Cargo:	Dirección		
Funciones:	Obtención (X) Uso (X) Registro ( ) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 21:	Socorro Venegas		
Cargo:	Directora de la DGPyFE		
Funciones:	Obtención (X) Uso (X) Registro ( ) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Dirección General de Publicaciones y Fomento Editorial			
Abreviatura del nombre del sistema	**PPC**		
Nombre del sistema	**Padrón de Proveedores y Contratistas**		
Datos personales contenidos en el sistema	- Nombre completo del usuario - Correo electrónico - Domicilio particular - Datos fiscales - Datos bancarios		

	- País		
Responsable del sistema			
Nombre:	Karen Hernández Negrete		
Cargo:	Coordinación de sistemas / DGPyFE UNAM		
Funciones:	Obtención () Uso (X) Registro () Organización () 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 mesa de ayuda de acuerdo a los permisos otorgados.		
Nombre:	David Gómez		
Cargo:	Unidad administrativa / DGPyFE UNAM		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación (X)	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento (X) Posesión (X) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 mesa de ayuda de acuerdo a los permisos otorgados.		
Encargados del sistema			
Nombre encargado 1:	Karen Hernández Negrete		
Cargo:	Coordinación de sistemas / DGPyFE UNAM		
Funciones:	Obtención () Uso () Registro () Organización () 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 mesa de ayuda de acuerdo a los permisos otorgados.		
Usuarios			
Nombre de usuario 1:	María de Jesús Cadena Sandoval		
Cargo:	Compras		
Funciones:	Obtención (X) Uso (X) Registro ( ) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Dirección General de Publicaciones y Fomento Editorial			
Abreviatura del nombre del sistema	**SIAF**		
Nombre del sistema	**Sistema Integral de Administración Financiera**		
Datos personales contenidos en el sistema	- Nombre completo - Datos fiscales - Dirección - Número telefónico particular - Correo electrónico - Datos bancarios		
Responsable del sistema			
Nombre:	Karen Hernández Negrete		
Cargo:	Coordinación de sistemas / DGPyFE UNAM		
Funciones:	Obtención () Uso () Registro () Organización () Elaboración ( ) Conservación (X)	Utilización () Comunicación ( ) Difusión ( ) Almacenamiento (X) Posesión () Acceso ()	Manejo () Aprovechamiento () Divulgación ( ) Transferencia ( ) Remisión ( ) Disposición ( )
Obligaciones:	- Guardar la confidencialidad de los datos personales. - Proteger los datos personales recibidos. - No modificar la información de datos personales contenidos en los documentos recibidos. - No difundir la información de datos personales contenidos en los documentos recibidos. - Mantener la información de datos personales en el archivo de la Unidad Administrativa. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de tienda electrónica de acuerdo a los permisos otorgados.		
Nombre:	David Gómez		
Cargo:	Unidad administrativa / DGPyFE UNAM		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación (X)	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento (X) Posesión (X) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 mesa de ayuda de acuerdo a los permisos otorgados.		
Encargados del sistema			
Nombre encargado 1:	Karen Hernández Negrete		
Cargo:	Coordinación de sistemas / DGPyFE UNAM		
Funciones:	Obtención () Uso () Registro () Organización () Elaboración ( ) Conservación (X)	Utilización () Comunicación ( ) Difusión ( ) Almacenamiento (X) Posesión () Acceso ()	Manejo () Aprovechamiento () Divulgación ( ) Transferencia ( ) Remisión ( ) Disposición ( )
Obligaciones:	- Guardar la confidencialidad de los datos personales. - Proteger los datos personales recibidos. - No modificar la información de datos personales contenidos en los documentos recibidos. - No difundir la información de datos personales contenidos en los documentos recibidos. - Mantener la información de datos personales en el archivo de la Unidad Administrativa. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de mesa de ayuda de acuerdo a los permisos otorgados.		
Usuarios			
Nombre de usuario 1:	Marcos Mancera Reyes		
Cargo:	Administrativa		
Funciones:	Obtención (X) Uso (X) Registro ( ) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 de usuario 2:	Juana Lima Castro		
Cargo:	Administrativa		
Funciones:	Obtención (X) Uso (X) Registro ( ) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área.		

	- No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 3:	David Gómez Gaytán		
Cargo:	Unidad administrativa		
Funciones:	Obtención (X) Uso (X) Registro ( ) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		

Dirección General de Publicaciones y Fomento Editorial			
Abreviatura del nombre del sistema	**SGA**		
Nombre del sistema	**Intelisis - Papyrus**		
Datos personales contenidos en el sistema	- Nombre completo - Datos fiscales - Dirección - Número telefónico particular - Correo electrónico - Datos bancarios		
Responsable del sistema			
Nombre:	Karen Hernández Negrete		
Cargo:	Coordinación de sistemas / DGPyFE UNAM		
Funciones:	Obtención (X) Uso (X) Registro () Organización (X) Elaboración ( ) Conservación (X)	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento (X) Posesión (X) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 tienda electrónica de acuerdo a los permisos otorgados.		
Nombre:	David Gómez		
Cargo:	Unidad administrativa / DGPyFE UNAM		
Funciones:	Obtención (X) Uso (X) Registro () Organización (X) Elaboración ( ) Conservación (X)	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento (X) Posesión (X) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 mesa de ayuda de acuerdo a los permisos otorgados.		
Encargados del sistema			
Nombre encargado 1:	Karen Hernández Negrete		
Cargo:	Coordinación de sistemas / DGPyFE UNAM		
Funciones:	Obtención (X) Uso (X) Registro () Organización (X) Elaboración ( ) Conservación (X)	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento (X) Posesión (X) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 mesa de ayuda de acuerdo a los permisos otorgados.		
Usuarios			
Nombre de usuario 1:	Karen Hernández Negrete		
Cargo:	Coordinación de sistemas / DGPyFE UNAM		
Funciones:	Obtención (X) Uso (X) Registro ( ) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 de usuario 2:	David Gómez		
Cargo:	Unidad administrativa / DGPyFE UNAM		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área.		

	- No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 3:	Alejandro Hernández Carmona		
Cargo:	Asistente de procesos		
Funciones:	Obtención (X) Uso (X) Registro ( ) Organización (X) Elaboración ( ) Conservación (X)	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento (X) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 4:	Marlene Fernández		
Cargo:	Asistente de procesos		
Funciones:	Obtención (X) Uso (X) Registro ( ) Organización (X) Elaboración ( ) Conservación (X)	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 5:	Patricia Muñetón		
Cargo:	Revistas académicas y publicaciones digitales		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 6:	Rosa María Escobedo Molina		
Cargo:	Derechos de autor		
Funciones:	Obtención (X) Uso (X)	Utilización (X) Comunicación ( )	Manejo (X) Aprovechamiento (X)

	Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 7:	Alejandro Villaseñor		
Cargo:	Comercialización		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 8:	Claudia Guerrero Juárez		
Cargo:	Comercialización		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 9:	Guadalupe Sánchez		
Cargo:	Comercialización		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 10:	Jorge Abrego		
Cargo:	Jefe de ventas		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 11:	Leticia Pérez		
Cargo:	Comercialización		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 12:	María de la Luz Nazario		
Cargo:	Comercialización		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 13:	María Eugenia Romero		
Cargo:	Comercialización		

Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 14:	Mónica Josefina Escorcia Sánchez		
Cargo:	Comercialización		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 15:	Oscar Santamaria González		
Cargo:	Jefe de desarrollo tecnológico		
Funciones:	Obtención (X) Uso (X) Registro () Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 16:	Virginia Palma Cortes		
Cargo:	Comercialización		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 17:	Felipe de Jesús Santa Rita Nava		
Cargo:	Derechos de autor		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 18:	Patricia Perea		
Cargo:	Derechos de autor		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 19:	Sandra Islas		
Cargo:	Derechos de autor		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		

Nombre de usuario 20:	Eulalia Luna Gómez		
Cargo:	Dirección		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 21:	Maricel Buiza		
Cargo:	Dirección		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 22:	Paola Velasco		
Cargo:	Dirección		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 23:	Socorro Venegas		
Cargo:	Directora		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X)	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( )	Manejo (X) Aprovechamiento (X) Divulgación ( ) Transferencia ( )

	Elaboración ( ) Conservación ( )	Posesión ( ) Acceso (X)	Remisión ( ) Disposición ( )
Obligaciones:	- Guardar la confidencialidad de los datos personales. - Proteger los datos personales recibidos. - No modificar la información de datos personales contenidos en los documentos recibidos. - No difundir la información de datos personales contenidos en los documentos recibidos. - Mantener la información de datos personales en el archivo de su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 24:	Ana Grisel Maldonado Carrasco		
Cargo:	Editorial		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 25:	Beatriz Vallarta Jiménez		
Cargo:	Editorial		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 26:	Elsa Botello		
Cargo:	Editorial		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área.		

	- No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 27:	Lilia Cruz		
Cargo:	Editorial		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 28:	Nataly Vaca Tapia		
Cargo:	Revistas académicas y publicaciones digitales		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 29:	Patricia Zama		
Cargo:	Editorial		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 30:	Rosalía Chavelas		
Cargo:	Editorial		
Funciones:	Obtención (X) Uso (X)	Utilización (X) Comunicación ( )	Manejo (X) Aprovechamiento (X)

	Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 31:	Víctor Cabrera		
Cargo:	Editorial		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 32:	Laura Mariana Orozco Cortes		
Cargo:	Comercialización		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 33:	Manuel Mendoza Tirado		
Cargo:	Comercialización		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 34:	Pablo Javier Quezada García		
Cargo:	Comercialización		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 35:	Fabiola Benítez Rodríguez		
Cargo:	Comercialización		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 36:	Benjamín Villanueva Elías		
Cargo:	Comercialización		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 37:	César Silva Castro		
Cargo:	Comercialización		

Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 38:	Ignacio Medina Leyva		
Cargo:	Comercialización		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 39:	Luz Elena Silva Guerrero		
Cargo:	Comercialización		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 40:	Magali Arámbula Morales		
Cargo:	Jefa de la librería Palacio de Minería		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 41:	Socorro Martínez Nava		
Cargo:	Jefa de la librería Palacio de Minería		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 42:	Víctor Manuel Sánchez Trejo		
Cargo:	Jefe de la libraría Jaime García Terrés		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 43:	Antonio Reyes		
Cargo:	Jefe de departamento de operación y control CxC		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		

Nombre de usuario 44:	Araceli Hernández Alvarado		
Cargo:	Jefa del departamento de personal		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 45:	Claudia Tome		
Cargo:	Administrativa		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 46:	Dania Erika Reveles Pimentel		
Cargo:	Administrativa		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 47:	Elsa Nava		
Cargo:	Administrativa		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X)	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( )	Manejo (X) Aprovechamiento (X) Divulgación ( ) Transferencia ( )

	Elaboración ( ) Conservación ( )	Posesión ( ) Acceso (X)	Remisión ( ) Disposición ( )
Obligaciones:	- Guardar la confidencialidad de los datos personales. - Proteger los datos personales recibidos. - No modificar la información de datos personales contenidos en los documentos recibidos. - No difundir la información de datos personales contenidos en los documentos recibidos. - Mantener la información de datos personales en el archivo de su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 48:	Gabriel Fernando Moreno León		
Cargo:	Administrativa		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 49:	Gerardo Israel López García de León		
Cargo:	Administrativa		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 50:	Graciela Correa Ibarra		
Cargo:	Administrativa		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área.		

	- No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 51:	Hugo Trujano		
Cargo:	Administrativa		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 52:	Javier Rosillo		
Cargo:	Administrativa		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 53:	Juana Lima Castro		
Cargo:	Administrativa		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 54:	Julio Álvarez Cardoso		
Cargo:	Administrativa		
Funciones:	Obtención (X) Uso (X)	Utilización (X) Comunicación ( )	Manejo (X) Aprovechamiento (X)

	Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 55:	Luis Roberto Barrios Cruz		
Cargo:	Administrativa		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 56:	Ma. de Jesús Cadena Sandoval		
Cargo:	Administrativa		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 57:	Marcos Mancera Reyes		
Cargo:	Administrativa		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 58:	María Esther Fregoso Ledesma		
Cargo:	Administrativa		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 59:	Marisol Reséndiz Callejas		
Cargo:	Administrativa		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 60:	Norma Salazar		
Cargo:	Administrativa		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 61:	Víctor Nicolas Ayub Romero		
Cargo:	Administrativa		

Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - No generar copias de los documentos en los equipos de trabajo. - Utilizar el sistema de gestión de acuerdo a los permisos otorgados.		
Nombre de usuario 62:	Soledad Castañeda		
Cargo:	Administrativa		
Funciones:	Obtención (X) Uso (X) Registro (X) Organización (X) Elaboración ( ) Conservación ( )	Utilización (X) Comunicación ( ) Difusión ( ) Almacenamiento ( ) Posesión ( ) Acceso (X)	Manejo (X) Aprovechamiento (X) 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 su área. - 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 General de Publicaciones y Fomento Editorial		
Abreviatura del nombre del sistema	**TE**	
Nombre del sistema	**Tienda electrónica libros UNAM**	
¿Cómo se resguardan los datos personales?	Físico ( ) Digital (X) Ambos ( )	
	Tipo de soporte	Físico ( ) Digital (X) Ambos ( )
	¿Dónde se aloja?	Computadora ( ) Servidor (X) Nube ( ) Correo ( ) Otros - Centro de datos DGTIC
	Descripción de la información que se resguarda	- Catálogo de artículos del almacén de la librería Henrique González Casanova, almacenados en una base de datos de SQL Server Managment Studio, estos archivos son .DBF, administrados mediante un ERP.
	Características del lugar donde se resguarda la información	Centro de datos DGTIC Servidor virtual con sistema operativo CentOS 7 vCPUs: 8 RAM: 32GB HDD1: 8GB HDD2: 300GB
Dirección General de Publicaciones y Fomento Editorial		
Abreviatura del nombre del sistema	**FD**	
Nombre del sistema	**Facturación Digital**	
¿Cómo se resguardan los datos personales?	Físico ( ) Digital (X) Ambos ( )	
	Tipo de soporte	Físico ( ) Digital (X) Ambos ( )
	¿Dónde se aloja?	Computadora ( ) Servidor (X) Nube ( ) Correo ( ) Otros (X) servidores de Patronato Universitario
	Descripción de la información que se resguarda	- Se resguardan los datos personales de los clientes y las facturas digitales, en los servidores de Patronato Universitario
	Características del lugar donde se resguarda la información	En el centro de cómputo de Patronato Universitario
Dirección General de Publicaciones y Fomento Editorial		
Abreviatura del nombre del sistema	**SIC**	
Nombre del sistema	**Sistema Institucional de Compras**	
¿Cómo se resguardan los datos personales?	Físico ( ) Digital (X) Ambos ( )	
	Tipo de soporte	Físico ( ) Digital ( ) Ambos (X)
	¿Dónde se aloja?	Computadora ( ) Servidor (X) Nube ( ) Correo ( ) Otros - Expediente físicos en archiveros.

		- Secretaría Administrativa. Dirección General de Publicaciones y Fomento Editorial. (SADGPyFE) - Centro de datos de la Dirección General de Proveeduría y en el centro de datos de Patronato Universitario.
	Descripción de la información que se resguarda	- Solicitudes - Cotización - Factura - Bóveda fiscal - Forma múltiple - Orden de compra - Cheque - Póliza de cheque
	Características del lugar donde se resguarda la información	- Carpeta compartida en red modelo cliente-servidor, cada quien tiene su cuenta de usuario para acceder. En el centro de cómputo de la Secretaría Administrativa, Dirección General de Proveeduría y Patronato Universitario.
Dirección General de Publicaciones y Fomento Editorial		
Abreviatura del nombre del sistema	**PPC**	
Nombre del sistema	**Padrón de Proveedores y Contratistas**	
¿Cómo se resguardan los datos personales?	Físico ( ) Digital (X) Ambos ( )	
	Tipo de soporte	Físico ( ) Digital (X) Ambos ( )
	¿Dónde se aloja?	Computadora ( ) Servidor (X) Nube ( ) Correo ( ) Otros (X) servidores de Patronato Universitario
	Descripción de la información que se resguarda	- Se resguardan los datos personales de los clientes y las facturas digitales, en los servidores de Patronato Universitario
	Características del lugar donde se resguarda la información	- La Dirección General de Control Presupuestal e Informática, por conducto de su Dirección de Organización y Sistemas. Patronato Universitario
Dirección General de Publicaciones y Fomento Editorial		
Abreviatura del nombre del sistema	**SIAF**	
Nombre del sistema	**Sistema Integral de Administración Financiera**	
¿Cómo se resguardan los datos personales?	Físico ( ) Digital (X) Ambos ( )	
	Tipo de soporte	Físico ( ) Digital ( ) Ambos (X)
	¿Dónde se aloja?	Computadora ( ) Servidor (X) Nube ( ) Correo ( ) Otros - Expediente físicos en archiveros. - Instituto de Ingeniería. Dirección General de Publicaciones y Fomento Editorial. (SADGPyFE)
	Descripción de la información que se resguarda	- Solicitudes - Cotización - Factura

		- Bóveda fiscal - Forma múltiple - Orden de compra - Cheque - Póliza de cheque - Convenios, contrato o pagaré
	Características del lugar donde se resguarda la información	- Carpeta compartida en red modelo cliente-servidor, cada quien tiene su cuenta de usuario para acceder. En el centro de cómputo del Instituto de Ingeniería
Dirección General de Publicaciones y Fomento Editorial		
Abreviatura del nombre del sistema	**SGA**	
Nombre del sistema	**Intelisis - Papyrus**	
¿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 ( ) Otros - SITE de la DGPyFE en la coordinación de sistemas
	Descripción de la información que se resguarda	- Información de catálogo de artículos, clientes, proveedores, movimientos de ventas y compras, control de inventario de artículos, administrados mediante un ERP.
	Características del lugar donde se resguarda la información	Centro de datos de la DGPyFE Servidor virtual con sistema operativo Windows Server 2008 vCPUs: 8 RAM: 4GB HDD1: 700GB HDD2

ANEXO 3

FUNCIONES Y OBLIGACIONES DE QUIENES TRATEN DATOS PERSONALES

DG – Director General
CS – Coordinador de sistemas
SB – Subdirectores
JD – Jefes de departamento
UA – Personal de la Unidad Administrativa
RDP - Responsable de datos personales

Dirección General de Publicaciones y Fomento Editorial						
Abreviatura del nombre del sistema	**TE**					
Nombre del sistema	**Tienda electrónica libros UNAM**					
Actividades	**DG**	**CS**	**SB**	**JD**	**UA**	**RDP**
Guardar información de los documentos recibidos en el sistema de gestión	X				X	
Notificar la obtención de la información para iniciar el trámite de entrega de mercancía			X		X	X
Consultar la información de datos personales en el correo institucional			X		X	X
Dar seguimiento al trámite de entrega de mercancía			X	X		X
Dar seguimiento a solicitudes de acceso a la información y ejercicio de derechos ARCO		X	X		X	X
Consulta información de datos personales en los documentos recibidos en el sistema de gestión			X		X	X
Guardar los documentos enviados por los titulares de los datos personales en el archivo físico y digital			X		X	X
Revisar los documentos entregados por los titulares de datos personales para detectar estos			X		X	X
Hacer sugerencias al área universitaria para quitar, testar o clasificar la información de documentos entregados según sea el caso			X		X	X
Mantener equipos de trabajo libres de documentos con datos personales		X			X	
Generar respaldos de sistemas		X				X
Proteger los datos personales contenidos en el sistema de accesos no autorizados		X				X
Mantener actualizados los servidores donde se alojan los sistemas de tratamiento de datos personales		X				X
Mantener actualizado el sistema de gestión	X	X	X	X	X	X
Dictar políticas para el aseguramiento de los datos personales en la DGPyFE	X	X	X	X	X	X
Dar capacitación en materia de protección de datos personales	X	X	X	X	X	X

Proteger el archivo físico de la DGPyFE de accesos no autorizados		X			X	X
Dirección General de Publicaciones y Fomento Editorial						
Abreviatura del nombre del sistema	**TE**					
Nombre del sistema	**Tienda electrónica libros UNAM**					
FUNCIONES DENTRO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES						
Actividades	**DG**	**CS**	**SB**	**JD**	**UA**	
Política y Objetivos del SGSDP	X	X	X	X	X	
Funciones y obligaciones		X	X	X	X	
Inventario de datos personales		X	X	X	X	
Análisis de riesgos de los datos personales		X	X	X	X	
Análisis de brecha de las medidas de seguridad		X	X	X	X	
Implementación de las medidas de seguridad		X	X	X	X	
Capacitación	X	X	X	X	X	
Revisiones y auditoría	X	X	X	X	X	
Dirección General de Publicaciones y Fomento Editorial						
Abreviatura del nombre del sistema	**TE**					
Nombre del sistema	**Tienda electrónica libros UNAM**					
MATRIZ DE RENDICIÓN DE CUENTAS						
Actividades	**DG**	**CS**	**SB**	**JD**	**UA**	
Unidad Administrativa	X					
Coordinador de sistemas	X		X		X	
Subdirectores	X				X	
Jefes de departamento	X	X	X		X	
Dirección General de Publicaciones y Fomento Editorial						
Abreviatura del nombre del sistema	**FD**					
Nombre del sistema	**Facturación Digital**					
Actividades	**CS**	**SB**	**JD**	**UA**	**RDP**	
Guardar información de los documentos recibidos en el sistema de gestión	X	X	X	X	X	
Consultar la información de datos personales en el correo institucional	X		X	X	X	
Notificar la obtención de los documentos para iniciar el trámite de pago			X	X	X	
Dar seguimiento a solicitudes de acceso a la información y ejercicio de derechos ARCO	X	X	X	X	X	
Consulta información de datos personales en los documentos recibidos en el sistema de gestión	X	X	X	X	X	
Guardar los documentos enviados por los titulares de los datos personales en el archivo físico y digital	X	X	X	X	X	
Revisar los documentos entregados por los titulares de datos personales para detectar estos	X	X	X	X	X	
Proteger los datos personales contenidos en el sistema de accesos no autorizados	X	X	X	X	X	

Mantener actualizados los servidores donde se alojan los sistemas de tratamiento de datos personales	X			X	X
Mantener actualizado el sistema de gestión	X	X	X	X	X
Dictar políticas para el aseguramiento de los datos personales en la DGPyFE				X	X
Dar capacitación en materia de protección de datos personales	X	X	X	X	X
Dirección General de Publicaciones y Fomento Editorial					
Abreviatura del nombre del sistema	**FD**				
Nombre del sistema	**Facturación Digital**				
FUNCIONES DENTRO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES					
Actividades	**CS**	**SB**	**JD**	**UA**	
Política y objetivos del SGSDP	X	X	X	X	
Funciones y obligaciones	X	X	X	X	
Inventario de datos personales	X	X	X	X	
Análisis de riesgos de los datos personales	X	X	X	X	
Análisis de brecha de las medidas de seguridad	X	X	X	X	
Implementación de las medidas de seguridad	X	X	X	X	
Capacitación	X	X	X	X	
Revisiones y auditoría	X	X	X	X	
Dirección General de Publicaciones y Fomento Editorial					
Abreviatura del nombre del sistema	**FD**				
Nombre del sistema	**Facturación Digital**				
MATRIZ DE RENDICIÓN DE CUENTAS					
Actividades	**DG**	**CS**	**SB**	**JD**	**UA**
Unidad Administrativa	X				
Coordinador de sistemas	X				X
Subdirectores	X				X
Jefes de departamento	X	X	X		X
Dirección General de Publicaciones y Fomento Editorial					
Abreviatura del nombre del sistema	**SIC**				
Nombre del sistema	**Sistema Institucional de Compras**				
Actividades	**DG**	**CS**	**SB**	**JD**	**UA**	**RDP**
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	X	X
Consultar la información de datos personales en el correo institucional			X	X	X	X
Dar seguimiento al trámite de pago				X	X	X
Dar seguimiento a solicitudes de acceso a la información y ejercicio de derechos ARCO		X	X	X	X	X
Consulta información de datos personales en los documentos recibidos en el sistema de gestión				X	X	X

Guardar los documentos enviados por los titulares de los datos personales en el archivo físico y/o digital				X	X	X
Revisar los documentos entregados por los titulares de datos personales para detectar estos				X	X	X
Hacer sugerencias al área universitaria para quitar, testar o clasificar la información de documentos entregados según sea el caso		X	X	X	X	X
Mantener equipos de trabajo libres de documentos con datos personales	X	X	X	X	X	X
Generar respaldos de sistemas		X			X	X
Proteger los datos personales relativos al área universitaria contenidos en el sistema de accesos no autorizados		X			X	X
Mantener actualizados los servidores donde se alojan los sistemas de tratamiento de datos personales		X			X	X
Mantener actualizado el sistema de gestión	X	X	X	X	X	X
Dictar políticas para el aseguramiento de los datos personales en la DGPyFE	X	X	X	X	X	X
Dar capacitación en materia de protección de datos personales		X	X	X	X	X
Proteger el archivo físico de la DGPyFE de accesos no autorizados				X	X	X

Dirección General de Publicaciones y Fomento Editorial					
Abreviatura del nombre del sistema	**SIC**				
Nombre del sistema	**Sistema Institucional de Compras**				
FUNCIONES DENTRO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES					
Actividades	**DG**	**CS**	**SB**	**JD**	**UA**
Elaborar políticas y objetivos del SGSDP	X	X	X	X	X
Aprobar políticas y objetivos del SGSDP		X	X	X	X
Asignar funciones y obligaciones	X	X	X	X	X
Elaborar inventario de datos personales		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	X
Capacitación	X	X	X	X	X
Revisiones y auditoría		X	X	X	X

Dirección General de Publicaciones y Fomento Editorial					
Abreviatura del nombre del sistema	**SIC**				
Nombre del sistema	**Sistema Institucional de Compras**				
MATRIZ DE RENDICIÓN DE CUENTAS					
Actividades	**DG**	**CS**	**SB**	**JD**	**UA**
Unidad Administrativa	X				
Coordinador de sistemas	X		X		X
Subdirectores	X				X

Jefes de departamento	X	X	X		X
Dirección General de Publicaciones y Fomento Editorial					
Abreviatura del nombre del sistema	**PPC**				
Nombre del sistema	**Padrón de Proveedores y Contratistas**				
Actividades	**CS**	**SB**	**JD**	**UA**	**RDP**
Guardar información de los documentos recibidos en el sistema de gestión			X	X	X
Consultar la información de datos personales en el correo institucional			X	X	X
Notificar la obtención de los documentos para iniciar el trámite de pago			X	X	X
Dar seguimiento a solicitudes de acceso a la información y ejercicio de derechos ARCO			X	X	X
Consulta información de datos personales en los documentos recibidos en el sistema de gestión			X	X	X
Guardar los documentos enviados por los titulares de los datos personales en el archivo físico y digital			X	X	X
Revisar los documentos entregados por los titulares de datos personales para detectar estos			X	X	X
Proteger los datos personales contenidos en el sistema de accesos no autorizados	X		X	X	X
Mantener actualizados los servidores donde se alojan los sistemas de tratamiento de datos personales	X			X	X
Mantener actualizado el sistema de gestión	X		X	X	X
Dictar políticas para el aseguramiento de los datos personales en la DGPyFE	X			X	X
Dar capacitación en materia de protección de datos personales	X	X	X	X	X
Dirección General de Publicaciones y Fomento Editorial					
Abreviatura del nombre del sistema	**PPC**				
Nombre del sistema	**Padrón de Proveedores y Contratistas**				
FUNCIONES DENTRO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES					
Actividades	**CS**	**SB**	**JD**	**UA**	
Política y objetivos del SGSDP	X	X	X	X	
Funciones y obligaciones	X	X	X	X	
Inventario de datos personales	X	X	X	X	
Análisis de riesgos de los datos personales	X	X	X	X	
Análisis de brecha de las medidas de seguridad	X	X	X	X	
Implementación de las medidas de seguridad	X	X	X	X	
Capacitación	X	X	X	X	
Revisiones y auditoría	X	X	X	X	
Dirección General de Publicaciones y Fomento Editorial					
Abreviatura del nombre del sistema	**PPC**				

Nombre del sistema	Padrón de Proveedores y Contratistas				
MATRIZ DE RENDICIÓN DE CUENTAS					
Actividades	**DG**	**CS**	**SB**	**JD**	**UA**
Unidad Administrativa	X				
Coordinador de sistemas	X				X
Subdirectores	X				X
Jefes de departamento	X	X	X		X

Dirección General de Publicaciones y Fomento Editorial						
Abreviatura del nombre del sistema	**SIAF**					
Nombre del sistema	**Sistema Integral de Administración Financiera**					
Actividades	**DG**	**CS**	**SB**	**JD**	**UA**	**RDP**
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	X	X
Consultar la información de datos personales en el correo institucional			X	X	X	X
Dar seguimiento al trámite de pago				X	X	X
Dar seguimiento a solicitudes de acceso a la información y ejercicio de derechos ARCO		X	X	X	X	X
Consulta información de datos personales en los documentos recibidos en el sistema de gestión				X	X	X
Guardar los documentos enviados por los titulares de los datos personales en el archivo físico y/o digital				X	X	X
Revisar los documentos entregados por los titulares de datos personales para detectar estos				X	X	X
Hacer sugerencias al área universitaria para quitar, testar o clasificar la información de documentos entregados según sea el caso		X	X	X	X	X
Mantener equipos de trabajo libres de documentos con datos personales	X	X	X	X	X	X
Generar respaldos de sistemas		X			X	X
Proteger los datos personales relativos al área universitaria contenidos en el sistema de accesos no autorizados		X			X	X
Mantener actualizados los servidores donde se alojan los sistemas de tratamiento de datos personales		X			X	X
Mantener actualizado el sistema de gestión	X	X	X	X	X	X
Dictar políticas para el aseguramiento de los datos personales en la DGPyFE	X	X	X	X	X	X
Dar capacitación en materia de protección de datos personales		X	X	X	X	X
Proteger el archivo físico de la DGPyFE de accesos no autorizados				X	X	X

Dirección General de Publicaciones y Fomento Editorial					
Abreviatura del nombre del sistema	**SIAF**				
Nombre del sistema	**Sistema Integral de Administración Financiera**				
FUNCIONES DENTRO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES					
Actividades	**DG**	**CS**	**SB**	**JD**	**UA**
Elaborar políticas y objetivos del SGSDP	X	X	X	X	X
Aprobar políticas y objetivos del SGSDP		X	X	X	X
Asignar funciones y obligaciones	X	X	X	X	X
Elaborar inventario de datos personales		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	X
Capacitación	X	X	X	X	X
Revisiones y auditoría		X	X	X	X

Dirección General de Publicaciones y Fomento Editorial					
Abreviatura del nombre del sistema	**SIAF**				
Nombre del sistema	**Sistema Integral de Administración Financiera**				
MATRIZ DE RENDICIÓN DE CUENTAS					
Actividades	**DG**	**CS**	**SB**	**JD**	**UA**
Unidad Administrativa	X				
Coordinador de sistemas	X		X		X
Subdirectores	X				X
Jefes de departamento	X	X	X		X

Dirección General de Publicaciones y Fomento Editorial						
Abreviatura del nombre del sistema	**SGA**					
Nombre del sistema	**Intelisis - Papyrus**					
Actividades	**DG**	**CS**	**SB**	**JD**	**UA**	**RDP**
Guardar información de los documentos recibidos en el sistema de gestión	X	X	X		X	X
Notificar la obtención de la información para el registro de los datos personales		X	X	X	X	X
Consultar la información de datos personales en el correo institucional		X	X	X	X	X
Dar seguimiento al trámite de registro de la información de datos personales		X	X	X	X	X
Dar seguimiento a solicitudes de acceso a la información y ejercicio de derechos ARCO		X	X		X	X
Consulta información de datos personales en los documentos recibidos en el sistema de gestión	X	X	X	X	X	X
Guardar los documentos enviados por los titulares de los datos personales en el archivo físico y digital		X	X	X	X	X
Revisar los documentos entregados por los titulares de datos personales para detectar estos		X	X	X	X	X
Hacer sugerencias al área universitaria para quitar, testar o clasificar la	X	X	X		X	X

información de documentos entregados según sea el caso						
Mantener equipos de trabajo libres de documentos con datos personales		X			X	X
Generar respaldos de sistemas		X	X	X	X	X
Proteger los datos personales contenidos en el sistema de accesos no autorizados		X			X	X
Mantener actualizados los servidores donde se alojan los sistemas de tratamiento de datos personales		X			X	X
Mantener actualizado el sistema de gestión	X	X	X	X	X	X
Dictar políticas para el aseguramiento de los datos personales en la DGPyFE	X	X	X	X	X	X
Dar capacitación en materia de protección de datos personales	X	X	X	X	X	X
Proteger el archivo físico de la DGPyFE de accesos no autorizados		X			X	X

Dirección General de Publicaciones y Fomento Editorial					
Abreviatura del nombre del sistema	**SGA**				
Nombre del sistema	**Intelisis - Papyrus**				
FUNCIONES DENTRO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES					
Actividades	**DG**	**CS**	**SB**	**JD**	**UA**
Política y Objetivos del SGSDP	X	X	X	X	X
Funciones y obligaciones		X	X	X	X
Inventario de datos personales		X	X	X	X
Análisis de riesgos de los datos personales		X	X	X	X
Análisis de brecha de las medidas de seguridad		X	X	X	X
Implementación de las medidas de seguridad	X	X	X	X	X
Capacitación	X	X	X	X	X
Revisiones y auditoría	X	X	X	X	X

Dirección General de Publicaciones y Fomento Editorial					
Abreviatura del nombre del sistema	**SGA**				
Nombre del sistema	**Intelisis - Papyrus**				
MATRIZ DE RENDICIÓN DE CUENTAS					
Actividades	**DG**	**CS**	**SB**	**JD**	**UA**
Unidad Administrativa	X				
Coordinador de sistemas	X		X		X
Subdirectores	X				X
Jefes de departamento	X	X	X		X

ANEXO 4

ANÁLISIS DE RIESGOS

Dirección General de Publicaciones y Fomento Editorial		
Abreviatura del nombre del sistema	**TE**	
Nombre del sistema	**Tienda electrónica libros UNAM**	
MATRIZ DE RENDICIÓN DE CUENTAS		
RIESGO	**IMPACTO**	**MITIGACIÓN**
Saturación del servidor (disco duro)	La tienda estaría fuera de servicio y posible pérdida de la información	Mantenimiento al servidor cada mes (limpieza de archivos temporales) y llevar a cabo los respaldos correspondientes
Hacker/cracker	-Acceso no autorizado al sistema -Robo de información -Borrado de información	Instalación y monitoreo un detector de intrusos, firewall, el cual detectará quien accede al servidor.
Problemas técnicos en el centro de datos de DGTIC	La tienda estaría fuera de servicio y posible pérdida de la información	DGTIC ha tomado las medidas pertinentes para el resguardo de la información ante cualquier contingencia
Cortes de luz	La tienda estaría fuera de servicio perdida de la información	Se desarrolló un proceso de monitoreo dentro una aplicación para revisar la conexión entre servidores
Certificado de seguridad	Desconfianza de los clientes al momento de realizar la transacción y la tienda esta fuera de servicio	Configuración, renovación y actualización del certificado de seguridad para asegurar que los datos personales del cliente están seguros al momento de realizar la transacción.
Dirección General de Publicaciones y Fomento Editorial		
Abreviatura del nombre del sistema	**FD**	
Nombre del sistema	**Facturación Digital**	
MATRIZ DE RENDICIÓN DE CUENTAS		
RIESGO	**IMPACTO**	**MITIGACIÓN**
Hacker/cracker	-Acceso no autorizado al sistema -Robo de información -Borrado de información	Instalación y monitoreo un detector de intrusos, firewall, el cual detectará quien accede al servidor.
Problemas técnicos con el servidor	No se podrá acceder al sistema FD y los clientes no recibirán su documento fiscal	Patronato Universitario da mantenimiento continuamente al servidor.
Actualizar el sistema	No se podrá acceder al sistema FD y no se podrán generar documentos fiscales	Realizar la actualización en un horario que no afecte el servicio de facturación
Cortes de luz	La factura queda incompleta y no se generará. El cliente no recibe su factura oportunamente	Patronato Universitario cuenta con las medidas para que el sistema este en línea en todo momento
Enviar documento fiscal a otro correo electrónico	Se puede hacer mal uso del documento fiscal	Se corrobora con el cliente los datos fiscales de manera puntual
Certificado de seguridad	Desconfianza de los clientes del trato de sus datos personales	Configuración, renovación y actualización del certificado de seguridad para asegurar que los datos personales del cliente están seguros.
Dirección General de Publicaciones y Fomento Editorial		
Abreviatura del nombre del sistema	**SIC**	
Nombre del sistema	**Sistema Institucional de Compras**	
MATRIZ DE RENDICIÓN DE CUENTAS		
RIESGO	**IMPACTO**	**MITIGACIÓN**
Hacker/cracker	- Acceso no autorizado al sistema - Robo de información - Borrado de información	Instalación y monitoreo un detector de intrusos, firewall, el cual detectará quien accede al servidor.

Problemas técnicos en el centro de datos de la Secretaría Administrativa	El sistema estaría fuera de servicio y posible pérdida de la información	La Secretaría Administrativa ha tomado las medidas pertinentes para el resguardo de la información ante cualquier contingencia
Certificado de seguridad	Desconfianza de los clientes al momento de realizar la transacción	Configuración, renovación y actualización del certificado de seguridad para asegurar que los datos personales del cliente están seguros al momento de realizar la transacción.
No contar con respaldos	Pérdida de la información	- Guardar información en discos extraíbles - Guardar información en la nube
Transferir información para la obtención de un beneficio y/o servicio	- Pérdida de datos personales - Robo información - Divulgación	Contar con políticas para una adecuada transferencia de datos
Eventos naturales (sismo, fenómenos climáticos o meteorológicos)	- Daño de documentos personales - Pérdida de información	- Alerta sísmica - Resguardo de la información en digital - Colocación de archiveros / libreros en lugares estratégicos
Uso no autorizado de equipo	- Obtención de información personal - Pérdida de información - Consulta de información de datos personales	- Contar con contraseñas personales e intransferibles. - Concientizar al personal del uso del sistema (cerrar cesión cuando no esté en su lugar de trabajo)
Omisión de reporte sobre fallas del sistema	- Pérdida de información - Robo de información - Uso indebido de información	- Reportar las fallas detectadas en el sistema - Corrección de las fallas reportadas - Revisión de los registros de fallas
Dirección General de Publicaciones y Fomento Editorial		
Abreviatura del nombre del sistema	**PPC**	
Nombre del sistema	**Padrón de Proveedores y Contratistas**	
MATRIZ DE RENDICIÓN DE CUENTAS		
RIESGO	**IMPACTO**	**MITIGACIÓN**
Hacker/cracker	-Acceso no autorizado al sistema -Robo de información -Borrado de información	Instalación y monitoreo un detector de intrusos, firewall, el cual detectará quien accede al servidor.
Problemas técnicos con el servidor	No se podrá acceder al sistema FD y los clientes no recibirán su documento fiscal	Patronato Universitario da mantenimiento continuamente al servidor.
Actualizar el sistema	No se podrá acceder al sistema FD y no se podrán generar documentos fiscales	Realizar la actualización en un horario que no afecte el servicio de facturación
Cortes de luz	La factura queda incompleta y no se generará. El cliente no recibe su factura oportunamente	Patronato Universitario cuenta con las medidas para que el sistema este en línea en todo momento
Enviar documento fiscal a otro correo electrónico	Se puede hacer mal uso del documento fiscal	Se corrobora con el cliente los datos fiscales de manera puntual
Certificado de seguridad	Desconfianza de los clientes del trato de sus datos personales	Configuración, renovación y actualización del certificado de seguridad para asegurar que los datos personales del cliente están seguros.
Dirección General de Publicaciones y Fomento Editorial		
Abreviatura del nombre del sistema	**SIAF**	
Nombre del sistema	**Sistema Integral de Administración Financiera**	
MATRIZ DE RENDICIÓN DE CUENTAS		
RIESGO	**IMPACTO**	**MITIGACIÓN**

Hacker/cracker	- Acceso no autorizado al sistema - Robo de información - Borrado de información	Instalación y monitoreo un detector de intrusos, firewall, el cual detectará quien accede al servidor.
Problemas técnicos en el centro de datos del Instituto de Ingeniería	El sistema estaría fuera de servicio y posible pérdida de la información	El Instituto de Ingeniería ha tomado las medidas pertinentes para el resguardo de la información ante cualquier contingencia
Certificado de seguridad	Desconfianza de los clientes al momento de realizar la transacción	Configuración, renovación y actualización del certificado de seguridad para asegurar que los datos personales del cliente están seguros al momento de realizar la transacción.
No contar con respaldos	Pérdida de la información	- Guardar información en discos extraíbles - Guardar información en la nube
Transferir información para la obtención de un beneficio y/o servicio	- Pérdida de datos personales - Robo información - Divulgación	Contar con políticas para una adecuada transferencia de datos
Eventos naturales (sismo, fenómenos climáticos o meteorológicos)	- Daño de documentos personales - Pérdida de información digital y física.	- Alerta sísmica - Resguardo de la información en digital - Colocación de archiveros / libreros en lugares estratégicos
Uso no autorizado de equipo	- Obtención de información personal - Pérdida de información - Consulta de información de datos personales	- Contar con contraseñas personales e intransferibles. - Concientizar al personal del uso del sistema (cerrar cesión cuando no esté en su lugar de trabajo)
Omisión de reporte sobre fallas del sistema	- Pérdida de información - Robo de información - Uso indebido de información	- Reportar las fallas detectadas en el sistema - Corrección de las fallas reportadas - Revisión de los registros de fallas
Dirección General de Publicaciones y Fomento Editorial		
Abreviatura del nombre del sistema	**SGA**	
Nombre del sistema	**Intelisis - Papyrus**	
MATRIZ DE RENDICIÓN DE CUENTAS		
RIESGO	**IMPACTO**	**MITIGACIÓN**
Saturación del servidor (disco duro)	El SGA estaría fuera de servicio y posible pérdida de la información	Mantenimiento al servidor cada mes (limpieza de archivos temporales) y llevar a cabo los respaldos correspondientes
Hacker/cracker	-Acceso no autorizado al sistema -Robo de información -Borrado de información	Instalación y monitoreo un detector de intrusos, firewall, el cual detectará quien accede al servidor.
Problemas técnicos en la red del SITE de la DGPyFE	EL SGA estaría fuera de servicio y posible pérdida de la información	La DGPyFE ha tomado las medidas pertinentes para el resguardo de la información ante cualquier contingencia
Cortes de luz	El SGA estaría fuera de servicio y posible pérdida de la información	Se desarrollo un proceso de monitoreo dentro una aplicación para revisar la conexión entre servidores
Certificado de seguridad	Desconfianza de los clientes al momento de enviar sus datos personales.	Configuración, renovación y actualización del certificado de seguridad para asegurar que los datos personales del cliente están seguros al momento de realizar el registro.
No contar con respaldos	Pérdida de la información	- Guardar información en discos extraíbles - Guardar información en la nube
Actualizar el sistema	No se podrá acceder al sistema SGA y por ende, no se generará	Realizar la actualización en un horario que no afecte el servicio de la operación

	ningún registro de las operaciones cotidianas	

ANEXO 5

ANÁLISIS DE BRECHA Y MEDIDAS DE SEGURIDAD

Dirección General de Publicaciones y Fomento Editorial		
Abreviatura del nombre del sistema	**TE**	
Nombre del sistema	**Tienda electrónica libros UNAM**	
ANÁLISIS DE BRECHA		
MEDIDAS DE SEGURIDAD ACTUAL	**MEDIDAS DE SEGURIDAD NECESARIAS**	**ACCIONES PARA REMEDIACIÓN**
Control de cambios operacionales	Elaboración de procedimientos	- Discutir, documentar y evaluar cualquier cambio que pueda afectar las operaciones relacionadas con datos personales
Protección contra software malicioso	Políticas de seguridad y control respecto al software malicioso	- Descargar el software de sitios confiables para el caso de código abierto - Instalar software con licencia
Respaldo de la información	Respaldos periódicos	- Probar los respaldos periódicamente para asegurar su correcto funcionamiento
Registros de operadores	Poder acceder a los registros de las actividades dentro del sistema	- Analizar periódicamente los registros de actividad
Revisión de privilegios de usuarios	Revisión periódica para verificar el adecuado y no excesivo uso de los privilegios de cada usuario	- Revisión a usuarios con privilegios especiales cada semestre.
Trazabilidad de tratamiento	Identificar quién tuvo acceso a los datos personales	- Monitoreo en el servidor y administración de magento.
Registro de eventos	generar registros de excepciones y eventos relevantes de seguridad	- Almacenar los datos y registros y evaluarlos en un periodo acordado para investigación y control de acceso de usuarios.
Control de software y sistemas	Probar cualquier cambio o actualización de sistemas críticos antes de implementarse en la organización	- Se deben aplicar los cambios a una copia concreta del software original y evaluar su funcionamiento y con ello evitar la pérdida de la información
Procedimientos de actualización de SGSDP	Revisión y actualización de las medidas de seguridad .	- Elaborar procedimientos para evitar la vulneración a la seguridad y mejorar el SGSDP
Dirección General de Publicaciones y Fomento Editorial		
Abreviatura del nombre del sistema	**FD**	
Nombre del sistema	**Facturación Digital**	
ANÁLISIS DE BRECHA		
MEDIDAS DE SEGURIDAD ACTUAL	**MEDIDAS DE SEGURIDAD NECESARIAS**	**ACCIONES PARA REMEDIACIÓN**
Control de cambios operacionales	Elaboración de procedimientos	Discutir, documentar y evaluar cualquier cambio que pueda afectar las operaciones relacionadas con datos personales
Estándares de configuración segura y actualización del sistema FD.	Identificar necesidades, así como, nuevas versiones del sistema	Configuraciones seguras en el sistema y base de datos
Protección contra software malicioso	Políticas de seguridad y control respecto al software malicioso	Instalar software con licencia
Respaldo de la información	Respaldos periódicos	Probar los respaldos periódicamente para asegurar su correcto funcionamiento

Seguridad en sistemas electrónicos	Llevar a cabo un uso adecuado del sistema de datos personales	Reducir el riesgo a través de guías y gestión de riesgos asociados con dicho sistema
Revisión de privilegios de usuarios	Revisión periódica para verificar el adecuado y no excesivo uso de los privilegios de cada usuario	Revisión a usuarios con privilegios especiales
Trazabilidad de tratamiento	Identificar quién tuvo acceso a los datos personales	Monitoreo con Patronato Universitario al detectar una anomalía
Registro de eventos	Generar registros de excepciones y eventos relevantes de seguridad	Almacenar los datos y registros y evaluarlos en un periodo acordado para investigación y control de acceso de usuarios.
Procedimientos de actualización de SGSDP	Revisión y actualización de las medidas de seguridad	Elaborar procedimientos para evitar la vulneración a la seguridad y mejorar el SGSDP
Dirección General de Publicaciones y Fomento Editorial		
Abreviatura del nombre del sistema	**SIC**	
Nombre del sistema	**Sistema Institucional de Compras**	
ANÁLISIS DE BRECHA		
MEDIDAS DE SEGURIDAD ACTUAL	**MEDIDAS DE SEGURIDAD NECESARIAS**	**ACCIONES PARA REMEDIACIÓN**
Control de cambios operacionales	Elaboración de procedimientos	Discutir, documentar y evaluar cualquier cambio que pueda afectar las operaciones relacionadas con datos personales
Estándares de configuración segura y actualización del sistema FD.	Identificar necesidades, así como, nuevas versiones del sistema	Configuraciones seguras en el sistema y base de datos
Protección contra software malicioso	Políticas de seguridad y control respecto al software malicioso	Instalar software con licencia
Respaldo de la información	Respaldos periódicos	Probar los respaldos periódicamente para asegurar su correcto funcionamiento
Seguridad en sistemas electrónicos	Llevar a cabo un uso adecuado del sistema de datos personales	Reducir el riesgo a través de guías y gestión de riesgos asociados con dicho sistema
Revisión de privilegios de usuarios	Revisión periódica para verificar el adecuado y no excesivo uso de los privilegios de cada usuario	Revisión a usuarios con privilegios especiales
Trazabilidad de tratamiento	Identificar quién tuvo acceso a los datos personales	Monitoreo con la Secretaría Administrativa al detectar una anomalía
Registro de eventos	Generar registros de excepciones y eventos relevantes de seguridad	Almacenar los datos y registros y evaluarlos en un periodo acordado para investigación y control de acceso de usuarios.
Procedimientos de actualización de SGSDP	Revisión y actualización de las medidas de seguridad	Elaborar procedimientos para evitar la vulneración a la seguridad y mejorar el SGSDP
Dirección General de Publicaciones y Fomento Editorial		
Abreviatura del nombre del sistema	**PPC**	
Nombre del sistema	**Padrón de Proveedores y Contratistas**	
ANÁLISIS DE BRECHA		
MEDIDAS DE SEGURIDAD ACTUAL	**MEDIDAS DE SEGURIDAD NECESARIAS**	**ACCIONES PARA REMEDIACIÓN**

Control de cambios operacionales	Elaboración de procedimientos	Discutir, documentar y evaluar cualquier cambio que pueda afectar las operaciones relacionadas con datos personales
Estándares de configuración segura y actualización del sistema FD.	Identificar necesidades, así como, nuevas versiones del sistema	Configuraciones seguras en el sistema y base de datos
Protección contra software malicioso	Políticas de seguridad y control respecto al software malicioso	Instalar software con licencia
Respaldo de la información	Respaldos periódicos	Probar los respaldos periódicamente para asegurar su correcto funcionamiento
Seguridad en sistemas electrónicos	Llevar a cabo un uso adecuado del sistema de datos personales	Reducir el riesgo a través de guías y gestión de riesgos asociados con dicho sistema
Revisión de privilegios de usuarios	Revisión periódica para verificar el adecuado y no excesivo uso de los privilegios de cada usuario	Revisión a usuarios con privilegios especiales
Trazabilidad de tratamiento	Identificar quién tuvo acceso a los datos personales	Monitoreo con Patronato Universitario al detectar una anomalía
Registro de eventos	Generar registros de excepciones y eventos relevantes de seguridad	Almacenar los datos y registros y evaluarlos en un periodo acordado para investigación y control de acceso de usuarios.
Procedimientos de actualización de SGSDP	Revisión y actualización de las medidas de seguridad	Elaborar procedimientos para evitar la vulneración a la seguridad y mejorar el SGSDP
Dirección General de Publicaciones y Fomento Editorial		
Abreviatura del nombre del sistema	**SIAF**	
Nombre del sistema	**Sistema Integral de Administración Financiera**	
ANÁLISIS DE BRECHA		
MEDIDAS DE SEGURIDAD ACTUAL	**MEDIDAS DE SEGURIDAD NECESARIAS**	**ACCIONES PARA REMEDIACIÓN**
Control de cambios operacionales	Elaboración de procedimientos	Discutir, documentar y evaluar cualquier cambio que pueda afectar las operaciones relacionadas con datos personales
Estándares de configuración segura y actualización del sistema SIAF.	Identificar necesidades, así como, nuevas versiones del sistema	Configuraciones seguras en el sistema y base de datos
Protección contra software malicioso	Políticas de seguridad y control respecto al software malicioso	Instalar software con licencia o autorización
Respaldo de la información	Respaldos periódicos	Probar los respaldos periódicamente para asegurar su correcto funcionamiento
Seguridad en sistemas electrónicos	Llevar a cabo un uso adecuado del sistema de datos personales	Reducir el riesgo a través de guías y gestión de riesgos asociados con dicho sistema
Revisión de privilegios de usuarios	Revisión periódica para verificar el adecuado y no excesivo uso de los privilegios de cada usuario	Revisión a usuarios con privilegios especiales
Trazabilidad de tratamiento	Identificar quién tuvo acceso a los datos personales	Monitoreo con el Instituto de Ingeniería al detectar una anomalía

Registro de eventos	Generar registros de excepciones y eventos relevantes de seguridad	Almacenar los datos y registros y evaluarlos en un periodo acordado para investigación y control de acceso de usuarios.
Procedimientos de actualización de SGSDP	Revisión y actualización de las medidas de seguridad	Elaborar procedimientos para evitar la vulneración a la seguridad y mejorar el SGSDP
Dirección General de Publicaciones y Fomento Editorial		
Abreviatura del nombre del sistema	**SGA**	
Nombre del sistema	**Intelisis - Papyrus**	
ANÁLISIS DE BRECHA		
MEDIDAS DE SEGURIDAD ACTUAL	**MEDIDAS DE SEGURIDAD NECESARIAS**	**ACCIONES PARA REMEDIACIÓN**
Control de cambios operacionales	Elaboración de procedimientos	Discutir, documentar y evaluar cualquier cambio que pueda afectar las operaciones relacionadas con datos personales
Protección contra software malicioso	Políticas de seguridad y control respecto al software malicioso	- Descargar el software de sitios confiables para el caso de código abierto - Instalar software con licencia
Respaldo de la información	Respaldos periódicos	Probar los respaldos periódicamente para asegurar su correcto funcionamiento
Registros de operadores	Poder acceder a los registros de las actividades dentro del sistema	Analizar periódicamente los registros de actividad
Revisión de privilegios de usuarios	Revisión periódica para verificar el adecuado y no excesivo uso de los privilegios de cada usuario	Revisión a usuarios con privilegios especiales cada semestre.
Trazabilidad de tratamiento	Identificar quién tuvo acceso a los datos personales	Monitoreo en el servidor y administración del SGA.
Registro de eventos	Generar registros de excepciones y eventos relevantes de seguridad	Almacenar los datos y registros y evaluarlos en un periodo acordado para investigación y control de acceso de usuarios.
Control de software y sistemas	Probar cualquier cambio o actualización de sistemas críticos antes de implementarse en la organización	Se deben aplicar los cambios a una copia concreta del software original y evaluar su funcionamiento y con ello evitar la pérdida de la información
Procedimientos de actualización de SGSDP	Revisión y actualización de las medidas de seguridad.	Elaborar procedimientos para evitar la vulneración a la seguridad y mejorar el SGSDP
Dirección General de Publicaciones y Fomento Editorial		
Abreviatura del nombre del sistema	**TE**	
Nombre del sistema	**Tienda electrónica libros UNAM**	
MEDIDAS DE SEGURIDAD		
¿Cómo se obtienen los datos personales?	Físico ( ) Digital (X) Ambos ( )	
¿Para qué se utilizan los datos personales?	Para enviar información a Patronato Universitario y a través de este, se realicen las transacciones de compra con la institución BBVA. Para el envío por paquetería (DHL) de los artículos adquiridos en la TE Para el registro de usuarios	
¿Los datos se transfieren o remiten?	Remiten (X) Transfieren ( )	
	¿A quién se remiten?	¿Para qué se remiten?

	Áreas Universitarias (X) Patronato Universitario Otro (X) Mensajería DHL	A Patronato Universitario, para emitir CFDI, tickets y transacciones con BBVA A DHL, para el envío al cliente los artículos adquiridos.
	¿A quién se transfieren? Gobierno Federal ( ) Gobierno Estatal ( ) Gobierno Municipal ( ) Personas Físicas ( ) Personas Morales ( ) **NO APLICA**	¿Para qué se transfieren? **NO APLICA**
¿Cuánto tiempo se da tratamiento?	Aproximadamente 15 días, contando desde la compra hasta la entrega de documentos fiscales y los artículos.	
¿Cómo se remiten los datos personales?	Mediante portales institucionales (DHL) y servicios web de Patronato Universitario Datos cifrados (X) Algoritmo sha Acuse de recibido (X) El sistema indica que ha sido aceptado el movimiento cuando se genera el CFDI o ticket Registra la transferencia en bitácora (X**)** Se registra el folio de Patronato del ticket o CFDI, los datos de la compra, la referencia bancaria y número de pedido en la base de datos de magento.	
Dirección General de Publicaciones y Fomento Editorial		
Abreviatura del nombre del sistema	**FD**	
Nombre del sistema	**Facturación Digital**	
MEDIDAS DE SEGURIDAD		
¿Cómo se obtienen los datos personales?	Físico ( ) Digital (X) Ambos ( )	
¿Para qué se utilizan los datos personales?	Para la elaboración de documentos fiscales (factura)	
¿Los datos se transfieren o remiten?	Remiten (X) Transfieren ( )	
	¿A quién se remiten? Áreas Universitarias (X) Otro (X) Al sistema de Facturación Digital Patronato Universitario, instituciones bancarias y SAT	¿Para qué se remiten? Para la elaboración de documentos fiscales (factura) y el timbrado de las mismas al PAC
	¿A quién se transfieren? Gobierno Federal ( ) Gobierno Estatal ( ) Gobierno Municipal ( ) Personas Físicas ( )	¿Para qué se transfieren? **NO APLICA**

	Personas Morales ( ) **NO APLICA**	
¿Cuánto tiempo se da tratamiento?	Aproximadamente 5 días.	
¿Cómo se remiten los datos personales?	A través del sistema de Facturación Digital	
Dirección General de Publicaciones y Fomento Editorial		
Abreviatura del nombre del sistema	**SIC**	
Nombre del sistema	**Sistema Institucional de Compras**	
MEDIDAS DE SEGURIDAD		
¿Cómo se obtienen los datos personales?	Físico ( ) Digital ( ) Ambos (X)	
¿Para qué se utilizan los datos personales?	Para realizar los pagos correspondientes de los servicios que se reciben en la DGPyFE.	
¿Los datos se transfieren o remiten?	Remiten (X) Transfieren ( )	
	¿A quién se remiten? Áreas Universitarias (X) Secretaría Administrativa Otro ( )	¿Para qué se remiten? A la Secretaría Administrativa, para realizar los pagos correspondientes.
	¿A quién se transfieren? Gobierno Federal ( ) Gobierno Estatal ( ) Gobierno Municipal ( ) Personas Físicas ( ) Personas Morales ( ) **NO APLICA**	¿Para qué se transfieren? **NO APLICA**
¿Cuánto tiempo se da tratamiento?	Aproximadamente dos meses, dependiendo de las condiciones de cada área y tipo de producto (extranjero)	
¿Cómo se remiten los datos personales?	Mediante el Sistema Institucional de Compras Datos cifrados (X) Acuse de recibido (X) Registra la transferencia en bitácora (**)**	
Dirección General de Publicaciones y Fomento Editorial		
Abreviatura del nombre del sistema	**PPC**	
Nombre del sistema	**Padrón de Proveedores y Contratistas**	
MEDIDAS DE SEGURIDAD		
¿Cómo se obtienen los datos personales?	Físico ( ) Digital (X) Ambos ( )	
¿Para qué se utilizan los datos personales?	Para el registro del proveedor en el padrón.	
¿Los datos se transfieren o remiten?	Remiten (X) Transfieren ( )	
	¿A quién se remiten? Áreas Universitarias (X) Otro (X) Al sistema de Padrón de Proveedores y Contratistas de Patronato Universitario.	¿Para qué se remiten? Para dar de alta al proveedor en el sistema de Padrón de Proveedores con los que cuenta la UNAM.
	¿A quién se transfieren?	¿Para qué se transfieren?

	Gobierno Federal ( ) Gobierno Estatal ( ) Gobierno Municipal ( ) Personas Físicas ( ) Personas Morales ( ) **NO APLICA**	**NO APLICA**
¿Cuánto tiempo se da tratamiento?	Aproximadamente 5 días.	
¿Cómo se remiten los datos personales?	A través del sistema de Padrón de Proveedores y Contratistas	
Dirección General de Publicaciones y Fomento Editorial		
Abreviatura del nombre del sistema	**SIAF**	
Nombre del sistema	**Sistema Integral de Administración Financiera**	
MEDIDAS DE SEGURIDAD		
¿Cómo se obtienen los datos personales?	Físico ( ) Digital ( ) Ambos (X)	
¿Para qué se utilizan los datos personales?	Para realizar procesos de egresos, almacén, PAPIIT, CONACYT, órdenes de compra, formas múltiples, ingresos extraordinarios, convenios y contratos, en la DGPyFE.	
¿Los datos se transfieren o remiten?	Remiten (X) Transfieren ( )	
	¿A quién se remiten? Áreas Universitarias (X) Instituto de Ingeniería Otro ( )	¿Para qué se remiten? Al Instituto de Ingeniería, para realizar los trámites correspondientes a través del SIAF
	¿A quién se transfieren? Gobierno Federal ( ) Gobierno Estatal ( ) Gobierno Municipal ( ) Personas Físicas ( ) Personas Morales ( ) **NO APLICA**	¿Para qué se transfieren? **NO APLICA**
¿Cuánto tiempo se da tratamiento?	Aproximadamente un mes, dependiendo de las condiciones de cada área y tipo de trámite que se trate.	
¿Cómo se remiten los datos personales?	Mediante el Sistema Integral de Administración Financiera MEDIDAS DE SEGURIDAD Datos cifrados (X) Acuse de recibido (X) Registra la transferencia en bitácora (**)**	
Dirección General de Publicaciones y Fomento Editorial		
Abreviatura del nombre del sistema	**SGA**	
Nombre del sistema	**Intelisis - Papyrus**	
MEDIDAS DE SEGURIDAD		
¿Cómo se obtienen los datos personales?	Físico ( ) Digital ( ) Ambos (X)	
¿Para qué se utilizan los datos personales?	Para realizar ventas, pagos, pedidos de artículos y registro de proveedores y clientes. Con ello llevar a cabo la comercialización y adquisición del acervo.	
¿Los datos se transfieren o remiten?	Remiten (X) Transfieren ( )	
	¿A quién se remiten?	¿Para qué se remiten?

	Áreas Universitarias (X) Otro ( )	A la Secretaría de Finanzas para realizar los pagos correspondientes.
	¿A quién se transfieren? Gobierno Federal ( ) Gobierno Estatal ( ) Gobierno Municipal ( ) Personas Físicas ( ) Personas Morales ( ) **NO APLICA**	¿Para qué se transfieren? **NO APLICA**
¿Cuánto tiempo se da tratamiento?	Los períodos para pago son de 30, 60, 90 días, contando desde el registro de la compra. Cuando se realiza una consignación va de 30, 60, 90 días, contando desde el registro de la venta. Estas operaciones varían dependiendo de las características del proveedor y del cliente.	
¿Cómo se remiten los datos personales?	Mediante correo electrónico Datos cifrados ( ) Acuse de recibido ( ) Registra la transferencia en bitácora (X**)** Se registra el SGA.	
Dirección General de Publicaciones y Fomento Editorial		
Abreviatura del nombre del sistema	**TE**	
Nombre del sistema	**Tienda electrónica libros UNAM**	
RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS		
Medias de seguridad implementadas para su resguardo	**NO APLICA**	
Personas con acceso a los soportes físicos del sistema	**NO APLICA**	
Dirección General de Publicaciones y Fomento Editorial		
Abreviatura del nombre del sistema	**FD**	
Nombre del sistema	**Facturación Digital**	
RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS		
Medias de seguridad implementadas para su resguardo	**NO APLICA**	
Personas con acceso a los soportes físicos del sistema	**NO APLICA**	

Dirección General de Publicaciones y Fomento Editorial	
Abreviatura del nombre del sistema	**SIC**
Nombre del sistema	**Sistema Institucional de Compras**
RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS	
Medias de seguridad implementadas para su resguardo	Se realizan los resguardos en archiveros
Personas con acceso a los soportes físicos del sistema	El personal autorizado que cuenta con las credenciales.
Dirección General de Publicaciones y Fomento Editorial	

Abreviatura del nombre del sistema	**PPC**
Nombre del sistema	**Padrón de Proveedores y Contratistas**
RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS	
Medias de seguridad implementadas para su resguardo	**NO APLICA**
Personas con acceso a los soportes físicos del sistema	**NO APLICA**
Dirección General de Publicaciones y Fomento Editorial	
Abreviatura del nombre del sistema	**SIAF**
Nombre del sistema	**Sistema Integral de Administración Financiera**
RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS	
Medias de seguridad implementadas para su resguardo	Se realizan los resguardos en archiveros
Personas con acceso a los soportes físicos del sistema	El personal autorizado que cuenta con las credenciales.
Dirección General de Publicaciones y Fomento Editorial	
Abreviatura del nombre del sistema	**SGA**
Nombre del sistema	**Intelisis - Papyrus**
RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS	
Medias de seguridad implementadas para su resguardo	Los resguardos se realizan en archiveros de cada área que tiene tratamiento de los datos personales.
Personas con acceso a los soportes físicos del sistema	El personal autorizado que cuenta con las credenciales de acceso al SGA.
Dirección General de Publicaciones y Fomento Editorial	
Abreviatura del nombre del sistema	**TE**
Nombre del sistema	**Tienda electrónica libros UNAM**
RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES DIGITALES	
Medias de seguridad implementadas para su resguardo	Los resguardos digitales se realizan en el área de sistemas, se llevan a cabo a través de medios digitales, con una periodicidad de cada ocho días. Esta medida se realiza como protección, ya que todos estos resguardos los genera DGTIC. Las medidas de seguridad con las que cuenta la coordinación de sistemas en donde se encuentran los soportes son: cámaras de seguridad y puertas con acceso controlado (huella digital y clave).
Personas con acceso a los soportes físicos del sistema	1. Karen Hernández Negrete – Coordinadora de sistemas 2. Marlene Fernández – Asistente de procesos
Dirección General de Publicaciones y Fomento Editorial	
Abreviatura del nombre del sistema	**FD**
Nombre del sistema	**Facturación Digital**
RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES DIGITALES	
Medias de seguridad implementadas para su resguardo	Esta medida de seguridad la realiza Patronato Universitario. Las medidas de seguridad con las que cuenta Patronato Universitario y la coordinación de sistemas en donde se encuentran los soportes son: cámaras de seguridad y puertas con acceso controlado (huella digital y clave).
Personas con acceso a los soportes físicos del sistema	Sólo pueden acceder al sistema de Facturación Digital, los usuarios que cuentan con usuario y contraseña, aprobada por Patronato Universitario.
Dirección General de Publicaciones y Fomento Editorial	
Abreviatura del nombre del sistema	**SIC**
Nombre del sistema	**Sistema Institucional de Compras**
RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES DIGITALES	
Medias de seguridad implementadas para su resguardo	Esta medida se realiza como protección, ya que todos estos resguardos los genera la Secretaría Administrativa. Las medidas de seguridad con las que

	cuenta la coordinación de sistemas en donde se encuentran los soportes son: cámaras de seguridad y puertas con acceso controlado (huella digital y clave).
Personas con acceso a los soportes físicos del sistema	David Gómez – jefe de la Unidad Administrativa Karen Hernández Negrete – Coordinadora de sistemas
Dirección General de Publicaciones y Fomento Editorial	
Abreviatura del nombre del sistema	**PPC**
Nombre del sistema	**Padrón de Proveedores y Contratistas**
RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES DIGITALES	
Medias de seguridad implementadas para su resguardo	Esta medida de seguridad la realiza Patronato Universitario. Las medidas de seguridad con las que cuenta Patronato Universitario y la coordinación de sistemas en donde se encuentran los soportes son: cámaras de seguridad y puertas con acceso controlado (huella digital y clave).
Personas con acceso a los soportes físicos del sistema	Sólo pueden acceder al sistema de Padrón de Proveedores y Contratistas, los usuarios que cuentan con usuario y contraseña, aprobada por Patronato Universitario.
Dirección General de Publicaciones y Fomento Editorial	
Abreviatura del nombre del sistema	**SIAF**
Nombre del sistema	**Sistema Integral de Administración Financiera**
RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES DIGITALES	
Medias de seguridad implementadas para su resguardo	Esta medida se realiza como protección, ya que todos estos resguardos los genera el Instituto de Ingeniería. Las medidas de seguridad con las que cuenta la coordinación de sistemas en donde se encuentran los soportes son: cámaras de seguridad y puertas con acceso controlado (huella digital y clave).
Personas con acceso a los soportes físicos del sistema	David Gómez – jefe de la Unidad Administrativa Karen Hernández Negrete – Coordinadora de sistemas
Dirección General de Publicaciones y Fomento Editorial	
Abreviatura del nombre del sistema	**SGA**
Nombre del sistema	**Intelisis - Papyrus**
RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES DIGITALES	
Medias de seguridad implementadas para su resguardo	Los resguardos digitales se realizan en el área de sistemas, se llevan a cabo a través de medios digitales, con una periodicidad diaria y cada 8 días de forma integral. Esta medida se realiza como protección ante cualquier eventualidad. Las medidas de seguridad con las que cuenta la coordinación de sistemas en donde se encuentran los soportes son: cámaras de seguridad y puertas con acceso controlado (huella digital y clave).
Personas con acceso a los soportes físicos del sistema	- David Gómez – jefe de la Unidad Administrativa - Los responsables que cuentan con las credenciales en el SGA para el tratamiento de datos personales
Dirección General de Publicaciones y Fomento Editorial	
Abreviatura del nombre del sistema	**TE**
Nombre del sistema	**Tienda electrónica libros UNAM**
REGISTRO DE INCIDENTES	
Descripción del procedimiento de atención de incidentes: 1. Realizar un informe del incidente al momento de detectarlo. 2. Se analizará el incidente para determinar la o las soluciones pertinentes. 3. El tiempo de respuesta a los incidentes deberá de ser máximo un día 4. Prevenir la ocurrencia de posibles incidentes de acuerdo al plan estratégico 5. Establecer variables de posibles riesgos de falla y tomar medidas. 6. Realizar una bitácora de los eventos ocurridos, fecha de inicio y término, incidente y medidas de solución. 7. Tener un enfoque estructurado y planificado que permita manejar de manera eficiente los incidentes.	

¿Quién y cada cuánto analiza(n) la(s) bitácora(s)?	Karen Hernández Negrete – Coordinadora de sistemas Marlene Fernández Martínez – Asistente de procesos La revisión se realizará semanalmente.
Dirección General de Publicaciones y Fomento Editorial	
Abreviatura del nombre del sistema	**FD**
Nombre del sistema	**Facturación Digital**
REGISTRO DE INCIDENTES	

Descripción del procedimiento de atención de incidentes:

1. Realizar un informe del incidente al momento de detectarlo a Patronato Universitario.
2. Se analizará el incidente para determinar la o las soluciones pertinentes en conjunto con Patronato Universitario.
3. El tiempo de respuesta a los incidentes dependerá del tiempo que considere Patronato Universitario.
4. Prevenir la ocurrencia de posibles incidentes de acuerdo al plan estratégico
5. Establecer variables de posibles riesgos de falla y tomar medidas.
6. Realizar una bitácora de los eventos ocurridos, fecha de inicio y término, incidente y medidas de solución.
7. Tener un enfoque estructurado y planificado que permita manejar de manera eficiente los incidentes.

¿Quién y cada cuánto analiza(n) la(s) bitácora(s)?	Karen Hernández Negrete – Coordinadora de sistemas Marlene Fernández Martínez – Asistente de procesos Oscar Santamaria González - Sistemas La revisión se realiza mensualmente.
Dirección General de Publicaciones y Fomento Editorial	
Abreviatura del nombre del sistema	**SIC**
Nombre del sistema	**Sistema Institucional de Compras**
REGISTRO DE INCIDENTES	

Descripción del procedimiento de atención de incidentes:

1. El encargado elaborará y entregará un informe al responsable, al menos 24 horas después de haber ocurrido el incidente;
2. En hoja de cálculo se describirá el incidente, quién resolvió, los archivos dañados y los archivos recuperados. Esta hoja se encontrará protegida por contraseña en el servicio de nube.
3. En caso de robo o extravío de datos personales, el responsable del sistema de tratamiento de datos personales, dará aviso inmediato al titular de la dependencia o entidad para su conocimiento.
4. Se deberá dar aviso a la Unidad de Transparencia de la UNAM, en un máximo de 48 horas de haber ocurrido el incidente, quien podrá sugerir acudir con el/la titular del área jurídica para presentar denuncias o querellas ante el MP para que, en el ámbito de sus atribuciones determine lo conducente.

Con el acompañamiento de la Unidad de Transparencia de la UNAM:

5. Máximo 3 días naturales después de haber ocurrido el incidente, el responsable del sistema de tratamiento de datos personales dará aviso al/los titular(es) mediante un desplegado de prensa en los medios y periódicos de mayor circulación, a fin de que estos puedan tomar las medidas necesarias para la defensa de sus derechos;
6. Máximo 5 días naturales de haber ocurrido el incidente, si éste fuera por robo o extravío de datos personales, el responsable del sistema de tratamiento de datos personales dará aviso por escrito a los titulares de dicha información para que tomen sus precauciones ante el posible uso ilegal de su información debiendo obtener acuse de recibido, adicionalmente se podrá dar aviso telefónicamente.
7. La información que el responsable deberá informar al/los titular(es) al menos debe ser la siguiente:
    a. La naturaleza del incidente:
    b. Los datos personales comprometidos;
    c. Recomendaciones acerca de las medidas que el/los titular(es) puede(n) adoptar para proteger sus intereses;
    d. Las acciones correctivas realizadas de forma inmediata
    e. Los medios donde puede(n) obtener más información al respecto
8. El responsable deberá analizar las causas por las cuales se pudo haber presentado el incidente e implementará en

su plan de trabajo las acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales a efecto de evitar futuros incidentes.

9. El responsable describirá en una bitácora:
    a. El incidente ocurrido;
    b. El motivo de éste;
    c. Quién lo resolvió;
    d. Las acciones correctivas implementadas de forma inmediata y definitiva.
    e. Los oficios documentos, expedientes, estantes o archiveros, tanto los dañados como los recuperados (para soportes físicos); y
    f. Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto los dañados como los recuperados, el nombre de los sistemas y la infraestructura afectada, además de indicar si el incidente afectó el servidor principal y los servidores de respaldo (para soportes electrónicos)

A la fecha de realización del presente documento no se ha presentado vulneración alguna a los soportes físicos ni electrónicos.

¿Quién y cada cuánto analiza(n) la(s) bitácora(s)?	Karen Hernández Negrete – Coordinadora de sistemas La revisión se realiza mensualmente.
Dirección General de Publicaciones y Fomento Editorial	
Abreviatura del nombre del sistema	**PPC**
Nombre del sistema	**Padrón de Proveedores y Contratistas**

REGISTRO DE INCIDENTES

Descripción del procedimiento de atención de incidentes:

1. Realizar un informe del incidente al momento de detectarlo a Patronato Universitario.
2. Se analizará el incidente para determinar la o las soluciones pertinentes en conjunto con Patronato Universitario.
3. El tiempo de respuesta a los incidentes dependerá del tiempo que considere Patronato Universitario.
4. Prevenir la ocurrencia de posibles incidentes de acuerdo al plan estratégico
5. Establecer variables de posibles riesgos de falla y tomar medidas.
6. Realizar una bitácora de los eventos ocurridos, fecha de inicio y término, incidente y medidas de solución.
7. Tener un enfoque estructurado y planificado que permita manejar de manera eficiente los incidentes.

¿Quién y cada cuánto analiza(n) la(s) bitácora(s)?	Karen Hernández Negrete – Coordinadora de sistemas María de Jesús Cadena – Compras La revisión se realiza mensualmente.
Dirección General de Publicaciones y Fomento Editorial	
Abreviatura del nombre del sistema	**SIAF**
Nombre del sistema	**Sistema Integral de Administración Financiera**

REGISTRO DE INCIDENTES

Descripción del procedimiento de atención de incidentes:

1. El encargado elaborará y entregará un informe al responsable, al menos 24 horas después de haber ocurrido el incidente;
2. En hoja de cálculo se describirá el incidente, quién resolvió, los archivos dañados y los archivos recuperados. Esta hoja se encontrará protegida por contraseña en el servicio de nube.
3. En caso de robo o extravío de datos personales, el responsable del sistema de tratamiento de datos personales, dará aviso inmediato al titular de la dependencia o entidad para su conocimiento.
4. Se deberá dar aviso a la Unidad de Transparencia de la UNAM, en un máximo de 48 horas de haber ocurrido el incidente, quien podrá sugerir acudir con el/la titular del área jurídica para presentar denuncias o querellas ante el MP para que, en el ámbito de sus atribuciones determine lo conducente.

Con el acompañamiento de la Unidad de Transparencia de la UNAM:

5. Máximo 3 días naturales después de haber ocurrido el incidente, el responsable del sistema de tratamiento de datos personales dará aviso al/los titular(es) mediante un desplegado de prensa en los medios y periódicos de mayor circulación, a fin de que estos puedan tomar las medidas necesarias para la defensa de sus derechos;

6. Máximo 5 días naturales de haber ocurrido el incidente, si éste fuera por robo o extravío de datos personales, el responsable del sistema de tratamiento de datos personales dará aviso por escrito a los titulares de dicha información para que tomen sus precauciones ante el posible uso ilegal de su información debiendo obtener acuse de recibido, adicionalmente se podrá dar aviso telefónicamente.
7. La información que el responsable deberá informar al/los titular(es) al menos debe ser la siguiente:
    a. La naturaleza del incidente
    b. Los datos personales comprometidos;
    c. Recomendaciones acerca de las medidas que el/los titular(es) puede(n) adoptar para proteger sus intereses;
    d. Las acciones correctivas realizadas de forma inmediata
    e. Los medios donde puede(n) obtener más información al respecto
8. El responsable deberá analizar las causas por las cuales se pudo haber presentado el incidente e implementará en su plan de trabajo las acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales a efecto de evitar futuros incidentes.
9. El responsable describirá en una bitácora:
    a. El incidente ocurrido;
    b. El motivo de éste;
    c. Quién lo resolvió;
    d. Las acciones correctivas implementadas de forma inmediata y definitiva.
    e. Los oficios documentos, expedientes, estantes o archiveros, tanto los dañados como los recuperados (para soportes físicos); y
    f. Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto los dañados como los recuperados, el nombre de los sistemas y la infraestructura afectada, además de indicar si el incidente afectó el servidor principal y los servidores de respaldo (para soportes electrónicos)

A la fecha de realización del presente documento no se ha presentado vulneración alguna a los soportes físicos ni electrónicos.

¿Quién y cada cuánto analiza(n) la(s) bitácora(s)?	Karen Hernández Negrete – Coordinadora de sistemas La revisión se realiza mensualmente.

Dirección General de Publicaciones y Fomento Editorial	
Abreviatura del nombre del sistema	**SGA**
Nombre del sistema	**Intelisis - Papyrus**

REGISTRO DE INCIDENTES

Descripción del procedimiento de atención de incidentes:

1. Realizar un informe del incidente al momento de detectarlo.
2. Se analizará el incidente para determinar la o las soluciones pertinentes.
3. El tiempo de respuesta a los incidentes se llevará a cabo en conjunto con la empresa Intelisis, quien es el proveedor que nos da soporte técnico del SGA.
4. Prevenir la ocurrencia de posibles incidentes de acuerdo al plan estratégico.
5. Establecer variables de posibles riesgos de falla y tomar medidas.
6. Realizar una bitácora de los eventos ocurridos, fecha de inicio y término, incidente y medidas de solución.
7. Tener un enfoque estructurado y planificado que permita manejar de manera eficiente los incidentes.

¿Quién y cada cuánto analiza(n) la(s) bitácora(s)?	Karen Hernández Negrete – Coordinadora de sistemas Marlene Fernández Martínez – Asistente de procesos Alejandro Hernández Carmona - Sistemas La revisión se realizará mensualmente.

Dirección General de Publicaciones y Fomento Editorial	
Abreviatura del nombre del sistema	**TE**
Nombre del sistema	**Tienda electrónica libros UNAM**

ACCESO A LAS INSTALACIONES. SEGURIDAD PERIMETRAL INTERIOR

Medidas de seguridad implementadas en los espacios donde se encuentran los soportes físicos	Las medidas de seguridad con las que cuenta la coordinación de sistemas en donde se encuentran los soportes son: cámaras de seguridad y puertas con acceso controlado (huella digital y clave).
Medidas de seguridad implementadas en los espacios donde se encuentran los soportes electrónicos	Los soportes digitales se encuentran en el servidor virtual de la DGTIC y cuenta con las medidas de seguridad que se requieren para este resguardo de la información.
REGISTRO DE INCIDENTES	
La DGTIC cuenta con las medidas de seguridad que se requieren para el resguardo de la información, así como, tiene restringido el acceso a personal no autorizado al centro de datos.	
Dirección General de Publicaciones y Fomento Editorial	
Abreviatura del nombre del sistema	**FD**
Nombre del sistema	**Facturación Digital**
ACCESO A LAS INSTALACIONES. SEGURIDAD PERIMETRAL INTERIOR	
Medidas de seguridad implementadas en los espacios donde se encuentran los soportes físicos	Las medidas de seguridad con las que cuenta Patronato Universitario y la Coordinación de sistemas de la DGPyFE en donde se encuentran los servidores son: cámaras de seguridad y puertas con acceso controlado (huella digital y clave).
Medidas de seguridad implementadas en los espacios donde se encuentran los soportes electrónicos	Los soportes digitales se encuentran en el servidor de Patronato Universitario y cuenta con las medidas de seguridad que se requieren para el resguardo de la información.
REGISTRO DE INCIDENTES	
Patronato Universitario cuenta con las medidas de seguridad que se requieren para el resguardo de la información, así como, tiene restringido el acceso a personal no autorizado al centro de datos.	
Dirección General de Publicaciones y Fomento Editorial	
Abreviatura del nombre del sistema	**SIC**
Nombre del sistema	**Sistema Institucional de Compras**
ACCESO A LAS INSTALACIONES. SEGURIDAD PERIMETRAL INTERIOR	
Medidas de seguridad implementadas en los espacios donde se encuentran los soportes físicos	Las medidas de seguridad con las que cuentan las áreas que usan el SIC en donde se encuentran los soportes son: cámaras de seguridad.
Medidas de seguridad implementadas en los espacios donde se encuentran los soportes electrónicos	Los soportes digitales se encuentran en los servidores de la Secretaría Administrativa y cuenta con las medidas de seguridad que se requieren para este resguardo de la información.
REGISTRO DE INCIDENTES	
La Secretaría Administrativa cuenta con las medidas de seguridad que se requieren para el resguardo de la información, así como, tiene restringido el acceso a personal no autorizado al centro de datos.	
Dirección General de Publicaciones y Fomento Editorial	
Abreviatura del nombre del sistema	**PPC**
Nombre del sistema	**Padrón de Proveedores y Contratistas**
ACCESO A LAS INSTALACIONES. SEGURIDAD PERIMETRAL INTERIOR	
Medidas de seguridad implementadas en los espacios donde se encuentran los soportes físicos	Las medidas de seguridad con las que cuenta Patronato Universitario y la Coordinación de sistemas de la DGPyFE en donde se encuentran los servidores son: cámaras de seguridad y puertas con acceso controlado (huella digital y clave).
Medidas de seguridad implementadas en los espacios donde se encuentran los soportes electrónicos	Los soportes digitales se encuentran en el servidor de Patronato Universitario y cuenta con las medidas de seguridad que se requieren para el resguardo de la información.
REGISTRO DE INCIDENTES	
Patronato Universitario cuenta con las medidas de seguridad que se requieren para el resguardo de la información, así como, tiene restringido el acceso a personal no autorizado al centro de datos.	
Dirección General de Publicaciones y Fomento Editorial	

Abreviatura del nombre del sistema	**SIAF**
Nombre del sistema	**Sistema Integral de Administración Financiera**
ACCESO A LAS INSTALACIONES. SEGURIDAD PERIMETRAL INTERIOR	
Medidas de seguridad implementadas en los espacios donde se encuentran los soportes físicos	Las medidas de seguridad con las que cuentan las áreas que usan el SIAF en donde se encuentran los soportes son: cámaras de seguridad y puerta con acceso controlado.
Medidas de seguridad implementadas en los espacios donde se encuentran los soportes electrónicos	Los soportes digitales se encuentran en los servidores del Instituto de Ingeniería y cuenta con las medidas de seguridad que se requieren para este resguardo de la información.
REGISTRO DE INCIDENTES	
El Instituto de Ingeniería cuenta con las medidas de seguridad que se requieren para el resguardo de la información, así como, tiene restringido el acceso a personal no autorizado al centro de datos.	
Dirección General de Publicaciones y Fomento Editorial	
Abreviatura del nombre del sistema	**SGA**
Nombre del sistema	**Intelisis - Papyrus**
ACCESO A LAS INSTALACIONES. SEGURIDAD PERIMETRAL INTERIOR	
Medidas de seguridad implementadas en los espacios donde se encuentran los soportes físicos	Las medidas de seguridad con las que cuenta la coordinación de sistemas en donde se encuentran los soportes son: cámaras de seguridad y puertas con acceso controlado (huella digital y clave).
Medidas de seguridad implementadas en los espacios donde se encuentran los soportes electrónicos	Los soportes digitales se encuentran en el servidor que se encuentra en el SITE de la coordinación de sistemas de la DGPyFE y cuenta con las medidas de seguridad que se requieren para el resguardo de la información.
REGISTRO DE INCIDENTES	
La coordinación de sistemas de la DGPyFE cuenta con las medidas de seguridad necesarias para el resguardo de la información, así como, tiene restringido el acceso a personal no autorizado al centro de datos, cámaras de seguridad y puertas con acceso controlado (huella digital y clave).	
Dirección General de Publicaciones y Fomento Editorial	
Abreviatura del nombre del sistema	**TE**
Nombre del sistema	**Tienda electrónica libros UNAM**
PERFILES DE USUARIO Y CONTRASEÑA	
Los accesos a la TE se determinaron de acuerdo al nivel de autorización y de acuerdo a las tareas asignadas.	
Perfiles de usuario y contraseñas en el sistema operativo de red (X**)**	Se tiene cuidado especial y riguroso en el perfil de usuarios. Se utiliza un cifrado de datos a través de SHA (algoritmo criptográfico).
Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de datos personales (X**)**	Podemos agregar usuarios, aparte del administrador, que puedan acceder al panel de control de nuestra tienda. Y, a la vez, podemos asignarles roles específicos para que sólo tengan acceso a ciertas partes de la misma.
Administración de perfiles de usuario y contraseñas	¿Quién da de alta nuevos perfiles? Karen Hernández Negrete – Coordinadora de sistemas Marlene Fernández Martínez – Asistente de procesos
	¿Quién autoriza la creación de nuevos perfiles? Karen Hernández Negrete – Coordinadora de sistemas
	¿Se lleva registro de la creación de nuevos perfiles? Si (X) No ( )
Acceso remoto al sistema de tratamiento de datos personales	¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema? Si (X) No ( )
	¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento? Si (X) No ( )
	¿Cómo se evita el acceso remoto no autorizado?

	Bloqueando el acceso a terceros a la cuenta root y aumentando el nivel de seguridad creando usuario y contraseñas con: mayúsculas, minúsculas, números y caracteres especiales.
Dirección General de Publicaciones y Fomento Editorial	
Abreviatura del nombre del sistema	**FD**
Nombre del sistema	**Facturación Digital**
PERFILES DE USUARIO Y CONTRASEÑA	
Los accesos al sistema de Facturación Digital los otorga Patronato Universitario, con previa solicitud de la Unidad administrativa y/o la Coordinación de sistemas.	
Perfiles de usuario y contraseñas en el sistema operativo de red (X)	Se tiene cuidado especial y riguroso en el perfil de usuarios de acuerdo a las tareas asignadas.
Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de datos personales (X)	Los perfiles de usuario se solicitan a Patronato Universitario de acuerdo a las tareas asignadas al personal de la DGPyFE, para que sólo tengan acceso a ciertos módulos del sistema de facturación.
Administración de perfiles de usuario y contraseñas	¿Quién da de alta nuevos perfiles? Patronato Universitario
	¿Quién autoriza la creación de nuevos perfiles? David Gómez – Unidad Administrativa Karen Hernández Negrete – Coordinadora de sistemas
	¿Se lleva registro de la creación de nuevos perfiles? Si (X) No ( )
Acceso remoto al sistema de tratamiento de datos personales	¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema? Si (X) No ( )
	¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento? Si (X) No ( )
	¿Cómo se evita el acceso remoto no autorizado? Bloqueando el acceso a terceros a la cuenta root y aumentando el nivel de seguridad creando usuario y contraseñas con: mayúsculas, minúsculas, números y caracteres especiales.
Dirección General de Publicaciones y Fomento Editorial	
Abreviatura del nombre del sistema	**SIC**
Nombre del sistema	**Sistema Institucional de Compras**
PERFILES DE USUARIO Y CONTRASEÑA	
Los accesos al SIC se determinaron de acuerdo al nivel de autorización y de acuerdo a las tareas asignadas. Las contraseñas son cifradas y creadas por cada uno de los usuarios	
Perfiles de usuario y contraseñas en el sistema operativo de red (X)	Se tiene cuidado especial y riguroso en el perfil de usuarios. Se utiliza un cifrado de datos.
Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de datos personales (X)	Dicho software ofrece un manejo riguroso de perfiles de usuario y contraseñas y cifra los nombres de usuario y las contraseñas cuando las almacena
Administración de perfiles de usuario y contraseñas	¿Quién da de alta nuevos perfiles? Jefe de Unidad Administrativa.
	¿Quién autoriza la creación de nuevos perfiles? David Gómez – Unidad Administrativa
	¿Se lleva registro de la creación de nuevos perfiles? Si ( ) No (X)
Acceso remoto al sistema de tratamiento de datos personales	¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema? Si (X) No ( )

	¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento? Si ( ) No (X)
	¿Cómo se evita el acceso remoto no autorizado? - Mediante claves con varios caracteres especiales - Las claves son personales e intransferibles
Dirección General de Publicaciones y Fomento Editorial	
Abreviatura del nombre del sistema	**PPC**
Nombre del sistema	**Padrón de Proveedores y Contratistas**
PERFILES DE USUARIO Y CONTRASEÑA	
Los accesos al sistema de Padrón de Proveedores y Contratistas los otorga Patronato Universitario, con previa solicitud de la Unidad administrativa y/o la Coordinación de sistemas.	
Perfiles de usuario y contraseñas en el sistema operativo de red (X)	Se tiene cuidado especial y riguroso en el perfil de usuarios de acuerdo a las tareas asignadas.
Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de datos personales (X)	Los perfiles de usuario se solicitan a Patronato Universitario de acuerdo a las tareas asignadas al personal de la DGPyFE, para que sólo tengan acceso a ciertos módulos del sistema de facturación.
Administración de perfiles de usuario y contraseñas	¿Quién da de alta nuevos perfiles? Patronato Universitario
	¿Quién autoriza la creación de nuevos perfiles? David Gómez – Unidad Administrativa
	¿Se lleva registro de la creación de nuevos perfiles? Si (X) No ( )
Acceso remoto al sistema de tratamiento de datos personales	¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema? Si (X) No ( )
	¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento? Si (X) No ( )
	¿Cómo se evita el acceso remoto no autorizado? Bloqueando el acceso a terceros a la cuenta root y aumentando el nivel de seguridad creando usuario y contraseñas con: mayúsculas, minúsculas, números y caracteres especiales.
Dirección General de Publicaciones y Fomento Editorial	
Abreviatura del nombre del sistema	**SIAF**
Nombre del sistema	**Sistema Integral de Administración Financiera**
PERFILES DE USUARIO Y CONTRASEÑA	
Los accesos al SIAF se determinaron de acuerdo al nivel de autorización y de acuerdo a las tareas asignadas. Las contraseñas son cifradas y creadas por cada uno de los usuarios	
Perfiles de usuario y contraseñas en el sistema operativo de red (X)	Se tiene cuidado especial y riguroso en el perfil de usuarios. Se utiliza un cifrado de datos.
Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de datos personales (X)	Dicho software ofrece un manejo riguroso de perfiles de usuario y contraseñas y cifra los nombres de usuario y las contraseñas cuando las almacena
Administración de perfiles de usuario y contraseñas	¿Quién da de alta nuevos perfiles? El Instituto de Ingeniería
	¿Quién autoriza la creación de nuevos perfiles? David Gómez – Unidad Administrativa
	¿Se lleva registro de la creación de nuevos perfiles? Si (X) No ( )

Acceso remoto al sistema de tratamiento de datos personales	¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema? Si (X) No ( )
	¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento? Si ( ) No (X)
	¿Cómo se evita el acceso remoto no autorizado? - Mediante claves con varios caracteres especiales - Las claves son personales e intransferibles
Dirección General de Publicaciones y Fomento Editorial	
Abreviatura del nombre del sistema	**SGA**
Nombre del sistema	**Intelisis - Papyrus**
PERFILES DE USUARIO Y CONTRASEÑA	
Los accesos al SGA se determinaron de acuerdo al nivel de autorización y de acuerdo a las tareas asignadas.	
Perfiles de usuario y contraseñas en el sistema operativo de red (X)	Se tiene cuidado especial y riguroso en el perfil de usuarios. Se utiliza un cifrado de datos a través de SHA (algoritmo criptográfico).
Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de datos personales (X)	Podemos agregar usuarios, aparte del administrador, para que pueda acceder a las bases de datos del SGA, así como, podemos asignar roles específicos para que sólo tengan acceso a ciertos módulos del mismo.
Administración de perfiles de usuario y contraseñas	¿Quién da de alta nuevos perfiles? Karen Hernández Negrete – Coordinadora de sistemas Alejandro Hernández Carmona – Sistemas
	¿Quién autoriza la creación de nuevos perfiles? David Gómez – Unidad Administrativa Karen Hernández Negrete – Coordinadora de sistemas Subdirectores
	¿Se lleva registro de la creación de nuevos perfiles? Si (X) No ( )
Acceso remoto al sistema de tratamiento de datos personales	¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema? Si (X) No ( )
	¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento? Si (X) No ( )
	¿Cómo se evita el acceso remoto no autorizado? Bloqueando el acceso a terceros a la cuenta root y aumentando el nivel de seguridad creando usuario y contraseñas con: mayúsculas, minúsculas, números y caracteres especiales, adicional se cuenta con firewall.
Dirección General de Publicaciones y Fomento Editorial	
Abreviatura del nombre del sistema	**TE**
Nombre del sistema	**Tienda electrónica libros UNAM**
PROCEDIMIENTO DE RESPALDO Y RECUPERACIÓN DE DATOS	
- El resguardo se realiza en dispositivos externos (disco duro). - Se realizan respaldos semanales de programación y base de datos. - DGTIC realiza snapshots semanalmente. - La recuperación se realiza a través de los respaldos generados periódicamente. - Los respaldos se tienen bajo resguardo en la coordinación de sistemas.	
Dirección General de Publicaciones y Fomento Editorial	
Abreviatura del nombre del sistema	**FD**
Nombre del sistema	**Facturación Digital**
PROCEDIMIENTO DE RESPALDO Y RECUPERACIÓN DE DATOS	

- Patronato Universitario realiza respaldos de acuerdo a su cronograma. - La recuperación se realiza a través de los respaldos generados periódicamente. - Los respaldos se tienen bajo resguardo de Patronato Universitario
Dirección General de Publicaciones y Fomento Editorial
Abreviatura del nombre del sistema | **SIC**
Nombre del sistema | **Sistema Institucional de Compras**
PROCEDIMIENTO DE RESPALDO Y RECUPERACIÓN DE DATOS
- La Secretaría Administrativa/Dirección de Proveeduría/Patronato Universitario realiza respaldos de acuerdo a su cronograma. - La recuperación se realiza a través de los respaldos generados periódicamente. - Los respaldos se tienen bajo resguardo de la La Secretaría Administrativa/Dirección de Proveeduría/Patronato Universitario.
Dirección General de Publicaciones y Fomento Editorial
Abreviatura del nombre del sistema | **PPC**
Nombre del sistema | **Padrón de Proveedores y Contratistas**
PROCEDIMIENTO DE RESPALDO Y RECUPERACIÓN DE DATOS
- Patronato Universitario realiza respaldos de acuerdo a su cronograma. - La recuperación se realiza a través de los respaldos generados periódicamente. - Los respaldos se tienen bajo resguardo de Patronato Universitario
Dirección General de Publicaciones y Fomento Editorial
Abreviatura del nombre del sistema | **SIAF**
Nombre del sistema | **Sistema Integral de Administración Financiera**
PROCEDIMIENTO DE RESPALDO Y RECUPERACIÓN DE DATOS
- El resguardo se realiza en dispositivos externos (disco duro). - Se realizan respaldos semanales de programación y base de datos. - El Instituto de Ingeniería realiza snapshots semanalmente. - La recuperación se realiza a través de los respaldos generados periódicamente. - Los respaldos se tienen bajo resguardo del Instituto de Ingeniería.
Dirección General de Publicaciones y Fomento Editorial
Abreviatura del nombre del sistema | **SGA**
Nombre del sistema | **Intelisis - Papyrus**
PROCEDIMIENTO DE RESPALDO Y RECUPERACIÓN DE DATOS
- El resguardo se realiza en dispositivos externos (disco duro) y BaaS. - Se realizan respaldos semanales de programación y base de datos. - La coordinación de sistemas realiza snapshots semanalmente. - La recuperación se realiza a través de los respaldos generados periódicamente. - Los respaldos se tienen bajo resguardo en la coordinación de sistemas.

ANEXO 6

PLAN DE TRABAJO

Dirección General de Publicaciones y Fomento Editorial			
Abreviatura del nombre del sistema	**TE**		
Nombre del sistema	**Tienda electrónica libros UNAM**		
ACTIVIDAD	**DESCRIPCIÓN**	**DURACIÓN**	**COBERTURA**
Elaborar políticas de datos personales	Establecer políticas de seguridad de la información que le permita planear de acuerdo con el rol asignado	Continuo	Alta Grupo 1 Mitigar
Realizar bitácoras	Elaborar las bitácoras de las acciones que se llevan a cabo dentro de la TE, para tener el control de los accesos autorizados y no autorizados a la información.	Continuo	Alta Grupo 1 Mitigar
Procedimientos de actualización de SGSDP	Deben existir procedimientos de revisión y actualización de las medidas de seguridad una vez mitigada la vulneración a la seguridad para mejorar el SGSDP.	Continuo	Media Grupo 2 Mitigar o aplazar
Estándares de configuración segura y actualización de sistemas, con el objeto de asegurar la información	Se deben tener identificadas las necesidades de nuevos sistemas, actualizaciones o nuevas versiones. Es recomendable realizar pruebas antes de implementar cualquiera de ellos, para evitar pérdidas de información	Continuo	Media Grupo 2 Mitigar o aplazar
Respaldo de la información	Se debe tener un adecuado control sobre la periodicidad de generación de respaldos y el respectivo almacenaje de los soportes físicos/electrónicos, especialmente para el ejercicio de derechos ARCO	Semanal	Alta Grupo 1 Mitigar
Registro de fallas en el sistema para evitar pérdida de información	Las fallas en sistemas y activos deben poder reportarse y gestionarse, esto incluye la corrección de la falla y revisión de los registros, para salvaguardar la información.	Semanal	Alta Grupo 1 Mitigar
Brindar mantenimiento al firewall del servidor y realizar reportes de monitoreo para evitar el hacker/cracker de la información	Realizar periódicamente el monitoreo del firewall para controlar el acceso no autorizado	Mensual	Alta Grupo 1 Mitigar
Documentación de seguridad del sistema	Toda la documentación de los sistemas y activos de información debe ser protegida de acceso no autorizado	Continuo	Media Grupo 2 Mitigar o aplazar
Reglas de control de acceso para asegurar el tratamiento de la información	Deben existir reglas y privilegios para cada usuario o grupo de usuarios conforme a sus responsabilidades	Continuo	Media Grupo 2 Mitigar o aplazar
Gestión de usuarios y contraseñas para asegurar la información dentro del sistema	Cada usuario debe tener un identificador único en el sistema al cuál se vincularán sus privilegios y acceso	Continuo	Media Grupo 2 Mitigar o aplazar
Protección de datos	Proteger los datos personales que obran en la TE y sobre los cuales se efectúa algún tratamiento tomando las medidas necesarias para cumplir con los principios y obligaciones señaladas en la Ley general de protección de datos personales	Continuo	Alta Grupo 1 Mitigar
Aviso de privacidad	Solicitar el consentimiento para el uso de datos personales	Continuo	Alta Grupo 1

			Mitigar
Dirección General de Publicaciones y Fomento Editorial			
Abreviatura del nombre del sistema	**FD**		
Nombre del sistema	**Facturación Digital**		
ACTIVIDAD	**DESCRIPCIÓN**	**DURACIÓN**	**COBERTURA**
Estándares de configuración segura y actualización de la versión del FD	Es recomendable realizar la actualización en horarios que no interfiera con la actividad de los usuarios	Cuando Patronato Universitario lo determine	Media Grupo 2 Mitigar o aplazar
Elaborar políticas de datos personales	Establecer políticas de seguridad de la información que le permita planear de acuerdo con el rol asignado	Continuo	Media Grupo 2 Mitigar o aplazar
Realizar bitácoras	Elaborar las bitácoras de los incidentes ocurridos y reportarlos a Patronato Universitario	Continuo	Alta Grupo 1 Mitigar
Procedimientos de actualización de SGSDP	Deben existir procedimientos de revisión y actualización de las medidas de seguridad una vez mitigada la vulneración a la seguridad para mejorar el SGSDP.	Continuo	Media Grupo 2 Mitigar o aplazar
Registro de fallas en el sistema para evitar pérdida de información	Las fallas en el FD se deben reportar y gestionar ante Patronato Universitario	Continuo	Alta Grupo 1 Mitigar
Brindar mantenimiento al firewall del servidor y realizar reportes de monitoreo	Realizar periódicamente el monitoreo del firewall para controlar el acceso no autorizado	Continuo	Alta Grupo 1 Mitigar
Gestión de usuarios y contraseñas para asegurar la información dentro del sistema	Cada usuario debe tener un identificador único en el sistema al cuál se vincularán sus privilegios y acceso	Continuo	Media Grupo 2 Mitigar o aplazar
Aviso de privacidad	Solicitar el consentimiento para el uso de datos personales	Continuo	Alta Grupo 1 Mitigar
Dirección General de Publicaciones y Fomento Editorial			
Abreviatura del nombre del sistema	**SIC**		
Nombre del sistema	**Sistema Institucional de Compras**		
ACTIVIDAD	**DESCRIPCIÓN**	**DURACIÓN**	**COBERTURA**
Estándares de configuración segura y actualización de la versión del SIC	Es recomendable realizar la actualización en horarios que no interfiera con la actividad de los usuarios	Cuando la Secretaría Administrativa lo determine	Media Grupo 2 Mitigar o aplazar
Elaborar políticas de datos personales	Establecer políticas de seguridad de la información que le permita planear de acuerdo con el rol asignado	Continuo	Media Grupo 2 Mitigar o aplazar
Realizar bitácoras	Elaborar las bitácoras de los incidentes ocurridos y reportarlos a la Secretaría Administrativa para evitar la pérdida de la información	Continuo	Alta Grupo 1 Mitigar
Procedimientos de actualización de SGSDP	Deben existir procedimientos de revisión y actualización de las medidas de seguridad una vez mitigada la	Continuo	Media Grupo 2 Mitigar o aplazar

	vulneración a la seguridad para mejorar el SGSDP.		
Registro de fallas en el sistema para evitar pérdida de información	Las fallas en el SIC se deben reportar y gestionar ante la Secretaría Administrativa	Continuo	Alta Grupo 1 Mitigar
Brindar mantenimiento al firewall del servidor y realizar reportes de monitoreo	Realizar periódicamente el monitoreo del firewall para controlar el acceso no autorizado	Continuo	Alta Grupo 1 Mitigar
Gestión de usuarios y contraseñas para asegurar la información dentro del sistema	Cada usuario debe tener un identificador único en el sistema al cuál se vincularán sus privilegios y acceso	Continuo	Media Grupo 2 Mitigar o aplazar
Aviso de privacidad	Solicitar el consentimiento para el uso de datos personales	Continuo	Alta Grupo 1 Mitigar
Dirección General de Publicaciones y Fomento Editorial			
Abreviatura del nombre del sistema	**PPC**		
Nombre del sistema	**Padrón de Proveedores y Contratistas**		
ACTIVIDAD	**DESCRIPCIÓN**	**DURACIÓN**	**COBERTURA**
Estándares de configuración segura y actualización de la versión del PPC	Es recomendable realizar la actualización en horarios que no interfiera con la actividad de los usuarios	Cuando Patronato Universitario lo determine	Media Grupo 2 Mitigar o aplazar
Elaborar políticas de datos personales	Establecer políticas de seguridad de la información que le permita planear de acuerdo con el rol asignado	Continuo	Media Grupo 2 Mitigar o aplazar
Realizar bitácoras	Elaborar las bitácoras de los incidentes ocurridos y reportarlos a Patronato Universitario	Continuo	Alta Grupo 1 Mitigar
Procedimientos de actualización de SGSDP	Deben existir procedimientos de revisión y actualización de las medidas de seguridad una vez mitigada la vulneración a la seguridad para mejorar el SGSDP.	Continuo	Media Grupo 2 Mitigar o aplazar
Registro de fallas en el sistema para evitar pérdida de información	Las fallas en el PPC se deben reportar y gestionar ante Patronato Universitario	Continuo	Alta Grupo 1 Mitigar
Brindar mantenimiento al firewall del servidor y realizar reportes de monitoreo	Realizar periódicamente el monitoreo del firewall para controlar el acceso no autorizado	Continuo	Alta Grupo 1 Mitigar
Gestión de usuarios y contraseñas para asegurar la información dentro del sistema	Cada usuario debe tener un identificador único en el sistema al cuál se vincularán sus privilegios y acceso	Continuo	Media Grupo 2 Mitigar o aplazar
Aviso de privacidad	Solicitar el consentimiento para el uso de datos personales	Continuo	Alta Grupo 1 Mitigar
Dirección General de Publicaciones y Fomento Editorial			
Abreviatura del nombre del sistema	**SIAF**		
Nombre del sistema	**Sistema Integral de Administración Financiera**		
ACTIVIDAD	**DESCRIPCIÓN**	**DURACIÓN**	**COBERTURA**

Estándares de configuración segura y actualización de la versión del SIAF	Es recomendable realizar la actualización en horarios que no interfiera con la actividad de los usuarios	Cuando el Instituto de Ingeniería lo determine	Media Grupo 2 Mitigar o aplazar
Elaborar políticas de datos personales	Establecer políticas de seguridad de la información que le permita planear de acuerdo con el rol asignado	Continuo	Media Grupo 2 Mitigar o aplazar
Realizar bitácoras	Elaborar las bitácoras de los incidentes ocurridos y reportarlos al Instituto de Ingeniería para evitar la pérdida de la información	Continuo	Alta Grupo 1 Mitigar
Procedimientos de actualización de SGSDP	Deben existir procedimientos de revisión y actualización de las medidas de seguridad una vez mitigada la vulneración a la seguridad para mejorar el SGSDP.	Continuo	Media Grupo 2 Mitigar o aplazar
Registro de fallas en el sistema para evitar pérdida de información	Las fallas en el SIAF se deben reportar y gestionar ante el Instituto de Ingeniería	Continuo	Alta Grupo 1 Mitigar
Brindar mantenimiento al firewall del servidor y realizar reportes de monitoreo	Realizar periódicamente el monitoreo del firewall para controlar el acceso no autorizado	Continuo	Alta Grupo 1 Mitigar
Gestión de usuarios y contraseñas para asegurar la información dentro del sistema	Cada usuario debe tener un identificador único en el sistema al cuál se vincularán sus privilegios y acceso	Continuo	Media Grupo 2 Mitigar o aplazar
Aviso de privacidad	Solicitar el consentimiento para el uso de datos personales	Continuo	Alta Grupo 1 Mitigar

Dirección General de Publicaciones y Fomento Editorial			
Abreviatura del nombre del sistema	**SGA**		
Nombre del sistema	**Intelisis - Papyrus**		
ACTIVIDAD	**DESCRIPCIÓN**	**DURACIÓN**	**COBERTURA**
Elaborar políticas de datos personales	Establecer políticas de seguridad de la información que le permita planear de acuerdo con el rol asignado	Continuo	Media Grupo 2 Mitigar o Aplazar
Realizar bitácoras	Elaborar las bitácoras de las acciones que se llevan a cabo dentro del SGA, para tener el control de los accesos autorizados y no autorizados a la información.	Continuo	Media Grupo 2 Mitigar o Aplazar
Procedimientos de actualización de SGSDP	Deben existir procedimientos de revisión y actualización de las medidas de seguridad una vez mitigada la vulneración a la seguridad para mejorar el SGSDP.	Continuo	Media Grupo 2 Mitigar o aplazar
Estándares de configuración segura y actualización de sistemas, con el objeto de asegurar la información	Se deben tener identificadas las necesidades de nuevos sistemas, actualizaciones o nuevas versiones. Es recomendable realizar pruebas antes de implementar cualquiera de ellos, para evitar pérdidas de información	Continuo	Media Grupo 2 Mitigar o aplazar
Respaldo de la información	Se debe tener un adecuado control sobre la periodicidad de generación de respaldos y el respectivo almacenaje de los soportes	Semanal	Alta Grupo 1 Mitigar

	físicos/electrónicos, especialmente para el ejercicio de derechos ARCO		
Registro de fallas en el sistema para evitar pérdida de información	Las fallas en sistemas y activos deben poder reportarse y gestionarse, esto incluye la corrección de la falla y revisión de los registros, para salvaguardar la información.	Semanal	Alta Grupo 1 Mitigar
Brindar mantenimiento al firewall del servidor y realizar reportes de monitoreo para evitar el hacker/cracker de la información	Realizar periódicamente el monitoreo del firewall para controlar el acceso no autorizado	Mensual	Alta Grupo 1 Mitigar
Documentación de seguridad del sistema	Toda la documentación de los sistemas y activos de información debe ser protegida de acceso no autorizado	Continuo	Media Grupo 2 Mitigar o aplazar
Reglas de control de acceso para asegurar el tratamiento de la información	Deben existir reglas y privilegios para cada usuario o grupo de usuarios conforme a sus responsabilidades	Continuo	Media Grupo 2 Mitigar o aplazar
Gestión de usuarios y contraseñas para asegurar la información dentro del sistema	Cada usuario debe tener un identificador único en el sistema al cuál se vincularán sus privilegios y acceso	Continuo	Media Grupo 2 Mitigar o aplazar
Protección de datos	Proteger los datos personales que obran en el SGA y sobre los cuales se efectúa algún tratamiento tomando las medidas necesarias para cumplir con los principios y obligaciones señaladas en la Ley general de protección de datos personales	Continuo	Alta Grupo 1 Mitigar
Aviso de privacidad	Solicitar el consentimiento para el uso de datos personales	Continuo	Alta Grupo 1 Mitigar

ANEXO 7

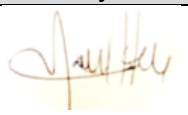
CAPACITACIÓN ADMINISTRATIVA BÁSICA

CAPACITACIÓN ADMINISTRATIVA BÁSICA	
DIRECCIÓN GENERAL DE PUBLICACIONES Y FOMENTO EDITORIAL	
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)

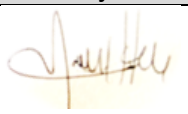
<table>
<tr><td colspan="3">Tienda electrónica libros UNAM</td><td colspan="2">DGPyFE/TE</td></tr>
<tr><td>Formato</td><td>1</td><td>Verificación anual</td><td>Acción concluida</td><td>( )</td></tr>
<tr><td colspan="2">Medida de seguridad técnica:</td><td colspan="3">Artículo 18. I. c) Utilizar datos no personales durante el desarrollo y pruebas de los sistemas.</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">Un día hábil.</td></tr>
<tr><td colspan="2">Importancia de la acción:</td><td colspan="3">Evitar usar datos personales mientras se está desarrollando, actualizando o modificando el código fuente de un sistema de información.</td></tr>
<tr><td colspan="2">Proceso recomendado:</td><td colspan="3">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.</td></tr>
<tr><td colspan="2">Mejores prácticas, referencias:</td><td colspan="3">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.</td></tr>
<tr><td colspan="2">Conocimientos requeridos:</td><td colspan="3">Administración de bases de datos. Consulta y actualización de tablas.</td></tr>
<tr><td colspan="3">Ejecución</td><td colspan="2">Fecha inicio</td></tr>
<tr><td colspan="3"> 
Karen Hernández Negrete</td><td colspan="2">01/08/2022</td></tr>
<tr><td colspan="3">Nombre y firma
Programador, desarrollador o diseñador del sistema de información</td><td colspan="2">Fecha término
01/08/2022</td></tr>
<tr><td>Observaciones / anotaciones</td><td colspan="4">Los privilegios que se determinan para cada usuario dentro de la DGPyFE, son única y exclusivamente, los relacionados con sus funciones y actividades laborales.</td></tr>
</table>

Tienda electrónica libros UNAM			DGPyFE/TE	
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**	
 Karen Hernández Negrete			01/08/2022	
Nombre y firma Administrador del sistema de información			**Fecha término** 01/08/2022	
Observaciones / anotaciones	Los privilegios que se determinan para cada usuario dentro de la DGPyFE, son única y exclusivamente, los que tienen que ver con sus actividades de trabajo.			

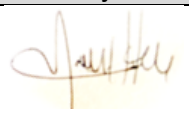
Tienda electrónica libros UNAM			DGPyFE/TE	
Formato:	**3**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 18. I. g) Instalar y mantener vigentes certificados de comunicación segura SSL en el caso de servicios basados en Web.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Dos 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**	
 Karen Hernández Negrete			01/08/2022	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** 02/08/2022	
Observaciones / anotaciones	Se tiene la previsión de mantener en todo momento actualizado el certificado de la tienda electrónica, de lo contrario estaría fuera de servicio.			

<table>
<tr><td colspan="3">Tienda electrónica libros UNAM</td><td colspan="2">DGPyFE/TE</td></tr>
<tr><td>Formato:</td><td>4</td><td>Verificación anual</td><td>Acción concluida</td><td>( )</td></tr>
<tr><td colspan="2">Medidas de seguridad técnicas:</td><td colspan="3">Artículo 18. I. h) Definir el plan de respaldos de la información, incluyendo periodicidad y alcance.</td></tr>
<tr><td colspan="2">Aplicable en:</td><td colspan="3">I. Bases de datos y sistemas de tratamiento.</td></tr>
<tr><td colspan="2">Tiempo estimado:</td><td colspan="3">Dos días hábiles.</td></tr>
<tr><td colspan="2">Importancia de la acción:</td><td colspan="3">En todo sistema de información es indispensable contar con un plan de respaldos periódicos, y especialmente en aquellos que contienen datos personales.</td></tr>
<tr><td colspan="2">Proceso recomendado:</td><td colspan="3">A) Elaborar documento con la secuencia de respaldos al menos con el siguiente orden:
- Diario – incremental.
- Semanal – incremental.
- Mensual – total.
B) Establecer en el plan los medios para resguardo del respaldo y su forma de identificación:
- En línea: mismo equipo donde se ejecuta el sistema.
- Respaldo como servicio: otro equipo de almacenamiento.
- Fuera de línea: medios magnéticos (cintas, discos) y/u ópticos.
C) Incluir en el plan:
- Responsables de cada tipo y medio de respaldo.
- Rotación de respaldos y medios.
- Áreas de resguardo.
- Métodos de cifrado.
- RTO: Recovery Time Objective. Tiempo objetivo de recuperación.
- RPO: Recovery Point Objective: Punto objetivo de recuperación.
D) Concluir este documento, adjuntarlo a SGPDP, llenar y firmar formato.</td></tr>
<tr><td colspan="2">Mejores prácticas, referencias:</td><td colspan="3">1.- Se deben tener al menos 3 respaldos del sistema y sus bases de datos en distintos medios.</td></tr>
<tr><td colspan="2">Conocimientos requeridos:</td><td colspan="3">Administración de sistema operativo. Gestión y programación de respaldos.</td></tr>
<tr><td colspan="3">Ejecución</td><td colspan="2">Fecha inicio</td></tr>
<tr><td colspan="3"> 
Karen Hernández Negrete</td><td colspan="2">02/08/2022</td></tr>
<tr><td colspan="3">Nombre y firma
Administrador del sistema de información o servidor</td><td colspan="2">Fecha término
03/08/2022</td></tr>
<tr><td>Observaciones / anotaciones</td><td colspan="4">- <u>Veeam (Respaldos locales)</u>
Tipo de respaldos: Incrementales a nivel de máquinas virtuales
Almacenamiento: Estos respaldos se almacenan en un Storage IBM Storwize V3700, con energía y fibras de transmisión de datos de forma redundante.
Ubicación: Centro de Datos de la dependencia de publicaciones digitales

- <u>BaaS (Backus as a Service)</u>
Tipo de respaldos: Respaldos mediante agente de Veeam a nivel de sistema operativo de cada servidor respaldado.
Almacenamiento: Este almacenamiento es administrado directamente por DGTIC.</td></tr>
</table>

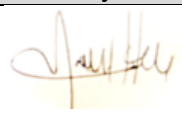
Tienda electrónica libros UNAM			DGPyFE/TE	
Formato:	**5**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 18. I. i) Definir el procedimiento para el borrado seguro.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Está en proceso de definición.		
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**	
 Karen Hernández Negrete				
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones	Está en proceso de definición.			

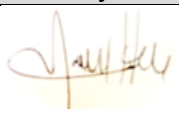
Tienda electrónica libros UNAM			DGPyFE/TE	
Formato:	**6**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 18. II. a) Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM**		
Aplicable en:		II. Sistemas operativos y servicios.		
Tiempo estimado:		Un día hábil.		
Importancia de la acción:		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.		
Proceso recomendado:		**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. *Por ejemplo*, 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.		
Mejores prácticas, referencias:		**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.		
Conocimientos requeridos:		Administración de sistema operativo.		
Ejecución			**Fecha inicio**	
 Karen Hernández Negrete				
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones	**NO APLICA**			

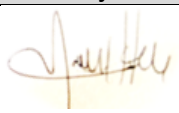
Tienda electrónica libros UNAM			DGPyFE/TE	
Formato:	**7**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 18. II. b) Instalar y mantener actualizado el software antimalware.**		
Aplicable en:		II. Sistemas operativos y servicios.		
Tiempo estimado:		Tres días 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**	
 Karen Hernández Negrete			03/08/2022	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
			05/08/2022	
Observaciones / anotaciones		Se mantiene actualizado y controlado este procedimiento a través de Kaspersky Security Center 13.2: Servicio optimizado para garantizar el mejor rendimiento, funciona en segundo plano, protegiendo sin ralentizar las PC, frente a las amenazas más recientes.		

Tienda electrónica libros UNAM			DGPyFE/TE	
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:		Dos 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**	
 Karen Hernández Negrete			02/08/2022	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** 03/08/2022	
Observaciones / anotaciones	Se mantienen como proceso continuo, actualizar las licencias de los sistemas que se encuentran en la DGPyFE.			

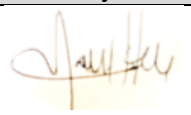
Tienda electrónica libros UNAM			DGPyFE/TE	
Formato:	**9**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 19. I. a) Aplicar un mecanismo de autenticación para las personas autorizadas con base en el principio del menor privilegio.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Dos 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**	
 Karen Hernández Negrete			03/08/2022	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** 04/08/2022	
Observaciones / anotaciones	Todos y cada uno de los privilegios asignados a cada usuario, están determinados de acuerdo a las actividades que desempeña.			

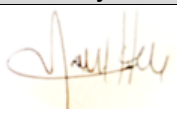
Tienda electrónica libros UNAM			DGPyFE/TE	
Formato:	**10**	**Verificación anual**	**Acción concluida**	( )
Medida de seguridad técnica:		**Artículo 19. II. b) Evitar la instalación de cualquier elemento de software que implique algún riesgo para el tratamiento de datos personales.**		
Aplicable en:		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**	
 Karen Hernández Negrete			03/08/2022	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** 04/08/2022	
Observaciones / anotaciones	Ningún usuario tiene los privilegios necesarios para instalar y desinstalar software			

Tienda electrónica libros UNAM			DGPyFE/TE	
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:		Tres 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**	
 Karen Hernández Negrete			02/08/2022	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** 04/08/2022	
Observaciones / anotaciones	Se cuenta con acceso controlado al personal que accede a la DGPyFE, así como, cámaras de seguridad.			

Tienda electrónica libros UNAM			DGPyFE/TE	
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**	
 Karen Hernández Negrete			05/08/2022	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** 05/08/2022	
Observaciones / anotaciones	Se cuenta con el formato estándar de control de entrada y salida de bienes proporcionado por las áreas administrativas de las entidades, así como, una bitácora de registro de salida y entrada de los mismos.			

Tienda electrónica libros UNAM			DGPyFE/TE	
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:		Dos 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**	
 Karen Hernández Negrete			04/08/2022	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** 05/08/2022	
Observaciones / anotaciones		SSL: En cada procesador de pagos (BBVA y PayPal) cuenta con certificado de SSL (Seguridad de la capa de transporte a través de protocolos criptográficos) en donde el cliente captura sus datos bancarios para realizar el pago de la compra.		

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

Facturación Digital			DGPyFE/FD	
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:		Determinado por Patronato Universitario		
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**	
 Karen Hernández Negrete			Determinado por Patronato Universitario	
Nombre y firma Programador, desarrollador o diseñador del sistema de información			**Fecha término**	
			Determinado por Patronato Universitario	
Observaciones / anotaciones	Estas medidas las lleva a cabo Patronato Universitario, quienes tienen toda la administración del sistema.			

Facturación Digital			DGPyFE/FD	
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:		Determinado por Patronato Universitario		
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**	
 Karen Hernández Negrete			Determinado por Patronato Universitario	
Nombre y firma Administrador del sistema de información			**Fecha término** Determinado por Patronato Universitario	
Observaciones / anotaciones	Estas medidas las lleva a cabo Patronato Universitario, quienes tienen toda la administración del sistema y de acuerdo a lo que la DGPyFE, le solicite para cada usuario.			

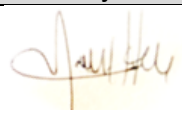
Facturación Digital			DGPyFE/FD	
Formato:	**3**	**Verificación anual**	**Acción concluida**	**( )**
Medidas de seguridad técnicas:		**Artículo 18. I. g) Instalar y mantener vigentes certificados de comunicación segura SSL en el caso de servicios basados en Web.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Determinado por Patronato Universitario		
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**	
 Karen Hernández Negrete			Determinado por Patronato Universitario	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** Determinado por Patronato Universitario	
Observaciones / anotaciones	Estas medidas las lleva a cabo Patronato Universitario, quienes tienen toda la administración del sistema.			

<table>
<tr><td colspan="3">Facturación Digital</td><td colspan="2">DGPyFE/FD</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">Determinado por Patronato Universitario</td></tr>
<tr><td colspan="2">Importancia de la acción:</td><td colspan="3">En todo sistema de información es indispensable contar con un plan de respaldos periódicos, y especialmente en aquellos que contienen datos personales.</td></tr>
<tr><td colspan="2">Proceso recomendado:</td><td colspan="3">A) Elaborar documento con la secuencia de respaldos al menos con el siguiente orden:
- Diario – incremental.
- Semanal – incremental.
- Mensual – total.
B) Establecer en el plan los medios para resguardo del respaldo y su forma de identificación:
- En línea: mismo equipo donde se ejecuta el sistema.
- Respaldo como servicio: otro equipo de almacenamiento.
- Fuera de línea: medios magnéticos (cintas, discos) y/u ópticos.
C) Incluir en el plan:
- Responsables de cada tipo y medio de respaldo.
- Rotación de respaldos y medios.
- Áreas de resguardo.
- Métodos de cifrado.
- RTO: Recovery Time Objective. Tiempo objetivo de recuperación.
- RPO: Recovery Point Objective: Punto objetivo de recuperación.
D) Concluir este documento, adjuntarlo a SGPDP, llenar y firmar formato.</td></tr>
<tr><td colspan="2">Mejores prácticas, referencias:</td><td colspan="3">1.- Se deben tener al menos 3 respaldos del sistema y sus bases de datos en distintos medios.</td></tr>
<tr><td colspan="2">Conocimientos requeridos:</td><td colspan="3">Administración de sistema operativo. Gestión y programación de respaldos.</td></tr>
<tr><td colspan="3">Ejecución</td><td colspan="2">Fecha inicio</td></tr>
<tr><td colspan="3"> 
Karen Hernández Negrete</td><td colspan="2">Determinado por Patronato Universitario</td></tr>
<tr><td colspan="3">Nombre y firma
Administrador del sistema de información o servidor</td><td colspan="2">Fecha término
Determinado por Patronato Universitario</td></tr>
<tr><td>Observaciones / anotaciones</td><td colspan="4">Estas medidas las lleva a cabo Patronato Universitario, quienes tienen toda la administración del sistema.</td></tr>
</table>

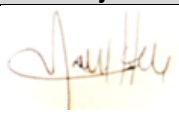
Facturación Digital			DGPyFE/FD	
Formato:	**5**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 18. I. i) Definir el procedimiento para el borrado seguro.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Determinado por Patronato Universitario		
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**	
 Karen Hernández Negrete			Determinado por Patronato Universitario	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** Determinado por Patronato Universitario	
Observaciones / anotaciones	Estas medidas las lleva a cabo Patronato Universitario, quienes tienen toda la administración del sistema.			

Facturación Digital			DGPyFE/FD	
Formato:	**6**	**Verificación anual**	**Acción concluida**	**( )**
Medidas de seguridad técnicas:		**Artículo 18. II. a) Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM**		
Aplicable en:		II. Sistemas operativos y servicios.		
Tiempo estimado:		Determinado por Patronato Universitario		
Importancia de la acción:		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.		
Proceso recomendado:		**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. *Por ejemplo*, 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.		
Mejores prácticas, referencias:		**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.		
Conocimientos requeridos:		Administración de sistema operativo.		
Ejecución			**Fecha inicio**	
 Karen Hernández Negrete			Determinado por Patronato Universitario	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** Determinado por Patronato Universitario	
Observaciones / anotaciones	Estas medidas las lleva a cabo Patronato Universitario, quienes tienen toda la administración del sistema.			

Facturación Digital			DGPyFE/FD	
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:		Determinado por Patronato Universitario		
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**	
 Karen Hernández Negrete			Determinado por Patronato Universitario	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** Determinado por Patronato Universitario	
Observaciones / anotaciones	Estas medidas las lleva a cabo Patronato Universitario, quienes tienen toda la administración del sistema.			

Facturación Digital			DGPyFE/FD	
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:		Determinado por Patronato Universitario		
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**	
 Karen Hernández Negrete			Determinado por Patronato Universitario	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** Determinado por Patronato Universitario	
Observaciones / anotaciones	Estas medidas las lleva a cabo Patronato Universitario, quienes tienen toda la administración del sistema.			

Facturación Digital			DGPyFE/FD	
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:		Determinado por Patronato Universitario		
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**	
Karen Hernández Negrete			Determinado por Patronato Universitario	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** Determinado por Patronato Universitario	
Observaciones / anotaciones	Estas medidas las lleva a cabo Patronato Universitario, quienes tienen toda la administración del sistema y de acuerdo a lo que solicite la DGPyFE.			

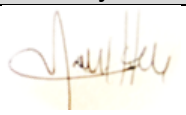
Facturación Digital			DGPyFE/FD	
Formato:	**10**	**Verificación anual**	**Acción concluida**	**( )**
Medida de seguridad técnica:		**Artículo 19. II. b) Evitar la instalación de cualquier elemento de software que implique algún riesgo para el tratamiento de datos personales.**		
Aplicable en:		II. Sistemas operativos.		
Tiempo estimado:		Determinado por Patronato Universitario		
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**	
 Karen Hernández Negrete			Determinado por Patronato Universitario	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** Determinado por Patronato Universitario	
Observaciones / anotaciones	Estas medidas las lleva a cabo Patronato Universitario, quienes tienen toda la administración del sistema.			

Facturación Digital			DGPyFE/FD	
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:		Determinado por Patronato Universitario		
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**	
Karen Hernández Negrete			Determinado por Patronato Universitario	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** Determinado por Patronato Universitario	
Observaciones / anotaciones	Estas medidas las lleva a cabo Patronato Universitario, quienes tienen toda la administración del sistema.			

Facturación Digital			DGPyFE/FD	
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:		Determinado por Patronato Universitario		
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**	
Karen Hernández Negrete			Determinado por Patronato Universitario	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor			Determinado por Patronato Universitario	
Observaciones / anotaciones	Estas medidas las lleva a cabo Patronato Universitario, quienes tienen toda la administración del sistema.			

Facturación Digital			DGPyFE/FD	
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:		Determinado por Patronato Universitario		
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**	
 Karen Hernández Negrete			Determinado por Patronato Universitario	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** Determinado por Patronato Universitario	
Observaciones / anotaciones	Estas medidas las lleva a cabo Patronato Universitario, quienes tienen toda la administración del sistema.			

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

Sistema Institucional de Compras			DGPyFE/SIC	
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:		Determinado por la Secretaría Administrativa		
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**	
 Karen Hernández Negrete			Determinado por la Secretaría Administrativa	
Nombre y firma Programador, desarrollador o diseñador del sistema de información			**Fecha término**	
			Determinado por la Secretaría Administrativa	
Observaciones / anotaciones	Estas medidas las lleva a cabo la Secretaría Administrativa, quienes tienen toda la administración del sistema.			

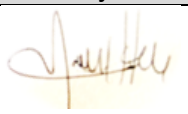
Sistema Institucional de Compras			DGPyFE/SIC	
Formato:	**2**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 18. I. e) Asignar o revocar los privilegios de acceso para los usuarios teniendo como base el principio del menor privilegio.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Determinado por la Secretaría Administrativa		
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**	
 Karen Hernández Negrete			Determinado por la Secretaría Administrativa	
Nombre y firma Administrador del sistema de información			**Fecha término** Determinado por la Secretaría Administrativa	
Observaciones / anotaciones	Estas medidas las lleva a cabo la Secretaría Administrativa, quienes tienen toda la administración del sistema y de acuerdo a lo que la DGPyFE, le solicite para cada usuario.			

Sistema Institucional de Compras			DGPyFE/SIC	
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:		Determinado por la Secretaría Administrativa		
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**	
 Karen Hernández Negrete			Determinado por la Secretaría Administrativa	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** Determinado por la Secretaría Administrativa	
Observaciones / anotaciones	Estas medidas las lleva a cabo la Secretaría Administrativa, quienes tienen toda la administración del sistema.			

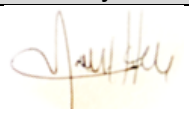
Sistema Institucional de Compras			DGPyFE/SIC	
Formato:	**4**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 18. I. h) Definir el plan de respaldos de la información, incluyendo periodicidad y alcance.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Determinado por la Secretaría Administrativa		
Importancia de la acción:		En todo sistema de información es indispensable contar con un plan de respaldos periódicos, y especialmente en aquellos que contienen datos personales.		
Proceso recomendado:		**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.		
Mejores prácticas, referencias:		**1.-** Se deben tener al menos 3 respaldos del sistema y sus bases de datos en distintos medios.		
Conocimientos requeridos:		Administración de sistema operativo. Gestión y programación de respaldos.		

Ejecución	**Fecha inicio**
 Karen Hernández Negrete	Determinado por la Secretaría Administrativa
Nombre y firma	**Fecha término**
Administrador del sistema de información o servidor	Determinado por la Secretaría Administrativa

Observaciones / anotaciones	Estas medidas las lleva a cabo la Secretaría Administrativa, quienes tienen toda la administración del sistema.

Sistema Institucional de Compras			DGPyFE/SIC	
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:		Determinado por la Secretaría Administrativa		
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**	
 Karen Hernández Negrete			Determinado por la Secretaría Administrativa	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** Determinado por la Secretaría Administrativa	
Observaciones / anotaciones	Estas medidas las lleva a cabo la Secretaría Administrativa, quienes tienen toda la administración del sistema.			

Sistema Institucional de Compras			DGPyFE/SIC	
Formato:	**6**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 18. II. a) Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM**		
Aplicable en:		II. Sistemas operativos y servicios.		
Tiempo estimado:		Determinado por la Secretaría Administrativa		
Importancia de la acción:		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.		
Proceso recomendado:		**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. *Por ejemplo*, 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.		
Mejores prácticas, referencias:		**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.		
Conocimientos requeridos:		Administración de sistema operativo.		
Ejecución			**Fecha inicio**	
 Karen Hernández Negrete			Determinado por la Secretaría Administrativa	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** Determinado por la Secretaría Administrativa	
Observaciones / anotaciones	Estas medidas las lleva a cabo la Secretaría Administrativa, quienes tienen toda la administración del sistema.			

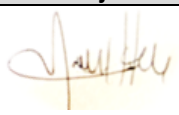
Sistema Institucional de Compras			DGPyFE/SIC	
Formato:	**7**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 18. II. b) Instalar y mantener actualizado el software antimalware.**		
Aplicable en:		II. Sistemas operativos y servicios.		
Tiempo estimado:		Determinado por la Secretaría Administrativa		
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**	
 Karen Hernández Negrete			Determinado por la Secretaría Administrativa	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** Determinado por la Secretaría Administrativa	
Observaciones / anotaciones	Estas medidas las lleva a cabo la Secretaría Administrativa, quienes tienen toda la administración del sistema.			

Sistema Institucional de Compras			DGPyFE/SIC	
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:		Determinado por la Secretaría Administrativa		
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**	
 Karen Hernández Negrete			Determinado por la Secretaría Administrativa	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** Determinado por la Secretaría Administrativa	
Observaciones / anotaciones	Estas medidas las lleva a cabo la Secretaría Administrativa, quienes tienen toda la administración del sistema.			

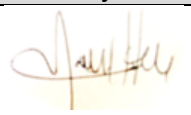
Sistema Institucional de Compras			DGPyFE/SIC	
Formato:	**9**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 19. I. a) Aplicar un mecanismo de autenticación para las personas autorizadas con base en el principio del menor privilegio.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Determinado por la Secretaría Administrativa		
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**	
 Karen Hernández Negrete			Determinado por la Secretaría Administrativa	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** Determinado por la Secretaría Administrativa	
Observaciones / anotaciones	Estas medidas las lleva a cabo la Secretaría Administrativa, quienes tienen toda la administración del sistema y de acuerdo a lo que solicite la DGPyFE.			

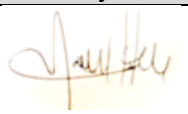
Sistema Institucional de Compras			DGPyFE/SIC	
Formato:	**10**	**Verificación anual**	**Acción concluida**	( )
Medida de seguridad técnica:		**Artículo 19. II. B) Evitar la instalación de cualquier elemento de software que implique algún riesgo para el tratamiento de datos personales.**		
Aplicable en:		II. Sistemas operativos.		
Tiempo estimado:		Determinado por la Secretaría Administrativa		
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**	
 Karen Hernández Negrete			Determinado por la Secretaría Administrativa	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** Determinado por la Secretaría Administrativa	
Observaciones / anotaciones	Estas medidas las lleva a cabo la Secretaría Administrativa, quienes tienen toda la administración del sistema.			

Sistema Institucional de Compras			DGPyFE/SIC	
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:		Determinado por la Secretaría Administrativa		
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**	
 Karen Hernández Negrete			Determinado por la Secretaría Administrativa	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** Determinado por la Secretaría Administrativa	
Observaciones / anotaciones	Estas medidas las lleva a cabo la Secretaría Administrativa, quienes tienen toda la administración del sistema.			

Sistema Institucional de Compras			DGPyFE/SIC	
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:		Determinado por la Secretaría Administrativa		
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**	
 Karen Hernández Negrete			Determinado por la Secretaría Administrativa	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** Determinado por la Secretaría Administrativa	
Observaciones / anotaciones	Estas medidas las lleva a cabo la Secretaría Administrativa, quienes tienen toda la administración del sistema.			

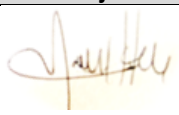
Sistema Institucional de Compras			DGPyFE/SIC	
Formato:	**13**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 19. IV. a) Realizar la transmisión de datos personales a través de un canal cifrado.**		
Aplicable en:		IV. Red de datos.		
Tiempo estimado:		Determinado por la Secretaría Administrativa		
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**	
 Karen Hernández Negrete			Determinado por la Secretaría Administrativa	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** Determinado por la Secretaría Administrativa	
Observaciones / anotaciones	Estas medidas las lleva a cabo la Secretaría Administrativa, quienes tienen toda la administración del sistema.			

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

Padrón de Proveedores y Contratistas			DGPyFE/PPC	
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:		Determinado por Patronato Universitario		
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**	
 Karen Hernández Negrete			Determinado por Patronato Universitario	
Nombre y firma Programador, desarrollador o diseñador del sistema de información			**Fecha término**	
			Determinado por Patronato Universitario	
Observaciones / anotaciones	Estas medidas las lleva a cabo la Dirección General de Control Presupuestal e Informática, por conducto de su Dirección de Organización y Sistemas, Patronato Universitario, quienes tienen toda la administración del sistema.			

Padrón de Proveedores y Contratistas			DGPyFE/PPC	
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:		Determinado por Patronato Universitario		
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**	
 Karen Hernández Negrete			Determinado por Patronato Universitario	
Nombre y firma Administrador del sistema de información			**Fecha término** Determinado por Patronato Universitario	
Observaciones / anotaciones		Estas medidas las lleva a cabo la Dirección General de Control Presupuestal e Informática, por conducto de su Dirección de Organización y Sistemas, Patronato Universitario, quienes tienen toda la administración del sistema y de acuerdo a lo que la DGPyFE, le solicite para cada usuario.		

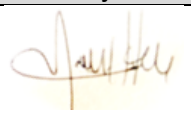
Padrón de Proveedores y Contratistas			DGPyFE/PPC	
Formato:	**3**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 18. I. g) Instalar y mantener vigentes certificados de comunicación segura SSL en el caso de servicios basados en Web.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Determinado por Patronato Universitario		
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**	
 Karen Hernández Negrete			Determinado por Patronato Universitario	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** Determinado por Patronato Universitario	
Observaciones / anotaciones	Estas medidas las lleva a cabo la Dirección General de Control Presupuestal e Informática, por conducto de su Dirección de Organización y Sistemas, Patronato Universitario, quienes tienen toda la administración del sistema.			

Padrón de Proveedores y Contratistas			DGPyFE/PPC	
Formato:	**4**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 18. I. h) Definir el plan de respaldos de la información, incluyendo periodicidad y alcance.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Determinado por Patronato Universitario		
Importancia de la acción:		En todo sistema de información es indispensable contar con un plan de respaldos periódicos, y especialmente en aquellos que contienen datos personales.		
Proceso recomendado:		**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.		
Mejores prácticas, referencias:		**1.-** Se deben tener al menos 3 respaldos del sistema y sus bases de datos en distintos medios.		
Conocimientos requeridos:		Administración de sistema operativo. Gestión y programación de respaldos.		
Ejecución			**Fecha inicio**	
 Karen Hernández Negrete			Determinado por Patronato Universitario	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** Determinado por Patronato Universitario	
Observaciones / anotaciones		Estas medidas las lleva a cabo la Dirección General de Control Presupuestal e Informática, por conducto de su Dirección de Organización y Sistemas, Patronato Universitario, quienes tienen toda la administración del sistema.		

Padrón de Proveedores y Contratistas			DGPyFE/PPC	
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:		Determinado por Patronato Universitario		
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**	
 Karen Hernández Negrete			Determinado por Patronato Universitario	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** Determinado por Patronato Universitario	
Observaciones / anotaciones	Estas medidas las lleva a cabo la Dirección General de Control Presupuestal e Informática, por conducto de su Dirección de Organización y Sistemas, Patronato Universitario, quienes tienen toda la administración del sistema.			

Padrón de Proveedores y Contratistas			DGPyFE/PPC	
Formato:	**6**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 18. II. a) Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM**		
Aplicable en:		II. Sistemas operativos y servicios.		
Tiempo estimado:		Determinado por Patronato Universitario		
Importancia de la acción:		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.		
Proceso recomendado:		**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. *Por ejemplo*, 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.		
Mejores prácticas, referencias:		**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.		
Conocimientos requeridos:		Administración de sistema operativo.		
Ejecución			**Fecha inicio**	
 Karen Hernández Negrete			Determinado por Patronato Universitario	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** Determinado por Patronato Universitario	
Observaciones / anotaciones		Estas medidas las lleva a cabo la Dirección General de Control Presupuestal e Informática, por conducto de su Dirección de Organización y Sistemas, Patronato Universitario, quienes tienen toda la administración del sistema.		

Padrón de Proveedores y Contratistas			DGPyFE/PPC	
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:		Determinado por Patronato Universitario		
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**	
 Karen Hernández Negrete			Determinado por Patronato Universitario	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** Determinado por Patronato Universitario	
Observaciones / anotaciones	Estas medidas las lleva a cabo la Dirección General de Control Presupuestal e Informática, por conducto de su Dirección de Organización y Sistemas, Patronato Universitario, quienes tienen toda la administración del sistema.			

Padrón de Proveedores y Contratistas			DGPyFE/PPC	
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:		Determinado por Patronato Universitario		
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**	
 Karen Hernández Negrete			Determinado por Patronato Universitario	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** Determinado por Patronato Universitario	
Observaciones / anotaciones	Estas medidas las lleva a cabo la Dirección General de Control Presupuestal e Informática, por conducto de su Dirección de Organización y Sistemas, Patronato Universitario, quienes tienen toda la administración del sistema.			

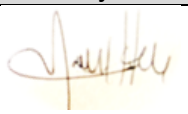
Padrón de Proveedores y Contratistas			DGPyFE/PPC	
Formato:	**9**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 19. I. a) Aplicar un mecanismo de autenticación para las personas autorizadas con base en el principio del menor privilegio.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Determinado por Patronato Universitario		
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**	
 Karen Hernández Negrete			Determinado por Patronato Universitario	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
			Determinado por Patronato Universitario	
Observaciones / anotaciones	Estas medidas las lleva a cabo la Dirección General de Control Presupuestal e Informática, por conducto de su Dirección de Organización y Sistemas, Patronato Universitario, quienes tienen toda la administración del sistema y de acuerdo a lo que solicite la DGPyFE.			

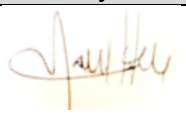
Padrón de Proveedores y Contratistas			DGPyFE/PPC	
Formato:	**10**	**Verificación anual**	**Acción concluida**	( )
Medida de seguridad técnica:		**Artículo 19. II. b) Evitar la instalación de cualquier elemento de software que implique algún riesgo para el tratamiento de datos personales.**		
Aplicable en:		II. Sistemas operativos.		
Tiempo estimado:		Determinado por Patronato Universitario		
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**	
 Karen Hernández Negrete			Determinado por Patronato Universitario	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** Determinado por Patronato Universitario	
Observaciones / anotaciones		Estas medidas las lleva a cabo la Dirección General de Control Presupuestal e Informática, por conducto de su Dirección de Organización y Sistemas, Patronato Universitario, quienes tienen toda la administración del sistema.		

Padrón de Proveedores y Contratistas			DGPyFE/PPC	
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:		Determinado por Patronato Universitario		
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**	
 Karen Hernández Negrete			Determinado por Patronato Universitario	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
			Determinado por Patronato Universitario	
Observaciones / anotaciones	Estas medidas las lleva a cabo la Dirección General de Control Presupuestal e Informática, por conducto de su Dirección de Organización y Sistemas, Patronato Universitario, quienes tienen toda la administración del sistema.			

Padrón de Proveedores y Contratistas			DGPyFE/PPC	
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:		Determinado por Patronato Universitario		
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**	
 Karen Hernández Negrete			Determinado por Patronato Universitario	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** Determinado por Patronato Universitario	
Observaciones / anotaciones	Estas medidas las lleva a cabo la Dirección General de Control Presupuestal e Informática, por conducto de su Dirección de Organización y Sistemas, Patronato Universitario, quienes tienen toda la administración del sistema.			

Padrón de Proveedores y Contratistas			DGPyFE/PPC	
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:		Determinado por Patronato Universitario		
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**	
 Karen Hernández Negrete			Determinado por Patronato Universitario	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** Determinado por Patronato Universitario	
Observaciones / anotaciones		Estas medidas las lleva a cabo la Dirección General de Control Presupuestal e Informática, por conducto de su Dirección de Organización y Sistemas, Patronato Universitario, quienes tienen toda la administración del sistema.		

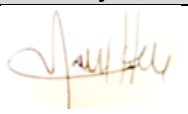
Padrón de Proveedores y Contratistas			DGPyFE/PPC	
Formato:	**14**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 20. Aplicar el procedimiento de borrado seguro que impida la recuperación en las bases de datos y todos sus respaldos.**		
Aplicable en:		Bases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

Sistema Integral de Administración Financiera			DGPyFE/SIAF	
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:		Determinado por el Instituto de Ingeniería		
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**	
 Karen Hernández Negrete			Determinado por el Instituto de Ingeniería	
Nombre y firma Programador, desarrollador o diseñador del sistema de información			**Fecha término**	
			Determinado por el Instituto de Ingeniería	
Observaciones / anotaciones	Estas medidas las lleva a cabo el Instituto de Ingeniería, quienes tienen toda la administración del sistema.			

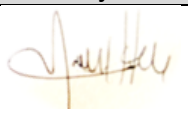
Sistema Integral de Administración Financiera			DGPyFE/SIAF	
Formato:	**2**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 18. I. e) Asignar o revocar los privilegios de acceso para los usuarios teniendo como base el principio del menor privilegio.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Determinado por el Instituto de Ingeniería		
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**	
 Karen Hernández Negrete			Determinado por el Instituto de Ingeniería	
Nombre y firma Administrador del sistema de información			**Fecha término** Determinado por el Instituto de Ingeniería	
Observaciones / anotaciones	Estas medidas las lleva a cabo el Instituto de Ingeniería, quienes tienen toda la administración del sistema y de acuerdo a lo que la DGPyFE, le solicite para cada usuario.			

Sistema Integral de Administración Financiera			DGPyFE/SIAF	
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:		Determinado por el Instituto de Ingeniería		
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**	
 Karen Hernández Negrete			Determinado por el Instituto de Ingeniería	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** Determinado por el Instituto de Ingeniería	
Observaciones / anotaciones	Estas medidas las lleva a cabo el Instituto de Ingeniería, quienes tienen toda la administración del sistema.			

Sistema Integral de Administración Financiera			DGPyFE/SIAF	
Formato:	**4**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 18. I. h) Definir el plan de respaldos de la información, incluyendo periodicidad y alcance.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Determinado por el Instituto de Ingeniería		
Importancia de la acción:		En todo sistema de información es indispensable contar con un plan de respaldos periódicos, y especialmente en aquellos que contienen datos personales.		
Proceso recomendado:		**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.		
Mejores prácticas, referencias:		**1.-** Se deben tener al menos 3 respaldos del sistema y sus bases de datos en distintos medios.		
Conocimientos requeridos:		Administración de sistema operativo. Gestión y programación de respaldos.		
Ejecución			**Fecha inicio**	
 Karen Hernández Negrete			Determinado por el Instituto de Ingeniería	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor			Determinado por el Instituto de Ingeniería	
Observaciones / anotaciones		Estas medidas las lleva a cabo el Instituto de Ingeniería, quienes tienen toda la administración del sistema.		

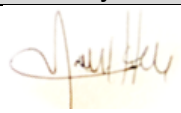
Sistema Integral de Administración Financiera			DGPyFE/SIAF	
Formato:	**5**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 18. I. i) Definir el procedimiento para el borrado seguro.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Determinado por el Instituto de Ingeniería		
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**	
 Karen Hernández Negrete			Determinado por el Instituto de Ingeniería	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** Determinado por el Instituto de Ingeniería	
Observaciones / anotaciones	Estas medidas las lleva a cabo el Instituto de Ingeniería, quienes tienen toda la administración del sistema.			

Sistema Integral de Administración Financiera			DGPyFE/SIAF	
Formato:	**6**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 18. II. a) Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM**		
Aplicable en:		II. Sistemas operativos y servicios.		
Tiempo estimado:		Determinado por el Instituto de Ingeniería		
Importancia de la acción:		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.		
Proceso recomendado:		**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. *Por ejemplo*, 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.		
Mejores prácticas, referencias:		**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.		
Conocimientos requeridos:		Administración de sistema operativo.		
Ejecución			**Fecha inicio**	
 Karen Hernández Negrete			Determinado por el Instituto de Ingeniería	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** Determinado por el Instituto de Ingeniería	
Observaciones / anotaciones	Estas medidas las lleva a cabo el Instituto de Ingeniería, quienes tienen toda la administración del sistema.			

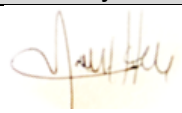
<table>
<tr><td colspan="3">Sistema Integral de Administración Financiera</td><td colspan="2">DGPyFE/SIAF</td></tr>
<tr><td>Formato:</td><td>7</td><td>Verificación anual</td><td>Acción concluida</td><td>( )</td></tr>
<tr><td colspan="2">Medidas de seguridad técnicas:</td><td colspan="3">Artículo 18. II. b) Instalar y mantener actualizado el software antimalware.</td></tr>
<tr><td colspan="2">Aplicable en:</td><td colspan="3">II. Sistemas operativos y servicios.</td></tr>
<tr><td colspan="2">Tiempo estimado:</td><td colspan="3">Determinado por el Instituto de Ingeniería</td></tr>
<tr><td colspan="2">Importancia de la acción:</td><td colspan="3">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.</td></tr>
<tr><td colspan="2">Proceso recomendado:</td><td colspan="3">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.</td></tr>
<tr><td colspan="2">Mejores prácticas, referencias:</td><td colspan="3">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.</td></tr>
<tr><td colspan="2">Conocimientos requeridos:</td><td colspan="3">Administración de sistema operativo. Instalación de aplicaciones.</td></tr>
<tr><td colspan="3">Ejecución</td><td colspan="2">Fecha inicio</td></tr>
<tr><td colspan="3"> 
Karen Hernández Negrete</td><td colspan="2">Determinado por el Instituto de Ingeniería</td></tr>
<tr><td colspan="3" rowspan="2">Nombre y firma
Administrador del sistema de información o servidor</td><td colspan="2">Fecha término</td></tr>
<tr><td colspan="2">Determinado por el Instituto de Ingeniería</td></tr>
<tr><td>Observaciones / anotaciones</td><td colspan="4">Estas medidas las lleva a cabo el Instituto de Ingeniería, quienes tienen toda la administración del sistema.</td></tr>
</table>

Sistema Integral de Administración Financiera			DGPyFE/SIAF	
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:		Determinado por el Instituto de Ingeniería		
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**	
 Karen Hernández Negrete			Determinado por el Instituto de Ingeniería	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** Determinado por el Instituto de Ingeniería	
Observaciones / anotaciones	Estas medidas las lleva a cabo el Instituto de Ingeniería, quienes tienen toda la administración del sistema.			

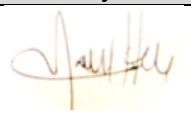
Sistema Integral de Administración Financiera			DGPyFE/SIAF	
Formato:	**9**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 19. I. a) Aplicar un mecanismo de autenticación para las personas autorizadas con base en el principio del menor privilegio.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Determinado por el Instituto de Ingeniería		
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**	
 Karen Hernández Negrete			Determinado por el Instituto de Ingeniería	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** Determinado por el Instituto de Ingeniería	
Observaciones / anotaciones	Estas medidas las lleva a cabo el Instituto de Ingeniería, quienes tienen toda la administración del sistema y de acuerdo a lo que solicite la DGPyFE.			

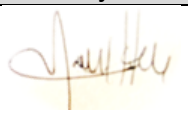
Sistema Integral de Administración Financiera			DGPyFE/SIAF	
Formato:	**10**	**Verificación anual**	**Acción concluida**	( )
Medida de seguridad técnica:		**Artículo 19. II. B) Evitar la instalación de cualquier elemento de software que implique algún riesgo para el tratamiento de datos personales.**		
Aplicable en:		II. Sistemas operativos.		
Tiempo estimado:		Determinado por el Instituto de Ingeniería		
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**	
 Karen Hernández Negrete			Determinado por el Instituto de Ingeniería	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** Determinado por el Instituto de Ingeniería	
Observaciones / anotaciones		Estas medidas las lleva a cabo la Secretaría Administrativa, quienes tienen toda la administración del sistema.		

Sistema Integral de Administración Financiera			DGPyFE/SIAF	
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:		Determinado por el Instituto de Ingeniería		
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**	
 Karen Hernández Negrete			Determinado por el Instituto de Ingeniería	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** Determinado por el Instituto de Ingeniería	
Observaciones / anotaciones	Estas medidas las lleva a cabo el Instituto de Ingeniería, quienes tienen toda la administración del sistema.			

Sistema Integral de Administración Financiera			DGPyFE/SIAF	
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:		Determinado por el Instituto de Ingeniería		
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**	
 Karen Hernández Negrete			Determinado por el Instituto de Ingeniería	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor			Determinado por el Instituto de Ingeniería	
Observaciones / anotaciones	Estas medidas las lleva a cabo el Instituto de Ingeniería, quienes tienen toda la administración del sistema.			

Sistema Integral de Administración Financiera			DGPyFE/SIAF	
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:		Determinado por el Instituto de Ingeniería		
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**	
 Karen Hernández Negrete			Determinado por el Instituto de Ingeniería	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** Determinado por el Instituto de Ingeniería	
Observaciones / anotaciones	Estas medidas las lleva a cabo el Instituto de Ingeniería, quienes tienen toda la administración del sistema.			

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

Intelisis - Papyrus			DGPyFE/SGA	
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**	
 Karen Hernández Negrete			08/08/2022	
Nombre y firma Programador, desarrollador o diseñador del sistema de información			**Fecha término**	
			08/08/2022	
Observaciones / anotaciones	En ningún caso se utilizan datos personales de ninguna entidad, todo el código fuente que se utiliza es propio de la aplicación.			

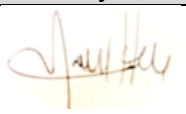
Intelisis - Papyrus			DGPyFE/SGA	
Formato:	**2**	**Verificación anual**	**Acción concluida**	**( )**
Medidas de seguridad técnicas:		**Artículo 18. I. e) Asignar o revocar los privilegios de acceso para los usuarios teniendo como base el principio del menor privilegio.**		
Aplicable en:		I. Bases de 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**	
 Karen Hernández Negrete			08/08/2022	
Nombre y firma Administrador del sistema de información			**Fecha término** 08/08/2022	
Observaciones / anotaciones	Los privilegios que se determinan para cada usuario dentro de la DGPyFE, son única y exclusivamente, los relacionados con sus funciones y actividades laborales.			

Intelisis - Papyrus			DGPyFE/SGA	
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:		Dos 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**	
 Karen Hernández Negrete			08/08/2022	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** 09/08/2022	
Observaciones / anotaciones	Se tiene la previsión de mantener en todo momento actualizado el certificado del SGA, de lo contrario estaría fuera de servicio.			

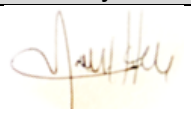
Intelisis - Papyrus			DGPyFE/SGA	
Formato:	**4**	**Verificación anual**	**Acción concluida**	**( )**
Medidas de seguridad técnicas:		**Artículo 18. I. h) Definir el plan de respaldos de la información, incluyendo periodicidad y alcance.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Dos días hábiles.		
Importancia de la acción:		En todo sistema de información es indispensable contar con un plan de respaldos periódicos, y especialmente en aquellos que contienen datos personales.		
Proceso recomendado:		**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.		
Mejores prácticas, referencias:		**1.-** Se deben tener al menos 3 respaldos del sistema y sus bases de datos en distintos medios.		
Conocimientos requeridos:		Administración de sistema operativo. Gestión y programación de respaldos.		

Ejecución	**Fecha inicio**
 Karen Hernández Negrete	09/08/2022
Nombre y firma	**Fecha término**
Administrador del sistema de información o servidor	10/08/2022

Observaciones / anotaciones	- *Veeam (Respaldos locales)* Tipo de respaldos: Incrementales a nivel de máquinas virtuales Almacenamiento: Estos respaldos se almacenan en un Storage IBM Storwize V3700, con energía y fibras de transmisión de datos de forma redundante. Ubicación: Centro de Datos de la dependencia de publicaciones digitales - *BaaS (Backus as a Service)* Tipo de respaldos: Respaldos mediante agente de Veeam a nivel de sistema operativo de cada servidor respaldado. Almacenamiento: Este almacenamiento es administrado directamente por DGTIC.

Intelisis - Papyrus			DGPyFE/SGA	
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:		Está en proceso de definición.		
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**	
 Karen Hernández Negrete				
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones	Está en proceso de definición.			

Intelisis - Papyrus			DGPyFE/SGA	
Formato:	**6**	**Verificación anual**	**Acción concluida**	**( )**
Medidas de seguridad técnicas:		**Artículo 18. II. a) Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM**		
Aplicable en:		II. Sistemas operativos y servicios.		
Tiempo estimado:		Un día hábil.		
Importancia de la acción:		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.		
Proceso recomendado:		**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. *Por ejemplo*, 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.		
Mejores prácticas, referencias:		**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.		
Conocimientos requeridos:		Administración de sistema operativo.		
Ejecución			**Fecha inicio**	
 Karen Hernández Negrete			NO APLICA	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** NO APLICA	
Observaciones / anotaciones	NO APLICA			

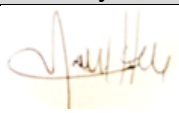
Intelisis - Papyrus			DGPyFE/SGA	
Formato:	**7**	**Verificación anual**	**Acción concluida**	**( )**
Medidas de seguridad técnicas:		**Artículo 18. II. b) Instalar y mantener actualizado el software antimalware.**		
Aplicable en:		II. Sistemas operativos y servicios.		
Tiempo estimado:		Dos días hábiles.		
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**	
 Karen Hernández Negrete			09/08/2022	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
			10/08/2022	
Observaciones / anotaciones		Se mantiene actualizado y controlado este procedimiento a través de Kaspersky Security Center 13.2: Servicio optimizado para garantizar el mejor rendimiento, funciona en segundo plano, protegiendo sin ralentizar las PC, frente a las amenazas más recientes.		

Intelisis - Papyrus			DGPyFE/SGA	
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:		Tres 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**	
 Karen Hernández Negrete			09/08/2022	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** 11/08/2022	
Observaciones / anotaciones	Se mantienen como proceso continuo, el actualizar las licencias de los sistemas que se encuentran operando en la DGPyFE.			

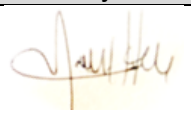
Intelisis - Papyrus			DGPyFE/SGA	
Formato:	**9**	**Verificación anual**	**Acción concluida**	**( )**
Medidas de seguridad técnicas:		**Artículo 19. I. a) Aplicar un mecanismo de autenticación para las personas autorizadas con base en el principio del menor privilegio.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Dos 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**	
 Karen Hernández Negrete			10/08/2022	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** 11/08/2022	
Observaciones / anotaciones	Todos y cada uno de los privilegios asignados a cada usuario, están determinados de acuerdo a las actividades que desempeña.			

Intelisis - Papyrus			DGPyFE/SGA	
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**	
Karen Hernández Negrete			10/08/2022	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** 11/08/2022	
Observaciones / anotaciones	Ningún usuario tiene los privilegios necesarios para instalar y desinstalar software.			

Intelisis - Papyrus			DGPyFE/SGA	
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**	
 Karen Hernández Negrete			11/08/2022	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** 12/08/2022	
Observaciones / anotaciones	Se cuenta con acceso controlado al personal que accede a la DGPyFE, así como, cámaras de seguridad.			

Intelisis - Papyrus			DGPyFE/SGA	
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**	
 Karen Hernández Negrete			11/08/2022	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** 11/08/2022	
Observaciones / anotaciones	Se cuenta con el formato estándar de control de entrada y salida de bienes, proporcionado por las áreas administrativas de las entidades, así como, una bitácora de registro de salida y entrada de los mismos.			

Intelisis - Papyrus			DGPyFE/SGA	
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. 09/08/2022		
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**	
 Karen Hernández Negrete			10/08/2022	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** 12/08/2022	
Observaciones / anotaciones	Las contraseñas se transmiten a través de la red interna de la dependencia de manera cifrada, por lo tanto, no hay salida al exterior.			

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

POLÍTICAS PARA LA PROTECCIÓN DE DATOS PERSONALES

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

[5] *Op. cit.*

MÉTODOS LÓGICOS DE BORRADO

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

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 DGPyFE.

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 DGPyFE 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 DGPyFE 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 DGPyFE 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.

[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

- 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.

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 DGPyFE 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 DGPyFE 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 DGPyFE 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 DGPyFE 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 DGPyFE 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 DGPyFE.

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

[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.

En términos de lo previsto en el artículo 60 de la Ley General, cuando el encargado incumpla las instrucciones de la DGPyFE 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.

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 DGPyFE 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 DGPyFE 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 DGPyFE 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 DGPyFE 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 DGPyFE 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 DGPyFE 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 DGPyFE.

[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.

En ningún caso, la DGPyFE 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 DGPyFE 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 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 DGPyFE 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 DGPyFE 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 DGPyFE 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 DGPyFE, 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 DGPyFE así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
- Permitir y colaborar con la DGPyFE 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 DGPyFE, 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 DGPyFE 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 DGPyFE. 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 DGPyFE 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 directa a la Coordinación de sistemas de la DGPyFE y no a través de terceros.

6. El director, subdirector, jefe de unidad administrativa de la DGPyFE, serán quienes podrán solicitar a la Coordinación de sistemas de la DGPyFE el alta de un usuario en el servicio de correo electrónico institucional.

7. El nombre de usuario es asignado por la Coordinación de sistemas de la DGPyFE, 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.

10. El cliente de correo electrónico institucional es @libros.unam.mx.

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 DGPyFE, a través de la coordinación de sistemas 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 coordinación de sistemas de la DGPyFE.

Se testan los anexos titulados “Análisis de Riesgos”, “Análisis de Brecha” y “Plan de Trabajo” por tratarse de información reservada, cuya divulgación obstruiría el deber de esta Universidad de establecer y mantener las medidas de seguridad técnica, administrativa y física de los datos personales, de conformidad con los artículos 106, fracción II y 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública, 98 fracción II, 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 Lineamientos Generales de Protección de Datos Personales para el Sector Público y las reglas generales de evaluación Décima Tercera y Décima Cuarta del apartado V. Reglas de Generales de Evaluación, del Documento Técnico de Evaluación y sus anexos de los Instrumentos Técnicos que refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en materia de Evaluación del Desempeño de los Sujetos Obligados del Sector Público Federal en el Cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.