

INTRODUCCIÓN

El presente *Documento de Seguridad* contiene las medidas de seguridad administrativa, física y técnica aplicables a los sistemas de tratamiento de datos personales de la Coordinación Universitaria para la Sustentabilidad (en adelante COUS) de la Universidad Nacional Autónoma de México, con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información personal que éstos contienen.

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

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

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

La COUS, con la finalidad de establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales y en cumplimiento a las disposiciones legales antes descritas, emite el presente *Documento de Seguridad*, en observancia de los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de los datos personales, con la intención de brindar homogeneidad en la organización y procesos para la protección de los datos personales de esta Coordinación.

El cimiento del presente *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 mismo considera el tamaño y estructura de la propia UNAM, objetivos, clasificación de la información, requerimientos de seguridad y procesos que se precisan en razón de los activos que posee esta Casa de Estudios, lo cual se encuentran contemplado en el estándar internacional en materia de seguridad de la información ISO/IEC 27002:2013 “Tecnología de la información - Técnicas de seguridad - Código de práctica para los controles de seguridad de la información”.

SUBDIRECCIÓN DE EDUCACIÓN Y VINCULACIÓN PARA LA SUSTENTABILIDAD

(1)

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Subdirección de Educación y Vinculación para la Sustentabilidad	
Identificador único*	COUS 1
(Nombre del sistema A1) *	Seminario Tópicos de Frontera en Sustentabilidad
Datos personales (sensibles o no) contenidos en el sistema*	1. Datos personales en general: a) Datos de identificación: Nombre completo, correo electrónico, CURP, fecha de nacimiento, nacionalidad. c) Datos académicos: Trayectoria educativa. 2. Datos personales sensibles: No se solicitan.
Responsable*:	
Nombre*	Alexandra Bárzana Sánchez Mejorada
Cargo*	
Funciones*	Recabar la información de los participantes en las sesiones del seminario Tópicos de Frontera en Sustentabilidad.
Obligaciones*	- Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. - Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados.
	Encargados:
(Nombre del Encargado 1*)	Raquel Radahy Rodríguez Granados
Cargo*:	Asistente administrativa
Funciones*:	Integrar la información de los participantes en las sesiones del seminario Tópicos de Frontera en Sustentabilidad.

	• Elaborar las constancias de los participantes en las sesiones del seminario Tópicos de Frontera en Sustentabilidad. • Enviar las constancias a los participantes en las sesiones del seminario Tópicos de Frontera en Sustentabilidad.
Obligaciones*:	• Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. • Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados.

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

Subdirección de Educación y Vinculación para la Sustentabilidad	
Identificador único**	COUS 1
(Nombre del sistema A1*)	Seminario Tópicos de Frontera en Sustentabilidad
Tipo de soporte: *	Soporte electrónico: Base de datos digital Google Drive y hojas de cálculo Excel.
Descripción: *	Hoja de cálculo Excel en Google Drive nombrada "Formato_sigeco_TFS" y en carpeta UNAM2S.3-5267-02021-1 en computadora UNAM 02403934.
Características del lugar donde se resguardan los soportes: *	Alojamiento en la nube de Google Drive y en computadora de escritorio.

3. ANÁLISIS DE RIESGOS

Eliminado: Cinco renglones en los que se especifican los riesgos, diez con el impacto y veinticuatro con la mitigación, correspondientes al análisis de riesgos. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Subdirección de Educación y Vinculación para la Sustentabilidad		
Identificador único**	COUS 1	
(Nombre del sistema A1*)	Seminario Tópicos de Frontera en Sustentabilidad	
Riesgo*	Impacto*	Mitigación*
Comentario	Comentario	Comentario
		Comentario
		Comentario
		Comentario
Comentario	Comentario	Comentario
Comentario	Comentario	Comentario

Eliminado: Tres renglones en los que se especifican los riesgos, dieciséis con el impacto y treinta y dos con la mitigación, correspondientes al análisis de riesgos.
Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

		Comentario
		Comentario
		Comentario
		Comentario
Comentario	Comentario	Comentario
Comentario	Comentario	Comentario Comentario
Comentario	Comentario	Comentario

4. ANÁLISIS DE BRECHA

Subdirección de Educación y Vinculación para la Sustentabilidad		
Identificador único**	COUS 1	
(Nombre del sistema A1*)	Seminario Tópicos de Frontera en Sustentabilidad	
Medida de seguridad actual*	Medida de seguridad necesaria*	Acciones para remediación*
Comentario	Comentario	Comentario
Comentario		
Comentario		Comentario

Eliminado: Diez renglones en los que se especifican las medidas de seguridad actuales, cinco con las medidas de seguridad necesarias y nueve con las acciones para remediación, correspondientes al análisis de brecha.
Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

5. PLAN DE TRABAJO

Eliminado: Doce renglones en los que se especifican las actividades, veintiuno con la descripción, cuatro con la duración y veintidós con la cobertura, correspondientes al plan de trabajo.
Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Subdirección de Educación y Vinculación para la Sustentabilidad			
Identificador único**	COUS 1		
(Nombre del sistema A1*)	Seminario Tópicos de Frontera en Sustentabilidad		
Actividad*	Descripción*	Duración*	Cobertura*
Comentario	Comentario	Comentario	Comentario
Comentario	Comentario	Comentario	Comentario
Comentario	Comentario	Comentario	Comentario
Comentario	Comentario	Comentario	Comentario

Eliminado: Dos renglones en los que se especifican las actividades, dos con la descripción, uno con la duración y cinco con la cobertura, correspondientes al plan de trabajo. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Comentario	Comentario	Comentario	Comentario

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Subdirección de Educación y Vinculación para la Sustentabilidad	
Identificador único**	COUS 1
(Nombre del sistema A1*)	Seminario Tópicos de Frontera en Sustentabilidad
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realiza traslado en soporte físico.
Transferencias mediante el traslado de soportes electrónicos:	No se realiza traslado en soporte electrónico.
Transferencias mediante el traslado sobre redes electrónicas:	El formulario se almacena en la nube privada de Google Drive y en correo electrónico institucional administrado por el Centro de Datos de la UNAM. En algunos casos, la información se envía cifrada mediante protocolos SSL/TLS al Sistema de Gestión de Constancias (SIGECO) administrado por la CUAIEED.

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

El Sistema de Gestión de Constancias (SIGECO), no realiza tratamiento de datos personales con soportes físicos, ya que se encuentra a través de soporte electrónico a través del mismo sistema, el cual esta albergado en los servidores de la CUAIEED.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

El Sistema de Gestión de Constancias (SIGECO) cuenta con una opción de Consulta, la cual permite visualizar los datos que se ingresaron para la emisión de las constancias; así como la fecha y hora en que se emitieron.

IV. REGISTRO DE INCIDENTES:

Se desconoce si se cuenta con este registro, debido a que el sistema es administrado por la CUAIEED.

V. ACCESO A LAS INSTALACIONES

Los accesos al Antiguo edificio de posgrado están asegurados por un sistema de identificación biométrica en el acceso al edificio y en el acceso al ala donde se encuentra la COUS. Adicionalmente el acceso a las oficinas de la COUS está asegurado por una puerta con dos llaves. El edificio cuenta con sistema de Circuito cerrado las 24 horas.

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

La Coordinación de Universidad Abierta, Innovación Educativa y Educación a Distancia (CUAIEED), es la encargada de realizar las actualizaciones y/o notificaciones de los posibles cambios realizados al sistema.

VII. PERFILES DE USUARIO Y CONTRASEÑAS

El Sistema de Gestión de Constancias (SIGECO) fue diseñado para que cada persona responsable tenga un usuario y contraseña y pueda tener acceso al sistema para cargar la información confidencial y pueda realizar la emisión de constancias correspondientes. Los usuarios y contraseñas son autorizados por el administrador del SIGECO, adscrito a la CUAIEED.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

El respaldo de la información recopilada por la Subdirección de Educación y Vinculación para la Sustentabilidad, se realiza mediante hojas de cálculo almacenadas en la nube institucional anclada al correo sustentabilidadunam@gmail.com.

En cuanto al proceso de recuperación de datos, es responsabilidad del administrador del SIGECO y se desconoce el procedimiento.

IX. PLAN DE CONTINGENCIA

Se desconoce el procedimiento ya que es responsabilidad de la CUIAEED.

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

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

Subdirección de Educación y Vinculación para la Sustentabilidad		
Identificador único	COUS 1	
Nombre del sistema	Seminario Tópicos de Frontera en Sustentabilidad	
Recurso*	Descripción*	Control*
N/A	N/A	N/A

7.2 Procedimiento para la revisión de las medidas de seguridad

Subdirección de Educación y Vinculación para la Sustentabilidad		
Identificador único	COUS 1	
Nombre del sistema	Seminario Tópicos de Frontera en Sustentabilidad	
Medida de seguridad*	Procedimiento*	Responsable*
N/A	N/A	N/A

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

Subdirección de Educación y Vinculación para la Sustentabilidad		
---	--	--

Identificador único	COUS 1	
Nombre del sistema	Seminario Tópicos de Frontera en Sustentabilidad	
Medida de seguridad*	Resultado de evaluación*	Responsable*
N/A	N/A	N/A

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

Subdirección de Educación y Vinculación para la Sustentabilidad		
Identificador único	COUS 1	
Nombre del sistema	Seminario Tópicos de Frontera en Sustentabilidad	
Medida de seguridad*	Acciones*	Responsable*
N/A	N/A	a) N/A

8 PROGRAMA ESPECÍFICO DE CAPACITACIÓN

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

Subdirección de Educación y Vinculación para la Sustentabilidad			
Identificador único	COUS 1		
Nombre del sistema	Seminario Tópicos de Frontera en Sustentabilidad		
Actividad*	Descripción*	Duración*	Cobertura*
La COUS solicitará a la Unidad de Transparencia de la UNAM programar un curso enfocado a la capacitación del personal involucrado en la captación,	Cursos relacionados con la protección y seguridad de datos personales	Capacitación por lo menos una vez al año.	Deberán asistir por lo menos dos personas de cada área que maneje datos personales en la COUS.

manejo, resguardo y seguridad de datos personales. De igual forma, se buscarán cursos relacionados que impartan otras instancias como el INAI.			
--	--	--	--

8.2 Programa de difusión de la protección a los datos personales

Subdirección de Educación y Vinculación para la Sustentabilidad			
Identificador único	COUS 1		
Nombre del sistema	Seminario Tópicos de Frontera en Sustentabilidad		
Actividad*	Descripción*	Duración*	Cobertura*
Difusión de protección de datos personales	El 25 de febrero de 2019, la UNAM difundió en la Gaceta UNAM los Lineamientos para la protección de datos personal en posesión de la UNAM	Permanente	Institucional

9 MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

Subdirección de Educación y Vinculación para la Sustentabilidad	
Identificador único*	COUS 1
Nombre del sistema	Seminario Tópicos de Frontera en Sustentabilidad

Actividad*	Descripción*	Duración*	Cobertura*
N/A	N/A	N/A	N/A

9.2 Actualización y mantenimiento de equipo de cómputo

Subdirección de Educación y Vinculación para la Sustentabilidad			
Identificador único	COUS 1		
Nombre del sistema	Seminario Tópicos de Frontera en Sustentabilidad		
Actividad*	Descripción*	Duración*	Cobertura*
Mantenimiento preventivo	Realizar el mantenimiento preventivo del equipo de cómputo tanto a nivel hardware como software para su funcionamiento óptimo.	2 veces por año	Equipos asignados a la Coordinación Universitaria para la Sustentabilidad (COUS).

9.3 Procesos para la conservación, preservación y respaldos de información

Subdirección de Educación y Vinculación para la Sustentabilidad		
Identificador único	COUS 1	
Nombre del sistema	Seminario Tópicos de Frontera en Sustentabilidad	
Proceso*	Descripción*	Responsable*
N/A	N/A	Esta actividad la realiza la Coordinación de Universidad Abierta, Innovación Educativa y

		Educación a Distancia (CUAIEED)
--	--	------------------------------------

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

Subdirección de Educación y Vinculación para la Sustentabilidad		
Identificador único	COUS 1	
Nombre del sistema	Seminario Tópicos de Frontera en Sustentabilidad	
Proceso	Descripción*	Responsable*
Procesos de borrado seguro y disposición final de equipos y componentes informáticos.	Procesos de borrado seguro y disposición final de equipos y componentes informáticos.	Jefa de Departamento de TIC de la SDI

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

Las personas que cuenten con usuario y contraseña al Sistema de Gestión de Constancias (SIGECO), no tiene injerencia en la cancelación de tratamiento de datos personales o del sistema, debido a que esta actividad depende de la Coordinación de Universidad Abierta, Innovación Educativa y Educación a Distancia (CUAIEED)

SUBDIRECCIÓN DE CAMPUS SUSTENTABLES

(2)

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Subdirección de Campus Sustentables	
Identificador único*	COUS 2
(Nombre del sistema A1) *	Consumo Sustentable
Datos personales (sensibles o no) contenidos en el sistema*	1. Datos personales en general: a) Datos de identificación: Nombre completo, correo electrónico, CURP, fecha de nacimiento, nacionalidad. b) Datos académicos: Trayectoria educativa. 2. Datos personales sensibles: No se solicitan.
Responsable*:	
Nombre*	David Sébastien Monachon
Cargo*	<u>Líder de proyecto</u>
Funciones*	Recabar la información de los participantes en las actividades relacionadas con el área de Consumo Sustentable.
Obligaciones*	- Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. - Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados.
	Encargados:
(Nombre del Encargado 1*)	Raquel Radahy Rodríguez Granados
Cargo*:	Asistente administrativa
Funciones*:	- Integrar la información de los participantes en las actividades de Consumo Sustentable. - Elaborar constancias de participantes en los cursos, diplomados y reuniones del programa de Consumo Sustentable.

	• Enviar las constancias de participantes en los cursos, diplomados y reuniones del programa de Consumo Sustentable.
Obligaciones*:	• Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. • Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados.

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

Subdirección de Campus Sustentables	
Identificador único**	COUS 2
(Nombre del sistema A1*)	Consumo Sustentable
Tipo de soporte: *	Soporte electrónico: Base de datos digital Google Forms y hojas de cálculo Excel.
Descripción: *	Nube UNAM One Drive Microsoft 360
Características del lugar donde se resguardan los soportes: *	Alojamiento en la nube institucional (cuenta de la UNAM) One Drive Microsoft 360.

3. ANÁLISIS DE RIESGOS

Subdirección de Campus Sustentables		
Identificador único**	COUS 2	
(Nombre del sistema A1*)	Consumo Sustentable	
Riesgo*	Impacto*	Mitigación*
Comentario	Comentario	Comentario
		Comentario
		Comentario
		Comentario
Comentario	Comentario	Comentario
		Comentario

Eliminado: Cinco renglones en los que se especifican los riesgos, diez con el impacto y veintiséis con la mitigación, correspondientes al análisis de riesgos.
Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Eliminado: Tres renglones en los que se especifican los riesgos, dieciséis con el impacto y treinta con la mitigación, correspondientes al análisis de riesgos. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

		Comentario
		Comentario
		Comentario
Comentario	Comentario	Comentario
Comentario	Comentario	Comentario Comentario
Comentario	Comentario	Comentario

4. ANÁLISIS DE BRECHA

Subdirección de Campus Sustentables		
Identificador único**	COUS 2	
(Nombre del sistema A1*)	Consumo Sustentable	
Medida de seguridad actual*	Medida de seguridad necesaria*	Acciones para remediación*
Comentario	Comentario	Comentario
Comentario		
Comentario		Comentario

Eliminado: Diez renglones en los que se especifican las medidas de seguridad actuales, cinco con las medidas de seguridad necesarias y diez con las acciones para remediación, correspondientes al análisis de brecha.
Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

5. PLAN DE TRABAJO

Eliminado: Diez renglones en los que se especifican las actividades, veintitrés con la descripción, cuatro con la duración y quince con la cobertura, correspondientes al plan de trabajo.
Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Subdirección de Campus Sustentables			
Identificador único**	COUS 2		
(Nombre del sistema A1*)	Consumo Sustentable		
Actividad*	Descripción*	Duración*	Cobertura*
Comentario	Comentario	Comentario	Comentario
Comentario	Comentario	Comentario	Comentario
Comentario	Comentario	Comentario	Comentario
Comentario	Comentario	Comentario	Comentario

Eliminado: Un renglón en el que se especifican las actividades, tres con la descripción, uno con la duración y tres con la cobertura, correspondientes al plan de trabajo.

Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Comentario	Comentario	Comentario	Comentario

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

II. TRANSFERENCIAS DE DATOS PERSONALES

Subdirección de Campus Sustentables	
Identificador único**	COUS 2
(Nombre del sistema A1*)	Consumo Sustentable
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realiza traslado en soporte físico.
Transferencias mediante el traslado de soportes electrónicos:	No se realiza traslado en soporte electrónico.
Transferencias mediante el traslado sobre redes electrónicas:	El formulario se almacena en la nube privada de Microsoft y en correo electrónico institucional administrado por el Centro de Datos de la UNAM. En algunos casos, la información se envía cifrada mediante protocolos SSL/TLS al Sistema de Gestión de Constancias (SIGECO) administrado por la CUAIEED.

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

El Sistema de Gestión de Constancias (SIGECO), no realiza tratamiento de datos personales con soportes físicos, ya que se encuentra a través de soporte electrónico a través del mismo sistema, el cual esta albergado en los servidores de la CUAIEED.

VIII. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

El Sistema de Gestión de Constancias (SIGECO) cuenta con una opción de Consulta, la cual permite visualizar los datos que se ingresaron para la emisión de las constancias; así como la fecha y hora en que se emitieron.

IX. REGISTRO DE INCIDENTES:

Se desconoce si se cuenta con este registro, debido a que el sistema es administrado por la CUAIEED.

X. ACCESO A LAS INSTALACIONES

Los accesos al Antiguo edificio de posgrado están asegurados por un sistema de identificación biométrica en el acceso al edificio y en el acceso al ala donde se encuentra la COUS. Adicionalmente el acceso a las oficinas de la COUS está asegurado por una puerta con dos llaves. El edificio cuenta con sistema de Circuito cerrado las 24 horas.

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

La Coordinación de Universidad Abierta, Innovación Educativa y Educación a Distancia (CUAIEED), es la encargada de realizar las actualizaciones y/o notificaciones de los posibles cambios realizados al sistema.

VII. PERFILES DE USUARIO Y CONTRASEÑAS

El Sistema de Gestión de Constancias (SIGECO) fue diseñado para que cada persona responsable tenga un usuario y contraseña y pueda tener acceso al sistema para cargar la información confidencial y pueda realizar la emisión de constancias correspondientes. Los usuarios y contraseñas son autorizados por el administrador del SIGECO, adscrito a la CUAIEED.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

El respaldo de la información recopilada por la Subdirección de Campus Sustentables, se realiza mediante hojas de cálculo almacenadas en la nube institucional.

En cuanto al proceso de recuperación de datos, es responsabilidad del administrador del SIGECO y se desconoce el procedimiento.

IX. PLAN DE CONTINGENCIA

Se desconoce el procedimiento ya que es responsabilidad de la CUAIEED.

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

10.1 Herramientas y recursos para monitoreo de la protección de datos personales

Subdirección de Campus Sustentables		
Identificador único	COUS 2	
Nombre del sistema	Consumo Sustentable	
Recurso*	Descripción*	Control*
N/A	N/A	N/A

10.2 Procedimiento para la revisión de las medidas de seguridad

Subdirección de Campus Sustentables		
Identificador único	COUS 2	
Nombre del sistema	Consumo Sustentable	
Medida de seguridad*	Procedimiento*	Responsable*
N/A	N/A	N/A

10.3 Resultados de la evaluación y pruebas a las medidas de seguridad

Subdirección de Campus Sustentables		
Identificador único	COUS 2	
Nombre del sistema	Consumo Sustentable	
Medida de seguridad*	Resultado de evaluación*	Responsable*

N/A	N/A	N/A
-----	-----	-----

10.4 Acciones para la corrección y actualización de las medidas de seguridad

Subdirección de Campus Sustentables		
Identificador único	COUS 2	
Nombre del sistema	Consumo Sustentable	
Medida de seguridad*	Acciones*	Responsable*
N/A	N/A	b) N/A

11 PROGRAMA ESPECÍFICO DE CAPACITACIÓN

11.1 Programa de capacitación a los responsables de seguridad de datos personales

Subdirección de Campus Sustentables			
Identificador único	COUS 2		
Nombre del sistema	Consumo Sustentable		
Actividad*	Descripción*	Duración*	Cobertura*
La COUS solicitará a la Unidad de Transparencia de la UNAM programar un curso enfocado a la capacitación del personal involucrado en la captación, manejo, resguardo y seguridad de datos personales. De igual forma, se buscarán cursos relacionados que impartan otras	Cursos relacionados con la protección y seguridad de datos personales	Capacitación por lo menos una vez al año.	Deberán asistir por lo menos dos personas de cada área que maneje datos personales en la COUS.

instancias como el INAI.			
--------------------------	--	--	--

11.2 Programa de difusión de la protección a los datos personales

Subdirección de Campus Sustentables			
Identificador único		COUS 2	
Nombre del sistema		Consumo Sustentable	
Actividad*	Descripción*	Duración*	Cobertura*
Difusión de protección de datos personales	El 25 de febrero de 2019, la UNAM difundió en la Gaceta UNAM los Lineamientos para la protección de datos personal en posesión de la UNAM	Permanente	Institucional

12 MEJORA CONTINUA

12.1 Actualización y mantenimiento de sistemas de información

Subdirección de Campus Sustentables			
Identificador único*		COUS 2	
Nombre del sistema		Consumo Sustentable	
Actividad*	Descripción*	Duración*	Cobertura*
N/A	N/A	N/A	N/A

12.2 Actualización y mantenimiento de equipo de cómputo

Subdirección de Campus Sustentables			
Identificador único	COUS 2		
Nombre del sistema	Consumo Sustentable		
Actividad*	Descripción*	Duración*	Cobertura*
Mantenimiento preventivo	Realizar el mantenimiento preventivo del equipo de cómputo tanto a nivel hardware como software para su funcionamiento óptimo.	2 veces por año	Equipos asignados a la Coordinación Universitaria para la Sustentabilidad (COUS).

12.3 Procesos para la conservación, preservación y respaldos de información

Subdirección de Campus Sustentables		
Identificador único	COUS 2	
Nombre del sistema	Consumo Sustentable	
Proceso*	Descripción*	Responsable*
N/A	N/A	Esta actividad la realiza la Coordinación de Universidad Abierta, Innovación Educativa y Educación a Distancia (CUAIEED)

12.4 Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Subdirección de Campus Sustentables		
Identificador único	COUS 2	
Nombre del sistema	Consumo Sustentable	
Proceso	Descripción*	Responsable*
Procesos de borrado seguro y disposición final de equipos y componentes informáticos.	Procesos de borrado seguro y disposición final de equipos y componentes informáticos.	Jefa de Departamento de TIC de la SDI

13 PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Las personas que cuenten con usuario y contraseña al Sistema de Gestión de Constancias (SIGECO), no tiene injerencia en la cancelación de tratamiento de datos personales o del sistema, debido a que esta actividad depende de la Coordinación de Universidad Abierta, Innovación Educativa y Educación a Distancia (CUAIEED)

SUBDIRECCIÓN DE CAMPUS SUSTENTABLES

(3)

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Subdirección de campus sustentables	
Identificador único*	COUS 7
(Nombre del sistema A1) *	Formularios página web
Datos personales (sensibles o no) contenidos en el sistema*	1. Datos personales en general: a) Datos de identificación: Nombre completo, correo electrónico, teléfono (opcional). 2. Datos personales sensibles: No se solicitan.
Responsable*:	
Nombre*	Alfonso de la Vega Rivera
Cargo*	Subdirector de Campus Sustentables
Funciones*	- Recibir al correo difusion.cous@unam.mx los registros recibidos del formulario de registro de la página web de la COUS. - Recibir al correo difusion.cous@unam.mx los registros recibidos del formulario de registro de iniciativas de sustentabilidad en la página web de la COUS.
Obligaciones*	- Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. - Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados.
Encargados:	
(Nombre del Encargado 1*)	Raquel Radahy Rodríguez Granados
Cargo*:	Asistente Administrativa
Funciones*:	Recibir al correo difusion.cous@unam.mx los registros recibidos del formulario de registro de la página web de la COUS.

	• Recibir al correo difusion.cous@unam.mx los registros recibidos del formulario de registro de iniciativas de sustentabilidad en la página web de la COUS.
Obligaciones*:	• Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. • Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados.

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

Comunicación e imagen	
Identificador único**	COUS 7
(Nombre del sistema A1*)	Formularios página web
Tipo de soporte: *	Soporte electrónico: Correo electrónico difusion.cous@unam.mx y base de datos digital en hojas de cálculo Excel.
Descripción: *	La base de datos se concentra en una hoja de Excel en la computadora institucional del responsable del sistema de Formularios página web.
Características del lugar donde se resguardan los soportes: *	Alojamiento en el disco duro de la computadora institucional del responsable del sistema de Formularios página web.

3. ANÁLISIS DE RIESGOS

Eliminado: Cinco renglones en los que se especifican los riesgos, diez con el impacto y veintiséis con la mitigación, correspondientes al análisis de riesgos.
Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Comunicación e imagen		
Identificador único**	COUS 7	
(Nombre del sistema A1*)	Formularios página web	
Riesgo*	Impacto*	Mitigación*
Comentario	Comentario	Comentario
		Comentario
		Comentario
		Comentario
Comentario	Comentario	Comentario
		Comentario

Eliminado: Tres renglones en los que se especifican los riesgos, diecisiete con el impacto y treinta con la mitigación, correspondientes al análisis de riesgos. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

		Comentario
		Comentario
		Comentario
Comentario	Comentario	Comentario
Comentario	Comentario	Comentario Comentario
Comentario	Comentario	Comentario

4. ANÁLISIS DE BRECHA

Eliminado: Diez renglones en los que se especifican las medidas de seguridad actuales, cinco con las medidas de seguridad necesarias y once con las acciones para remediación, correspondientes al análisis de brecha. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Comunicación e imagen		
Identificador único**	COUS 7	
(Nombre del sistema A1*)	Formularios página web	
Medida de seguridad actual*	Medida de seguridad necesaria*	Acciones para remediación*
Comentario	Comentario	Comentario
Comentario		
Comentario		Comentario

5. PLAN DE TRABAJO

Eliminado: Diez renglones en los que se especifican las actividades, veintiocho con la descripción, cuatro con la duración y dieciséis con la cobertura, correspondientes al plan de trabajo. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Comunicación e imagen			
Identificador único**	COUS 7		
(Nombre del sistema A1*)	Formularios página web		
Actividad*	Descripción*	Duración*	Cobertura*
Comentario	Comentario	Comentario	Comentario
Comentario	Comentario	Comentario	Comentario
Comentario	Comentario	Comentario	Comentario
Comentario	Comentario	Comentario	Comentario

Eliminado: Un renglón en el que se especifican las actividades, cinco con la descripción, uno con la duración y siete con la cobertura, correspondientes al plan de trabajo.
Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

	Comentario		Comentario
Comentario	Comentario	Comentario	Comentario

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Comunicación e imagen	
Identificador único**	COUS 7
(Nombre del sistema A1*)	Formularios página web
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realiza traslado en soporte físico.
Transferencias mediante el traslado de soportes electrónicos:	No se realiza traslado en soporte electrónico.
Transferencias mediante el traslado sobre redes electrónicas:	El formulario se almacena en el correo electrónico institucional administrado por el Centro de Datos de la UNAM.

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

N/A

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

N/A

IV. REGISTRO DE INCIDENTES:

N/A

V. ACCESO A LAS INSTALACIONES

Los accesos al Antiguo edificio de posgrado están asegurados por un sistema de identificación biométrica en el acceso al edificio y en el acceso al ala donde se encuentra la COUS. Adicionalmente el acceso a las oficinas de la COUS está asegurado por una puerta con dos llaves. El edificio cuenta con sistema de Circuito cerrado las 24 horas.

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

La COUS con el apoyo de la Jefatura de TIC's de la SDI realiza las actualizaciones de software y hardware en los equipos en los que se encuentra contenido el sistema de tratamiento de datos personales.

VII. PERFILES DE USUARIO Y CONTRASEÑAS

El responsable del programa de Formularios página web es el administrador único de las contraseñas y de la información relacionada con datos personales.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

El respaldo de la información recopilada se realiza por el responsable de los formularios de la página web y se almacena en el correo difusión.cous@unam.mx

La cuenta de correo electrónico es administrado por la Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC) de la UNAM.

IX. PLAN DE CONTINGENCIA

Se desconoce el procedimiento ya que es responsabilidad de la DGTIC.

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

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

Comunicación e imagen

Identificador único	COUS 7	
Nombre del sistema	Formularios página web	
Recurso*	Descripción*	Control*
N/A	N/A	N/A

7.2 Procedimiento para la revisión de las medidas de seguridad

Comunicación e imagen		
Identificador único	COUS 7	
Nombre del sistema	Formularios página web	
Medida de seguridad*	Procedimiento*	Responsable*
N/A	N/A	N/A

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

Comunicación e imagen		
Identificador único	COUS 7	
Nombre del sistema	Formularios página web	
Medida de seguridad*	Resultado de evaluación*	Responsable*
N/A	N/A	N/A

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

Comunicación e imagen		
------------------------------	--	--

Identificador único	COUS 7	
Nombre del sistema	Formularios página web	
Medida de seguridad*	Acciones*	Responsable*
N/A	N/A	c) N/A

8 PROGRAMA ESPECÍFICO DE CAPACITACIÓN

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

Comunicación e imagen			
Identificador único	COUS 7		
Nombre del sistema	Formularios página web		
Actividad*	Descripción*	Duración*	Cobertura*
La COUS solicitará a la Unidad de Transparencia de la UNAM programar un curso enfocado a la capacitación del personal involucrado en la captación, manejo, resguardo y seguridad de datos personales. De igual forma, se buscarán cursos relacionados que impartan otras instancias como el INAI.	Cursos relacionados con la protección y seguridad de datos personales	Capacitación por lo menos una vez al año.	Deberán asistir por lo menos dos personas de cada área que maneje datos personales en la COUS.

8.2 Programa de difusión de la protección a los datos personales

Comunicación e imagen			
Identificador único	COUS 7		
Nombre del sistema	Formularios página web		
Actividad*	Descripción*	Duración*	Cobertura*
Difusión de protección de datos personales	El 25 de febrero de 2019, la UNAM difundió en la Gaceta UNAM los Lineamientos para la protección de datos personal en posesión de la UNAM	Permanente	Institucional

9 MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

Comunicación e imagen			
Identificador único*	COUS 7		
Nombre del sistema	Formularios página web		
Actividad*	Descripción*	Duración*	Cobertura*
N/A	N/A	N/A	N/A

9.2 Actualización y mantenimiento de equipo de cómputo

Comunicación e imagen	
Identificador único	COUS 7

Nombre del sistema		Formularios página web	
Actividad*	Descripción*	Duración*	Cobertura*
Mantenimiento preventivo	Realizar el mantenimiento preventivo del equipo de cómputo tanto a nivel hardware como software para su funcionamiento óptimo.	2 veces por año	Equipos asignados a la Coordinación Universitaria para la Sustentabilidad (COUS).

9.3 Procesos para la conservación, preservación y respaldos de información

Comunicación e imagen		
Identificador único	COUS 7	
Nombre del sistema	Formularios página web	
Proceso*	Descripción*	Responsable*
N/A	N/A	N/A

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

Comunicación e imagen		
Identificador único	COUS 7	
Nombre del sistema	Formularios página web	
Proceso	Descripción*	Responsable*

Procesos de borrado seguro y disposición final de equipos y componentes informáticos.	Procesos de borrado seguro y disposición final de equipos y componentes informáticos.	Jefa de Departamento de TIC de la SDI
---	---	---------------------------------------

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

N/A

SUBDIRECCIÓN DE CAMPUS SUSTENTABLES

(4)

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Subdirección de Campus Sustentables	
Identificador único*	COUS 4
(Nombre del sistema A1) *	Red Universitaria para la Sustentabilidad
Datos personales (sensibles o no) contenidos en el sistema*	1. Datos personales en general: a) Datos de identificación: Nombre completo, correo electrónico. b) Datos administrativos: Oficio de designación firmado por el responsable de su entidad, que lo acredita como representante designado, dicho oficio contiene el nombre del representante y la entidad de que procede. 2. Datos personales sensibles: No se solicitan.
Responsable*:	
Nombre*	Lydia Lara Barragán Vite
Cargo*	<u>Líder de proyecto.</u>
Funciones*	Recabar la información de los representantes de la Red Universitaria para la Sustentabilidad.
Obligaciones*	- Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. - Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados.
	Encargados:
(Nombre del Encargado 1*)	Raquel Radahy Rodríguez Granados
Cargo*:	Asistente administrativo
Funciones*:	- Integrar la información de los representantes de la Red Universitaria para la Sustentabilidad. - Elaborar y enviar oficios de invitación y minutas de las reuniones de la Red Universitaria para la Sustentabilidad.

Obligaciones*:	• Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. • Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados.
-----------------------	---

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

Subdirección de Campus Sustentables	
Identificador único**	COUS 4
(Nombre del sistema A1*)	Red Universitaria para la Sustentabilidad
Tipo de soporte: *	-Soporte electrónico: Computadora de la responsable de la Red Universitaria para la Sustentabilidad en base de datos digital en hojas de cálculo Excel. -Correos electrónicos: rus.cous@unam.mx; cous@unam.mx (correo manejado por DGTIC)
Descripción: *	-Correos institucionales manejados por DGTIC.
Características del lugar donde se resguardan los soportes: *	Alojamiento en los correos electrónicos institucionales y en la computadora de escritorio de la responsable del sistema Red Universitaria para la Sustentabilidad.

3. ANÁLISIS DE RIESGOS

Eliminado: Cinco renglones en los que se especifican los riesgos, diez con el impacto y veinticuatro con la mitigación, correspondientes al análisis de riesgos.
Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Subdirección de Campus Sustentables		
Identificador único**	COUS 4	
(Nombre del sistema A1*)	Red Universitaria para la Sustentabilidad	
Riesgo*	Impacto*	Mitigación*
Comentario	Comentario	Comentario
		Comentario
		Comentario
		Comentario
		Comentario
Comentario	Comentario	Comentario

Eliminado: Tres renglones en los que se especifican los riesgos, diecisiete con el impacto y treinta y siete con la mitigación, correspondientes al análisis de riesgos.
Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

		Comentario
		Comentario
		Comentario
		Comentario
Comentario	Comentario	Comentario
Comentario	Comentario	Comentario Comentario
Comentario	Comentario	Comentario

Eliminado: Tres renglones en los que se especifica la mitigación, correspondiente al análisis de riesgos. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

		Comentario
--	--	-------------------

4. ANÁLISIS DE BRECHA

Eliminado: Diez renglones en los que se especifican las medidas de seguridad actuales, cinco con las medidas de seguridad necesarias y once con las acciones para remediación, correspondientes al análisis de brecha. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Subdirección de Campus Sustentables		
Identificador único**	COUS 4	
(Nombre del sistema A1*)	Red Universitaria para la Sustentabilidad	
Medida de seguridad actual*	Medida de seguridad necesaria*	Acciones para remediación*
Comentario	Comentario	Comentario
Comentario		
Comentario		Comentario

5. PLAN DE TRABAJO

Eliminado: Seis renglones en los que se especifican las actividades, treinta con la descripción, tres con la duración y once con la cobertura, correspondientes al plan de trabajo. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Subdirección de Campus Sustentables			
Identificador único**	COUS 4		
(Nombre del sistema A1*)	Red Universitaria para la Sustentabilidad		
Actividad*	Descripción*	Duración*	Cobertura*
Comentario	Comentario	Comentario	Comentario
Comentario	Comentario	Comentario	Comentario
Comentario	Comentario	Comentario	Comentario

Eliminado: Cuatro renglones en los que se especifican las actividades, catorce con la descripción, dos con la duración y nueve con la cobertura, correspondientes al plan de trabajo. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

	Comentario		
Comentario	Comentario	Comentario	Comentario
Comentario	Comentario	Comentario	Comentario

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Subdirección de Campus Sustentables	
Identificador único**	COUS 4
(Nombre del sistema A1*)	Red Universitaria para la Sustentabilidad
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realiza traslado en soporte físico.
Transferencias mediante el traslado de soportes electrónicos:	No se realiza traslado en soporte electrónico.
Transferencias mediante el traslado sobre redes electrónicas:	La información de datos personales se almacena en los correos electrónicos administrados por el Centro de Datos de la UNAM.

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

N/A

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

N/A

IV. REGISTRO DE INCIDENTES:

N/A

V. ACCESO A LAS INSTALACIONES

Los accesos al Antiguo edificio de posgrado están asegurados por un sistema de identificación biométrica en el acceso al edificio y en el acceso al ala donde se encuentra la COUS. Adicionalmente el acceso a las oficinas de la COUS está asegurado por una puerta con dos llaves. El edificio cuenta con sistema de Circuito cerrado las 24 horas.

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

La COUS con el apoyo de la Jefatura de TIC's de la SDI realiza las actualizaciones de software y hardware en los equipos en los que se encuentra contenido el sistema de tratamiento de datos personales.

VII. PERFILES DE USUARIO Y CONTRASEÑAS

La responsable de la Red Universitaria para la Sustentabilidad es la administradora única de las contraseñas y de la información relacionada con datos personales.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

El respaldo de la información recopilada por la encargada de la Red Universitaria para la Sustentabilidad se almacena en los correos: cous@unam.mx y rus.cous@unam.mx.

Ambas cuentas de correo electrónico son administradas por la Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC) de la UNAM.

IX. PLAN DE CONTINGENCIA

Se desconoce el procedimiento ya que es responsabilidad de la DGTIC.

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

VI.1 Herramientas y recursos para monitoreo de la protección de datos personales

Subdirección de Campus Sustentables

Identificador único	COUS 4	
Nombre del sistema	Red Universitaria para la Sustentabilidad	
Recurso*	Descripción*	Control*
N/A	N/A	N/A

7.1 Procedimiento para la revisión de las medidas de seguridad

Subdirección de Campus Sustentables		
Identificador único	COUS 4	
Nombre del sistema	Red Universitaria para la Sustentabilidad	
Medida de seguridad*	Procedimiento*	Responsable*
N/A	N/A	N/A

7.2 Resultados de la evaluación y pruebas a las medidas de seguridad

Subdirección de Campus Sustentables		
Identificador único	COUS 4	
Nombre del sistema	Red Universitaria para la Sustentabilidad	
Medida de seguridad*	Resultado de evaluación*	Responsable*
N/A	N/A	N/A

7.3 Acciones para la corrección y actualización de las medidas de seguridad

Subdirección de Campus Sustentables		
--	--	--

Identificador único	COUS 4	
Nombre del sistema	Red Universitaria para la Sustentabilidad	
Medida de seguridad*	Acciones*	Responsable*
N/A	N/A	d) N/A

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

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

Subdirección de Campus Sustentables			
Identificador único	COUS 4		
Nombre del sistema	Red Universitaria para la Sustentabilidad		
Actividad*	Descripción*	Duración*	Cobertura*
La COUS solicitará a la Unidad de Transparencia de la UNAM programar un curso enfocado a la capacitación del personal involucrado en la captación, manejo, resguardo y seguridad de datos personales. De igual forma, se buscarán cursos relacionados que impartan otras instancias como el INAI.	Cursos relacionados con la protección y seguridad de datos personales	Capacitación por lo menos una vez al año.	Deberán asistir por lo menos dos personas de cada área que maneje datos personales en la COUS.

8.2 Programa de difusión de la protección a los datos personales

Subdirección de Campus Sustentables			
Identificador único	COUS 4		
Nombre del sistema	Red Universitaria para la Sustentabilidad		
Actividad*	Descripción*	Duración*	Cobertura*
Difusión de protección de datos personales	El 25 de febrero de 2019, la UNAM difundió en la Gaceta UNAM los Lineamientos para la protección de datos personal en posesión de la UNAM	Permanente	Institucional

9. MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

Subdirección de Campus Sustentables			
Identificador único*	COUS 4		
Nombre del sistema	Red Universitaria para la Sustentabilidad		
Actividad*	Descripción*	Duración*	Cobertura*
N/A	N/A	N/A	N/A

9.2 Actualización y mantenimiento de equipo de cómputo

Subdirección de Campus Sustentables	
Identificador único	COUS 4

Nombre del sistema		Red Universitaria para la Sustentabilidad	
Actividad*	Descripción*	Duración*	Cobertura*
Mantenimiento preventivo	Realizar el mantenimiento preventivo del equipo de cómputo tanto a nivel hardware como software para su funcionamiento óptimo.	2 veces por año	Equipos asignados a la Coordinación Universitaria para la Sustentabilidad (COUS).

9.3 Procesos para la conservación, preservación y respaldos de información

Subdirección de Campus Sustentables		
Identificador único	COUS 4	
Nombre del sistema	Red Universitaria para la Sustentabilidad	
Proceso*	Descripción*	Responsable*
N/A	N/A	N/A

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

Subdirección de Campus Sustentables		
Identificador único	COUS 4	
Nombre del sistema	Red Universitaria para la Sustentabilidad	
Proceso	Descripción*	Responsable*

Procesos de borrado seguro y disposición final de equipos y componentes informáticos.	Procesos de borrado seguro y disposición final de equipos y componentes informáticos.	Jefa de Departamento de TIC de la SDI
---	---	---------------------------------------

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

N/A

COORDINACIÓN DE CAMPUS SUSTENTABLES

(5)

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Coordinación de Campus Sustentables	
Identificador único*	(COUS-3)
(Nombre del sistema A1) *	Bitácora del responsable Sanitario de la Coordinación Universitaria para la Sustentabilidad (COUS) / Comité de Seguimiento COVID-19
Datos personales (sensibles o no) contenidos en el sistema*	1. Datos personales en general: a) Datos de identificación: Nombre, correo electrónico, RFC. b) Datos laborales: Número de Trabajador, Nombramiento, correo electrónico institucional. 2. Datos personales sensibles: Estado de salud del personal de la COUS, sospechoso o confirmado de COVID-19 y esquema de vacunación de COVID-19.
Responsable*:	
Nombre*	María Alejandra Fonseca Salazar
Cargo*	<u>Jefe de departamento</u>
Funciones*	• Difundir las medidas implementadas por la Universidad para la protección de la salud de la comunidad, en apego a los Lineamientos generales para el regreso a las actividades universitarias en el marco de la pandemia de COVID-19. • Recibir a través del correo institucional, la notificación por parte del personal de la COUS, sospechoso o confirmado de la enfermedad COVID-19. • Establecer comunicación con el personal de la COUS, que se reporten como sospechosos o confirmados de COVID-19. • En los casos confirmados de COVID 19, promover el cumplimiento del Protocolo para el regreso a las actividades universitarias en el marco de la pandemia de COVID-19, de la COUS • Mantener actualizada la Bitácora del responsable Sanitario en la plataforma del Comité de Seguimiento Covid-19, que incluye: – El personal de la COUS que pertenecen a la población en probable situación de

	vulnerabilidad, de acuerdo con los criterios de vulnerabilidad que emite el Comité de Expertos o las autoridades de salud. – Registro de personal sospechosos o confirmados de COVID-19. – Registro de personal con esquema de vacunación de la COUS.
Obligaciones*	• Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. • Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados.

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

Coordinación de Enlace y Seguimiento	
• Identificador único**	• (COUS-3)
• (Nombre del sistema A1*)	• Bitácora del responsable Sanitario de la Coordinación Universitaria para la Sustentabilidad (COUS) / Comité de Seguimiento COVID-19
Tipo de soporte: *	Soporte electrónico
Descripción: *	Soporte electrónico: • Disco magnético HD. • Nube privada.
Características del lugar donde se resguardan los soportes: *	Disco magnético HD de la computadora asignada al responsable. Nube privada iCloudDrive asociada a la cuenta de correo institucional del responsable: alejandra.fonseca@unam.mx. Plataforma del Comité de Seguimiento COVID-19, en servidor administrado por la Secretaría Administrativa de la UNAM.

3. ANÁLISIS DE RIESGOS

Eliminado: Seis renglones en los que se especifican los riesgos, ocho con el impacto y dieciocho con la mitigación, correspondientes al análisis de riesgos. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Coordinación de Enlace y Seguimiento		
Identificador único**	(COUS-3)	
(Nombre del sistema A1*)	Bitácora del responsable Sanitario de la Coordinación Universitaria para la Sustentabilidad (COUS) / Comité de Seguimiento COVID-19	
Riesgo*	Impacto*	Mitigación*
Comentario	Comentario	Comentario
		Comentario
Comentario	Comentario	Comentario

4. ANÁLISIS DE BRECHA

Eliminado: Dieciséis renglones en los que se especifican las medidas de seguridad actuales, tres con las medidas de seguridad necesarias y doce con las acciones para remediación, correspondientes al análisis de brecha.
Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Coordinación de Enlace y Seguimiento		
Identificador único**	(COUS-3)	
(Nombre del sistema A1*)	Bitácora del responsable Sanitario de la Coordinación Universitaria para la Sustentabilidad (COUS) / Comité de Seguimiento COVID-19	
Medida de seguridad actual*	Medida de seguridad necesaria*	Acciones para remediación*
Comentario		
Comentario	Comentario	Comentario
Comentario	Comentario	Comentario

5. PLAN DE TRABAJO

Eliminado: Cuatro renglones en los que se especifican las actividades, once con la descripción, uno con la duración y cinco con la cobertura, correspondientes al plan de trabajo.
Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Coordinación de Enlace y Seguimiento			
Identificador único**	(COUS-3)		
(Nombre del sistema A1*)	Bitácora del responsable Sanitario de la Coordinación Universitaria para la Sustentabilidad (COUS) / Comité de Seguimiento COVID-19		
Actividad*	Descripción*	Duración*	Cobertura*
Comentario	Comentario	Comentario	Comentario

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Coordinación de Enlace y Seguimiento	
Identificador único**	(COUS-3)
(Nombre del sistema A1*)	Bitácora del responsable Sanitario de la Coordinación Universitaria para la Sustentabilidad (COUS) / Comité de Seguimiento COVID-19
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No aplica
Transferencias mediante el traslado de soportes electrónicos:	No aplica
Transferencias mediante el traslado sobre redes electrónicas:	La transferencia de la información es cifrada mediante protocolos SSL/TLS en la red interna.

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

La Bitácora del responsable Sanitario de la COUS no realiza tratamiento de datos personales con soportes físicos, ya que se encuentra en electrónico a través del mismo sistema.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

La Bitácora del responsable Sanitario de la COUS cuenta con una opción de Consulta, la cual permite visualizar el reporte de los casos sospechosos o confirmados, así como el esquema de vacunación del personal de la COUS.

I. REGISTRO DE INCIDENTES

No contamos con un procedimiento de atención de incidentes.

V. ACCESO A LAS INSTALACIONES

Los accesos al Antiguo edificio de posgrado están asegurados por un sistema de identificación biométrica en el acceso al edificio y en el acceso al ala donde se encuentra la COUS. Adicionalmente el acceso a las oficinas de la COUS está asegurado por una puerta con dos llaves. El edificio cuenta con sistema de Circuito cerrado las 24 horas.

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

La Secretaría Administrativa de la UNAM, es la encargada realizar las actualizaciones y/o notificaciones de los posibles cambios realizados a la Plataforma.

VII. PERFILES DE USUARIO Y CONTRASEÑAS

La Plataforma del Comité de Seguimiento COVID-19 de la UNAM está diseñado para que cada responsable Sanitario tenga un usuario y contraseña, para ingresar a la Bitácora de responsable Sanitario de su dependencia, para la actualización. Los usuarios y contraseñas son autorizados por el Comité de Seguimiento.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

Esta actividad es garantizada por el Comité de Seguimiento a través de la Secretaría Administrativa de la UNAM.

IX. PLAN DE CONTINGENCIA

Esta actividad es garantizada por el Comité de Seguimiento a través de la Secretaría Administrativa de la UNAM.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD Herramientas y recursos para monitoreo de la protección de datos personales

Coordinación de Enlace y Seguimiento	
Identificador único	(COUS-3)

Nombre del sistema	Bitácora del responsable Sanitario de la Coordinación Universitaria para la Sustentabilidad (COUS) / Comité de Seguimiento COVID-19	
Recurso*	Descripción*	Control*
N/A	N/A	N/A

7.1 Procedimiento para la revisión de las medidas de seguridad

Coordinación de Enlace y Seguimiento		
Identificador único	(COUS-3)	
Nombre del sistema	Bitácora del responsable Sanitario de la Coordinación Universitaria para la Sustentabilidad (COUS) / Comité de Seguimiento COVID-19	
Medida de seguridad*	Procedimiento*	Responsable*
N/A	N/A	N/A

7.2 Resultados de la evaluación y pruebas a las medidas de seguridad

Coordinación de Enlace y Seguimiento		
Identificador único	(COUS-3)	
Nombre del sistema	Bitácora del responsable Sanitario de la Coordinación Universitaria para la Sustentabilidad (COUS) / Comité de Seguimiento COVID-19	
Medida de seguridad*	Resultado de evaluación*	Responsable*
N/A	N/A	N/A

7.3 Acciones para la corrección y actualización de las medidas de seguridad

Coordinación de Enlace y Seguimiento		
Identificador único	(COUS-3)	
(Nombre del sistema A1)*	Bitácora del responsable Sanitario de la Coordinación Universitaria para la Sustentabilidad (COUS) / Comité de Seguimiento COVID-19	
Medida de seguridad*	Acciones*	Responsable*
N/A	N/A	N/A

8 PROGRAMA ESPECÍFICO DE CAPACITACIÓN

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

Coordinación de Enlace y Seguimiento			
Identificador único	(COUS-3)		
Nombre del sistema	Bitácora del responsable Sanitario de la Coordinación Universitaria para la Sustentabilidad (COUS) / Comité de Seguimiento COVID-19		
Actividad*	Descripción*	Duración*	Cobertura*
La COUS solicitará a la Unidad de Transparencia de la UNAM programar un curso enfocado a la capacitación del personal involucrado en la captación, manejo, resguardo y seguridad de datos personales. De igual forma, se buscarán cursos relacionados que	Cursos relacionados con la protección y seguridad de datos personales	Capacitación por lo menos una vez al año.	Deberán asistir por lo menos dos personas de cada área que maneje datos personales en la COUS.

impartan otras instancias como el INAI.			
---	--	--	--

8.2 Programa de difusión de la protección a los datos personales

Coordinación de Enlace y Seguimiento			
Identificador único	(COUS-3)		
Nombre del sistema	Bitácora del responsable Sanitario de la Coordinación Universitaria para la Sustentabilidad (COUS) / Comité de Seguimiento COVID-19		
Actividad*	Descripción*	Duración*	Cobertura*
Difusión de protección de datos personales	El 25 de febrero de 2019, la UNAM difundió en la Gaceta UNAM los Lineamientos para la protección de datos personal en posesión de la UNAM.	Permanente	Institucional

9 MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

Coordinación de Enlace y Seguimiento	
Identificador único*	(COUS-3)
Nombre del sistema	Bitácora del responsable Sanitario de la Coordinación Universitaria para la Sustentabilidad (COUS) / Comité de Seguimiento COVID-19

Actividad*	Descripción*	Duración*	Cobertura*
Registro de casos sospechosos, confirmados y esquema de vacunación.	Alimentar la bitácora del responsable Sanitario de la COUS.	Hasta que las autoridades lo consideren pertinente.	Contribuir a mantener actualizados los datos para el Comité de Seguimiento COVID-19 de la UNAM.

9.2 Actualización y mantenimiento de equipo de cómputo

Coordinación de Enlace y Seguimiento

Identificador único	(COUS-3)		
Nombre del sistema	Bitácora del responsable Sanitario de la Coordinación Universitaria para la Sustentabilidad (COUS) / Comité de Seguimiento COVID-19		
Actividad*	Descripción*	Duración*	Cobertura*
Identificar los requerimientos técnicos, para ingresar a la Bitácora del responsable Sanitario del Comité de Seguimiento COVID-19.	Proporcionar a las áreas de trabajo los equipos de cómputo para una mejor funcionalidad.	Permanente	Se trata de mantener actualizada la Bitácora sobre el Seguimiento Covid-19.

9.3 Procesos para la conservación, preservación y respaldos de información

Coordinación de Enlace y Seguimiento

Identificador único	(COUS-3)		
---------------------	----------	--	--

Nombre del sistema	Bitácora del responsable Sanitario de la Coordinación Universitaria para la Sustentabilidad (COUS) / Comité de Seguimiento COVID-19	
Proceso*	Descripción*	Responsable*
N/A	N/A	Esta actividad la realiza la Secretaría Administrativa de la UNAM.

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

Coordinación de Enlace y Seguimiento		
Identificador único	(COUS-3)	
Nombre del sistema	Bitácora del responsable Sanitario de la Coordinación Universitaria para la Sustentabilidad (COUS) / Comité de Seguimiento COVID-19	
Proceso	Descripción*	Responsable*
Procesos de borrado seguro y disposición final de equipos y componentes informáticos.	Procesos de borrado seguro y disposición final de equipos y componentes informáticos.	Jefa de Departamento de Gestión Institucional

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

Las personas que cuenten con usuario y contraseña en la Bitácora del responsable Sanitario del Comité de Seguimiento COVID-19, no tiene injerencia en el procedimiento para la cancelación del sistema de tratamiento de datos personales, debido a que esta actividad depende de la Secretaría Administrativa de la UNAM.

SUBDIRECCIÓN DE EDUCACIÓN Y VINCULACIÓN PARA LA SUSTENTABILIDAD

(6)

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Subdirección de Educación y Vinculación para la Sustentabilidad	
Identificador único*	COUS 5
(Nombre del sistema A1) *	Taller de Profesores de introducción a la Sustentabilidad
Datos personales (sensibles o no) contenidos en el sistema*	1. Datos personales en general: a) Datos de identificación: Nombre completo, género, correo electrónico, teléfono. 2. Datos personales sensibles: No se solicitan.
Responsable*:	
Nombre*	Verónica Elena Solares Rojas
Cargo*	Subdirectora de Educación y Vinculación para la Sustentabilidad
Funciones*	Recabar la información de los asistentes al Taller de Profesores de introducción a la Sustentabilidad.
Obligaciones*	- Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. - Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados.
	Encargados:
(Nombre del Encargado 1*)	Raquel Radahy Rodríguez Granados
Cargo*:	Asistente administrativo
Funciones*:	- Integrar la información de los asistentes al Taller de Profesores de introducción a la Sustentabilidad. - Enviar el temario e información referente al Taller de Profesores de introducción a la Sustentabilidad.

Obligaciones*:	• Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. • Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados.
-----------------------	---

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

Subdirección de Educación y Vinculación para la Sustentabilidad	
Identificador único**	COUS 5
(Nombre del sistema A1*)	Taller de Profesores de introducción a la Sustentabilidad
Tipo de soporte: *	Soporte electrónico: Base de datos digital en hojas de cálculo Excel.
Descripción: *	La base de datos está en una hoja de cálculo Excel en el disco duro de la computadora de la responsable.
Características del lugar donde se resguardan los soportes: *	La información se resguarda en el disco duro de la computadora de la responsable.

3. ANÁLISIS DE RIESGOS

Eliminado: Cinco renglones en los que se especifican los riesgos, diez con el impacto y veintiséis con la mitigación, correspondientes al análisis de riesgos.
Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Subdirección de Educación y Vinculación para la Sustentabilidad		
Identificador único**	COUS 5	
(Nombre del sistema A1*)	Taller de Profesores de introducción a la Sustentabilidad	
Riesgo*	Impacto*	Mitigación*
Comentario	Comentario	Comentario
		Comentario
		Comentario
		Comentario
Comentario	Comentario	Comentario
		Comentario

Eliminado: Tres renglones en los que se especifican los riesgos, dieciséis con el impacto y treinta con la mitigación, correspondientes al análisis de riesgos. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

		Comentario
		Comentario
		Comentario
Comentario	Comentario	Comentario
Comentario	Comentario	Comentario Comentario
Comentario	Comentario	Comentario

4. ANÁLISIS DE BRECHA

Eliminado: Diez renglones en los que se especifican las medias de seguridad actuales, cinco con las medidas de seguridad necesarias y once con las acciones para remediación, correspondientes al análisis de brecha. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Subdirección de Educación y Vinculación para la Sustentabilidad		
Identificador único**	COUS 5	
(Nombre del sistema A1*)	Taller de Profesores de introducción a la Sustentabilidad	
Medida de seguridad actual*	Medida de seguridad necesaria*	Acciones para remediación*
Comentario		Comentario
Comentario	Comentario	
Comentario		Comentario

5. PLAN DE TRABAJO

Eliminado: Seis renglones en los que se especifican las actividades, veintisiete con la descripción, tres con la duración y once con la cobertura, correspondientes al plan de trabajo. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Subdirección de Educación y Vinculación para la Sustentabilidad			
Identificador único**	COUS 5		
(Nombre del sistema A1*)	Taller de Profesores de introducción a la Sustentabilidad		
Actividad*	Descripción*	Duración*	Cobertura*
Comentario	Comentario	Comentario	Comentario
Comentario	Comentario	Comentario	Comentario
Comentario	Comentario	Comentario	Comentario
Comentario	Comentario	Comentario	Comentario

Eliminado: Cuatro renglones en los que se especifican las actividades, doce con la descripción, dos con la duración y nueve con la cobertura, correspondientes al plan de trabajo. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Comentario	Comentario	Comentario	Comentario
Comentario	Comentario	Comentario	Comentario

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Subdirección de Educación y Vinculación para la Sustentabilidad	
Identificador único**	COUS 5
(Nombre del sistema A1*)	Taller de Profesores de introducción a la Sustentabilidad
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realiza traslado en soporte físico.
Transferencias mediante el traslado de soportes electrónicos:	No se realiza traslado en soporte electrónico.
Transferencias mediante el traslado sobre redes electrónicas:	El formulario se almacena en el correo electrónico institucional administrado por el Centro de Datos de la UNAM.

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

N/A

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

N/A

IV. REGISTRO DE INCIDENTES:

N/A

V. ACCESO A LAS INSTALACIONES

Los accesos al Antiguo edificio de posgrado están asegurados por un sistema de identificación biométrica en el acceso al edificio y en el acceso al ala donde se encuentra la COUS. Adicionalmente el acceso a las oficinas de la COUS está asegurado por una puerta con dos llaves. El edificio cuenta con sistema de Circuito cerrado las 24 horas.

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

La COUS con el apoyo de la Jefatura de TIC's de la SDI realiza las actualizaciones de software y hardware en los equipos en los que se encuentra contenido el sistema de tratamiento de datos personales.

VII. PERFILES DE USUARIO Y CONTRASEÑAS

La responsable de la Taller de Profesores de introducción a la Sustentabilidad es la administradora única de las contraseñas y de la información relacionada con datos personales.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

El respaldo de la información recopilada por la encargada de la Taller de Profesores de introducción a la Sustentabilidad se almacena en los correos cous@unam.mx y veronica.solares@unam.mx.

Ambas cuentas de correo electrónico son administradas por la Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC) de la UNAM.

IX. PLAN DE CONTINGENCIA

Se desconoce el procedimiento ya que es responsabilidad de la DGTIC.

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

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

Subdirección de Educación y Vinculación para la Sustentabilidad

Identificador único	COUS 5	
Nombre del sistema	Taller de Profesores de introducción a la Sustentabilidad	
Recurso*	Descripción*	Control*
N/A	N/A	N/A

7.2 Procedimiento para la revisión de las medidas de seguridad

Subdirección de Educación y Vinculación para la Sustentabilidad		
Identificador único	COUS 5	
Nombre del sistema	Taller de Profesores de introducción a la Sustentabilidad	
Medida de seguridad*	Procedimiento*	Responsable*
N/A	N/A	N/A

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

Subdirección de Educación y Vinculación para la Sustentabilidad		
Identificador único	COUS 5	
Nombre del sistema	Taller de Profesores de introducción a la Sustentabilidad	
Medida de seguridad*	Resultado de evaluación*	Responsable*
N/A	N/A	N/A

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

Subdirección de Educación y Vinculación para la Sustentabilidad		
--	--	--

Identificador único	COUS 5	
Nombre del sistema	Taller de Profesores de introducción a la Sustentabilidad	
Medida de seguridad*	Acciones*	Responsable*
N/A	N/A	e) N/A

8 PROGRAMA ESPECÍFICO DE CAPACITACIÓN

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

Subdirección de Educación y Vinculación para la Sustentabilidad			
Identificador único	COUS 5		
Nombre del sistema	Taller de Profesores de introducción a la Sustentabilidad		
Actividad*	Descripción*	Duración*	Cobertura*
La COUS solicitará a la Unidad de Transparencia de la UNAM programar un curso enfocado a la capacitación del personal involucrado en la captación, manejo, resguardo y seguridad de datos personales. De igual forma, se buscarán cursos relacionados que impartan otras instancias como el INAI.	Cursos relacionados con la protección y seguridad de datos personales	Capacitación por lo menos una vez al año.	Deberán asistir por lo menos dos personas de cada área que maneje datos personales en la COUS.

8.2 Programa de difusión de la protección a los datos personales

Subdirección de Educación y Vinculación para la Sustentabilidad			
Identificador único	COUS 5		
Nombre del sistema	Taller de Profesores de introducción a la Sustentabilidad		
Actividad*	Descripción*	Duración*	Cobertura*
Difusión de protección de datos personales	El 25 de febrero de 2019, la UNAM difundió en la Gaceta UNAM los Lineamientos para la protección de datos personal en posesión de la UNAM	Permanente	Institucional

9 MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

Subdirección de Educación y Vinculación para la Sustentabilidad			
Identificador único*	COUS 5		
Nombre del sistema	Taller de Profesores de introducción a la Sustentabilidad		
Actividad*	Descripción*	Duración*	Cobertura*
N/A	N/A	N/A	N/A

9.2 Actualización y mantenimiento de equipo de cómputo

Subdirección de Educación y Vinculación para la Sustentabilidad	
Identificador único	COUS 5

Nombre del sistema		Taller de Profesores de introducción a la Sustentabilidad	
Actividad*	Descripción*	Duración*	Cobertura*
Mantenimiento preventivo	Realizar el mantenimiento preventivo del equipo de cómputo tanto a nivel hardware como software para su funcionamiento óptimo.	2 veces por año	Equipos asignados a la Coordinación Universitaria para la Sustentabilidad (COUS).

9.3 Procesos para la conservación, preservación y respaldos de información

Subdirección de Educación y Vinculación para la Sustentabilidad		
Identificador único	COUS 5	
Nombre del sistema	Taller de Profesores de introducción a la Sustentabilidad	
Proceso*	Descripción*	Responsable*
N/A	N/A	N/A

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

Subdirección de Educación y Vinculación para la Sustentabilidad		
Identificador único	COUS 5	
Nombre del sistema	Taller de Profesores de introducción a la Sustentabilidad	
Proceso	Descripción*	Responsable*

Procesos de borrado seguro y disposición final de equipos y componentes informáticos.	Procesos de borrado seguro y disposición final de equipos y componentes informáticos.	Jefa de Departamento de TIC de la SDI
---	---	---------------------------------------

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

N/A

SUBDIRECCIÓN DE EDUCACIÓN Y VINCULACIÓN PARA LA SUSTENTABILIDAD

(7)

1 INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Participación incluyente	
Identificador único*	COUS 6
(Nombre del sistema A1) *	Programa de participación incluyente
Datos personales (sensibles o no) contenidos en el sistema*	1. Datos personales en general: a) Datos de identificación: Nombre completo, correo electrónico. b) Datos académicos: Trayectoria educativa, Número de cuenta. 2. Datos personales sensibles: No se solicitan.
Responsable*:	
Nombre*	Lydia Lara Barragán Vite
Cargo*	<u>Líder de proyecto.</u>
Funciones*	Recabar la información de los participantes en las actividades de Participación incluyente.
Obligaciones*	- Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. - Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados.
	Encargados:
(Nombre del Encargado 1*)	Raquel Radahy Rodríguez Granados
Cargo*:	Asistente administrativa
Funciones*:	- Integrar la información de los participantes en las actividades del programa de participación incluyente. - Elaborar y enviar convocatorias, programas e información relacionada con las actividades del programa de participación incluyente.

Obligaciones*:	• Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. • Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados.
-----------------------	---

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

Participación incluyente	
Identificador único**	COUS 6
(Nombre del sistema A1*)	Programa de participación incluyente
Tipo de soporte: *	-Soporte electrónico: Computadora de la responsable del programa de participación incluyente en base de datos digital en hojas de cálculo Excel. -Correos electrónicos: lydya.lara@unam.mx; participacion.cous@unam.mx
Descripción: *	-Correos institucionales manejados por DGTIC
Características del lugar donde se resguardan los soportes: *	Alojamiento en el correo electrónico institucional y en la computadora de escritorio de la responsable del programa de participación incluyente.

3. ANÁLISIS DE RIESGOS

Eliminado: Cinco renglones en los que se especifican los riesgos, diez con el impacto y veinticinco con la mitigación, correspondientes al análisis de riesgos.
Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Participación incluyente		
Identificador único**	COUS 6	
(Nombre del sistema A1*)	Programa de participación incluyente	
Riesgo*	Impacto*	Mitigación*
Comentario	Comentario	Comentario
		Comentario
		Comentario
		Comentario
Comentario	Comentario	Comentario
Comentario	Comentario	Comentario

Eliminado: Tres renglones en los que se especifican los riesgos, diecisiete con el impacto y treinta y cuatro con la mitigación, correspondientes al análisis de riesgos.
Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

		Comentario Comentario Comentario Comentario
Comentario	Comentario	Comentario
Comentario	Comentario	Comentario Comentario
Comentario	Comentario	Comentario

4. ANÁLISIS DE BRECHA

Eliminado: Catorce renglones en los que se especifican las medidas de seguridad actuales, cinco con las medidas de seguridad necesarias y diez con las acciones para remediación, correspondientes al análisis de brecha.
Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Participación incluyente		
Identificador único**	COUS 6	
(Nombre del sistema A1*)	Programa de participación incluyente	
Medida de seguridad actual*	Medida de seguridad necesaria*	Acciones para remediación*
Comentario	Comentario	Comentario
Comentario		
Comentario		Comentario
Comentario		

5. PLAN DE TRABAJO

Eliminado: Once renglones en los que se especifican las actividades, veintitrés con la descripción, cuatro con la duración y quince con la cobertura, correspondientes al plan de trabajo. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Participación incluyente			
Identificador único**	COUS 6		
(Nombre del sistema A1*)	Programa de participación incluyente		
Actividad*	Descripción*	Duración*	Cobertura*
Comentario	Comentario	Comentario	Comentario
Comentario	Comentario	Comentario	Comentario
Comentario	Comentario	Comentario	Comentario
Comentario	Comentario	Comentario	Comentario
Comentario	Comentario	Comentario	Comentario

Eliminado: Dos renglones en los que se especifican las actividades, cinco con la descripción, uno con la duración y siete con la cobertura, correspondientes al plan de trabajo.
Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

	Comentario		Comentario
Comentario	Comentario	Comentario	Comentario

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

1. TRANSFERENCIAS DE DATOS PERSONALES

Participación incluyente	
Identificador único**	COUS 6
(Nombre del sistema A1*)	Programa de participación incluyente
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realiza traslado en soporte físico.
Transferencias mediante el traslado de soportes electrónicos:	No se realiza traslado en soporte electrónico.
Transferencias mediante el traslado sobre redes electrónicas:	El formulario se almacena en el correo electrónico institucional administrado por el Centro de Datos de la UNAM.

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

N/A

3. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

N/A

4. REGISTRO DE INCIDENTES:

N/A

5. ACCESO A LAS INSTALACIONES

Los accesos al Antiguo edificio de posgrado están asegurados por un sistema de identificación biométrica en el acceso al edificio y en el acceso al ala donde se encuentra la COUS. Adicionalmente el acceso a las oficinas de la COUS está asegurado por una puerta con dos llaves. El edificio cuenta con sistema de Circuito cerrado las 24 horas.

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

La COUS con el apoyo de la Jefatura de TIC's de la SDI realiza las actualizaciones de software y hardware en los equipos en los que se encuentra contenido el sistema de tratamiento de datos personales.

VII. PERFILES DE USUARIO Y CONTRASEÑAS

La responsable de la Participación incluyente es la administradora única de las contraseñas y de la información relacionada con datos personales.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

El respaldo de la información recopilada por la encargada de la Participación incluyente se almacena en los correos lydia.lara@unam.mx y participacion.cous@unam.mx

Ambas cuentas de correo electrónico son administradas por la Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC) de la UNAM.

IX. PLAN DE CONTINGENCIA

Se desconoce el procedimiento ya que es responsabilidad de la DGTIC.

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

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

Participación incluyente		
Identificador único	COUS 6	
Nombre del sistema	Programa de participación incluyente	
Recurso*	Descripción*	Control*
N/A	N/A	N/A

b. Procedimiento para la revisión de las medidas de seguridad

Participación incluyente		
Identificador único	COUS 6	
Nombre del sistema	Programa de participación incluyente	
Medida de seguridad*	Procedimiento*	Responsable*
N/A	N/A	N/A

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

Participación incluyente		
Identificador único	COUS 6	
Nombre del sistema	Programa de participación incluyente	
Medida de seguridad*	Resultado de evaluación*	Responsable*
N/A	N/A	N/A

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

Participación incluyente		
Identificador único	COUS 6	
Nombre del sistema	Programa de participación incluyente	
Medida de seguridad*	Acciones*	Responsable*
N/A	N/A	1. N/A

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

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

Participación incluyente			
Identificador único	COUS 6		
Nombre del sistema	Programa de participación incluyente		
Actividad*	Descripción*	Duración*	Cobertura*
La COUS solicitará a la Unidad de Transparencia de la UNAM programar un curso enfocado a la capacitación del personal involucrado en la captación, manejo, resguardo y seguridad de datos personales. De igual forma, se buscarán cursos relacionados que impartan otras instancias como el INAI.	Cursos relacionados con la protección y seguridad de datos personales	Capacitación por lo menos una vez al año.	Deberán asistir por lo menos dos personas de cada área que maneje datos personales en la COUS.

8.2 Programa de difusión de la protección a los datos personales

Participación incluyente			
Identificador único	COUS 6		
Nombre del sistema	Programa de participación incluyente		
Actividad*	Descripción*	Duración*	Cobertura*
Difusión de protección de datos personales	El 25 de febrero de 2019, la UNAM difundió en la Gaceta UNAM los Lineamientos para la protección de datos personal en posesión de la UNAM	Permanente	Institucional

9. MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

Participación incluyente			
Identificador único*	COUS 6		
Nombre del sistema	Programa de participación incluyente		
Actividad*	Descripción*	Duración*	Cobertura*
N/A	N/A	N/A	N/A

9.2 Actualización y mantenimiento de equipo de cómputo

Participación incluyente	
Identificador único	COUS 6

Nombre del sistema		Programa de participación incluyente	
Actividad*	Descripción*	Duración*	Cobertura*
Mantenimiento preventivo	Realizar el mantenimiento preventivo del equipo de cómputo tanto a nivel hardware como software para su funcionamiento óptimo.	2 veces por año	Equipos asignados a la Coordinación Universitaria para la Sustentabilidad (COUS).

9.3 Procesos para la conservación, preservación y respaldos de información

Participación incluyente		
Identificador único	COUS 6	
Nombre del sistema	Programa de participación incluyente	
Proceso*	Descripción*	Responsable*
N/A	N/A	N/A

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

Participación incluyente		
Identificador único	COUS 6	
Nombre del sistema	Programa de participación incluyente	
Proceso	Descripción*	Responsable*

Procesos de borrado seguro y disposición final de equipos y componentes informáticos.	Procesos de borrado seguro y disposición final de equipos y componentes informáticos.	Jefa de Departamento de TIC de la SDI
---	---	---------------------------------------

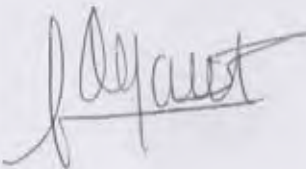
10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

N/A

Coordinación Universitaria para la Sustentabilidad
Documento de Seguridad
Partes clasificadas: Análisis de riesgos (riesgo, impacto y mitigación), páginas 4, 5, 18, 19, 32, 33, 46, 47, 48, 61, 73, 74, 87 y 88; Análisis de brecha (medida de seguridad actual, medida de seguridad necesaria y acciones para remediación), páginas 6, 20, 34, 49, 62, 75 y 89, y Plan de trabajo (actividad, descripción duración y cobertura), páginas 7, 8, 21, 22, 35, 36, 50, 51, 63, 76, 77, 90 y 91.
Periodo de reserva: Por un periodo de cinco años, que se computarán a partir de la fecha de la resolución.
Fundamento: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP) y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP). En virtud de tratarse de información reservada que obstruya la prevención o persecución de los delitos.
Fecha y número de acta de la sesión: 24/08/2022 y acta CTUNAM/528/2022.



11. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

		Nombre y firma de quienes revisaron el presente documento:
Responsable del desarrollo:	M. en C. Alfonso de la Vega Rivera Subdirector de Campus Sustentables en la Coordinación Universitaria para la Sustentabilidad	
Revisó:	Dra. María Alejandra Fonseca Salazar Jefa de Departamento en la Coordinación Universitaria para la Sustentabilidad	
Autorizó:	Dra. Leticia Merino Pérez Coordinadora en la Coordinación Universitaria para la Sustentabilidad	
Fecha de aprobación:	22 de agosto de 2022	
Fecha de actualización:	22 de agosto de 2022	



COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/528/2022

Visto el expediente relativo a la clasificación de reserva total de una parte de la información, para la elaboración de la versión pública, que someten el **Programa Universitario de Estudios del Desarrollo**, la **Dirección General de Actividades Cinematográficas**, la **Dirección General de Publicaciones y Fomento Editorial**, el **Instituto de Ciencias Físicas**, la **Coordinación de Relaciones y Asuntos Internacionales**, el **Programa Universitario de Estudios sobre Asia y África**, la **Dirección General del Patrimonio Universitario**, el **Consejo Académico del Área de las Humanidades y las Artes**, el **Instituto de Astronomía**, la **Escuela Nacional Preparatoria**, **Planteles 9 “Pedro de Alba”**, **2 “Erasmus Castellanos Quinto”** y **7 “Ezequiel A. Chávez”**, la **Unidad Coordinadora de Servicios de Apoyo Administrativo a los Consejos Académicos de Área**, la **Facultad de Estudios Superiores Iztacala**, la **Facultad de Medicina Veterinaria y Zootecnia**, la **Coordinación de Vinculación con el Consejo Universitario**, la **Secretaría Administrativa**, el **Instituto de Investigaciones Estéticas**, el **Centro de Investigaciones Interdisciplinarias en Ciencias y Humanidades**, el **Programa Universitario de Bioética**, la **Dirección General de Bibliotecas y Servicios Digitales de Información**, el **Centro de Enseñanza para Extranjeros**, el **Instituto de Ciencias Aplicadas y Tecnología**, el **Centro de Investigaciones sobre América Latina y el Caribe**, la **Facultad de Estudios Superiores Aragón**, la **Coordinación Universitaria para la Sustentabilidad**, el **Tribunal Universitario**, la **Escuela Nacional Preparatoria, Plantel 1 “Gabino Barreda”**, la **Escuela Nacional de Estudios Superiores, Unidad León**, la **Dirección General de Administración Escolar** y la **Oficina de la Abogacía General**, en relación con sus respectivos **Documentos de Seguridad**, se procede a dictar la presente resolución con base en los siguientes:

ANTECEDENTES

- I. Con fecha 26 de enero de 2017 se publicó en el Diario Oficial de la Federación el Decreto por el que se expide la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, reglamentaria de los artículos 6o., Base A y 16, segundo párrafo, de la Constitución Política de los Estados Unidos Mexicanos, en materia de protección de datos personales en posesión de sujetos obligados.
- II. Mediante Acuerdo **ACT-PUB/19/12/2017.10**, de fecha 19 de diciembre de 2017, publicado en el Diario Oficial de la Federación con fecha 26 de enero de 2018, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales aprobó los Lineamientos Generales de Protección de Datos Personales para el Sector Público.
- III. A través del Acuerdo **ACT-PUB/11/11/2020.05**, de fecha 11 de noviembre de 2020, publicado en el Diario Oficial de la Federación con fecha 25 de noviembre de 2020, dicho Órgano Garante aprobó la adición de un Título Décimo a los Lineamientos Generales de Protección de Datos Personales para el Sector Público, a fin de establecer las disposiciones generales que permitirán desarrollar el procedimiento de diseño y aplicación del sistema y procedimiento para llevar a cabo la evaluación sobre el desempeño de los responsables respecto al cumplimiento de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y demás disposiciones que resulten aplicables en la materia.



COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/528/2022

- IV. Por Acuerdo **ACT-PUB/17/11/2021.05**, de fecha 17 de noviembre de 2021, publicado en el Diario Oficial de la Federación con fecha 26 de noviembre de 2021, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales aprobó los “Instrumentos Técnicos que refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en materia de evaluación del desempeño de los sujetos obligados del sector público federal en el cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados”.
- V. Los artículos 247 y 248 de Lineamientos Generales de Protección de Datos Personales para el Sector Público, así como las reglas Décima Tercera y Décima Cuarta del apartado “V. Reglas de Generales de Evaluación” del Documento Técnico de Evaluación y sus anexos de los Instrumentos Técnicos que refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en materia de Evaluación del Desempeño de los Sujetos Obligados del Sector Público Federal en el Cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, establecen que la información y documentos que se pongan a disposición de los titulares de datos personales y del Instituto, deberán ser revisados por el responsable a fin de verificar que no contengan información confidencial o reservada y, de ser el caso, deberá publicarse la versión pública de dicha documentación.
- Por otra parte, en el apartado “VI. Metodología, criterios, formatos e indicadores en materia de evaluación del desempeño de los responsables respecto al cumplimiento de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y demás disposiciones que resulten aplicables en la materia”, Capítulo II. Criterios y formatos, **Vertiente 2: Deberes, Variable 2.1** Deber de seguridad, se establece que el responsable, por ningún motivo, debe publicar el documento de seguridad de manera íntegra, por lo que deberá poner a disposición la versión pública del mismo, en la cual se deberá proteger la información relativa al plan de trabajo, el análisis de riesgo y el análisis de brecha.
- VI. En términos de los artículos 106, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública; 98 fracción II de la Ley Federal de Transparencia y Acceso a la Información Pública, así como 34, fracción II del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, la clasificación de la información será procedente cuando, entre otros supuestos, se determiné mediante una resolución de autoridad competente.
- VII. La Presidencia del Comité de Transparencia recibió diversos oficios, mediante los cuales las Áreas Universitarias sometieron a consideración de este Cuerpo Colegiado, la clasificación de reserva total de una parte de la información de sus Documentos de Seguridad, mismos que se enlistan a continuación:



**COMITÉ DE TRANSPARENCIA DE LA
UNIVERSIDAD NACIONAL AUTÓNOMA DE
MÉXICO**

RESOLUCIÓN: CTUNAM/528/2022

Oficio	Área Universitaria	Fecha de presentación
CH/PUED/COORD/0058/2022	Programa Universitario de Estudios del Desarrollo	18/08/2022
DGAC/CoNTI/018/2022	Dirección General de Actividades Cinematográficas	
DGPYFE/DG/487/2022	Dirección General de Publicaciones y Fomento Editorial	
ICF/139/2022	Instituto de Ciencias Físicas	
CRAI/232/2022	Coordinación de Relaciones y Asuntos Internacionales	
COHU/PUEAA/128/2022	Programa Universitario de Estudios sobre Asia y África	
DGPU/1806/2022	Dirección General del Patrimonio Universitario	
CJHA/357/2022	Consejo Académico del Área de las Humanidades y las Artes	
IAST/DIR/798/248/590-22	Instituto de Astronomía	
ENP/P9/DIR/048/R/2022	Escuela Nacional Preparatoria, Plantel 9 "Pedro de Alba"	
ENP/PL2/D205/2022	Escuela Nacional Preparatoria 2, "Erasmus Castellanos Quinto"	
ENP7/D/107/22	Escuela Nacional Preparatoria 7, "Ezequiel A. Chávez"	19/08/2022
CAAUCA/241/2022	Unidad Coordinadora de Servicios de Apoyo Administrativo a los Consejos Académicos de Área	
FESI/DIR/MCAA/0387/2022	Facultad de Estudios Superiores, Iztacala	
FMVZ/D/FSG/193/2022	Facultad de Medicina Veterinaria y Zootecnia	
ETR/003/2022	Coordinación de Vinculación con el Consejo Universitario	
SADM/294/2022	Secretaría Administrativa	
IIE/D/159/2022	Instituto de Investigaciones Estéticas	
CEII/D/0265/2022	Centro de Investigaciones Interdisciplinarias en Ciencias y Humanidades	22/08/2022
PUB/DIR/105/2022	Programa Universitario de Bioética	
DGBSDI/640/2022	Dirección General de Bibliotecas y Servicios Digitales de Información	
CEPE/D*CPO/270/2022	Centro de Enseñanza para Extranjeros	
Oficio sin número	Instituto de Ciencias Aplicadas y Tecnología	



COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/528/2022

CIAL/DIR/333/22	Centro de Investigaciones sobre América Latina y el Caribe	23/08/2022
FESAR/DIRA/OJUR/907/2022	Facultad de Estudios Superiores, Aragón	
COUS/087/2022	Coordinación Universitaria para la Sustentabilidad	
T-22/023/01	Tribunal Universitario	
ENP 1/D/147/2022	Escuela Nacional Preparatoria, Plantel 1 "Gabino Barreda"	
ENES-León/OJ/099/2022	Escuela Nacional de Estudios Superiores, Unidad León	
SG/DGAE/1018/2022	Dirección General de Administración Escolar	
OAG/ST/1729/2022	Oficina de la Abogacía General	

En dichos oficios, las Áreas Universitarias informaron lo siguiente:

“Los Instrumentos Técnicos a los que se refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público en materia de evaluación del desempeño de los sujetos obligados del sector público federal en el cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados¹; 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

¹ DOF: 26 de noviembre de 2021



**COMITÉ DE TRANSPARENCIA DE LA
UNIVERSIDAD NACIONAL AUTÓNOMA DE
MÉXICO**

RESOLUCIÓN: CTUNAM/528/2022

Obligados del Sector Público Federal en el Cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

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

Anexos o Políticas	Contenido y su afectación	Páginas
<i>a) Análisis de riesgos</i>	<i>El análisis de riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica ... y otorga herramientas a las personas para implementar un ataque informático a los activos críticos y no críticos.</i>	<i>...</i>
<i>b) Análisis de brecha</i>	<i>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.</i>	<i>...</i>
<i>c) Plan de Trabajo</i>	<i>El plan de trabajo define los controles de seguridad a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes con base en el riesgo real detectado. El uso de esta información permite inferir nuestros riesgos, por cuánto tiempo seguirán así hasta el momento que se implementen nuevos controles.</i>	<i>...</i>

Los fundamentos y motivos se exponen a continuación:

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



COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/528/2022

exacta de las vulnerabilidades de un área universitaria, lo que esta serie de documentos les otorga directamente si se difundiera la información.

- Divulgar el análisis de riesgo, el análisis de brecha ... y el plan de trabajo ... evidencian los nuevos controles que estamos pendientes de implementar, describen la forma en cómo almacenamos técnicamente los datos personales, cómo protegemos los sistemas automatizados de información, qué medidas de seguridad administrativas, físicas y técnicas planeamos establecer de manera gradual y de conformidad con las prioridades y presupuestos otorgado.*
- En este sentido la revelación de la información que obra el análisis de riesgo, el análisis de brecha ... y el plan de trabajo de esta área revela y hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales que obran en nuestros archivos y dejaría imposibilitada a esta área para reaccionar ante posibles amenazas.*

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

En esa inteligencia, el dar a conocer el análisis de riesgo, el análisis de brecha y el plan de trabajo de esta área universitaria, no podrían prevenirse actos ilícitos que pudieran realizarse en contra de los sistemas de información y tratamiento de datos personales, así como en contra de los activos e infraestructura crítica de esta dependencia; por lo que es posible advertir que algunas de las posibles consecuencias de divulgar dicha información podrían derivar en la comisión de diversos delitos tipificados en el Código Penal Federal, como accesos no autorizados a los sistemas, robos de información, suplantación de identidades, entre otros. Es decir, se advierte que la negativa de acceso a la información se motiva en evitar o prevenir la comisión del delito al vulnerar las medidas de seguridad establecidas por esta Área Universitaria, con relación al cumplimiento de los principios de protección de datos personales previsto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

En tal sentido, proteger la información de los documentos relativos al análisis de riesgo, al análisis de brecha y al plan de trabajo de esta área se adecua al principio de proporcionalidad porque se justifica negar su divulgación, toda vez que la pretensión de fondo que persigue la reserva de la información consiste en prevenir las conductas antijurídicas tipificadas, aunado a que la restricción es temporal, hasta en tanto las medidas tomadas caduquen; de igual manera, con la no divulgación de



COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/528/2022

la información se contribuye a garantizar la protección de los datos personales de no solo la comunidad universitaria sino de cualquiera que ponga la confianza en esta Universidad para resguardar sus datos personales.

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

En virtud de lo anterior, le solicito de la manera más atenta que ese Cuerpo Colegiado tenga a bien emitir la resolución que en derecho corresponda ...” (sic).

Establecidos los antecedentes del presente asunto, este Comité procede al análisis de los argumentos referidos con antelación, al tenor de las siguientes:

CONSIDERACIONES

PRIMERA. Con fundamento en lo dispuesto por los artículos 10 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, así como 8, fracción VI del Reglamento de Responsabilidades Administrativas de las y los Funcionarios y Empleados de la Universidad Nacional Autónoma de México, este Órgano Colegiado rige su funcionamiento, entre otros, bajo los principios de imparcialidad, certeza, legalidad, objetividad y profesionalismo. Por ello, al ser un asunto propuesto, entre otras Áreas Universitarias, por la **Oficina de la Abogacía General**, en este acto, el Abogado General y Presidente del Comité de Transparencia, Alfredo Sánchez Castañeda, así como el Director General de Asuntos Jurídicos y Secretario Técnico del Comité de Transparencia, Lic. Jorge Barrera Gutiérrez, formalmente se excusan de conocer del caso, para no afectar la imparcialidad del mismo.

SEGUNDA. De conformidad con lo dispuesto en los artículos 1, 10 y 15, fracción X del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, el Comité de Transparencia de la Universidad Nacional Autónoma de México es competente para analizar la clasificación de reserva total de una parte de la información, para la elaboración de la versión pública de los Documentos de Seguridad, propuesta por el **Programa Universitario de Estudios del Desarrollo**, la **Dirección General de Actividades Cinematográficas**, la **Dirección General de Publicaciones y Fomento Editorial**, el **Instituto de Ciencias Físicas**, la **Coordinación de Relaciones y Asuntos Internacionales**, el **Programa Universitario de Estudios sobre Asia y África**, la **Dirección General del Patrimonio Universitario**, el **Consejo Académico del Área de las Humanidades y las Artes**, el **Instituto de Astronomía**, la **Escuela Nacional Preparatoria**, **Planteles 9 “Pedro de Alba”**, **2 “Erasmus Castellanos Quinto”** y **7 “Ezequiel A. Chávez”**, la **Unidad Coordinadora de Servicios de Apoyo Administrativo a los Consejos Académicos de Área**, la **Facultad de Estudios Superiores Iztacala**, la **Facultad de Medicina Veterinaria y Zootecnia**, la **Coordinación de Vinculación con el Consejo Universitario**, la **Secretaría Administrativa**, el **Instituto de Investigaciones Estéticas**, el **Centro de Investigaciones Interdisciplinarias en Ciencias y**



COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/528/2022

Humanidades, el Programa Universitario de Bioética, la Dirección General de Bibliotecas y Servicios Digitales de Información, el Centro de Enseñanza para Extranjeros, el Instituto de Ciencias Aplicadas y Tecnología, el Centro de Investigaciones sobre América Latina y el Caribe, la Facultad de Estudios Superiores Aragón, la Coordinación Universitaria para la Sustentabilidad, el Tribunal Universitario, la Escuela Nacional Preparatoria, Plantel 1 “Gabino Barreda”, la Escuela Nacional de Estudios Superiores, Unidad León, la Dirección General de Administración Escolar y la Oficina de la Abogacía General, y determinar, en consecuencia, si la confirma, modifica o revoca.

TERCERA. De conformidad con lo dispuesto en los artículos 97 de la Ley Federal de Transparencia y Acceso a la Información Pública, así como 33 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, **los titulares de las Áreas Universitarias son responsables de clasificar la información que obre en sus archivos**, debiendo comunicar al Comité mediante oficio, de forma fundada y motivada, esa clasificación.

En tal virtud el Programa Universitario de Estudios del Desarrollo, la Dirección General de Actividades Cinematográficas, la Dirección General de Publicaciones y Fomento Editorial, el Instituto de Ciencias Físicas, la Coordinación de Relaciones y Asuntos Internacionales, el Programa Universitario de Estudios sobre Asia y África, la Dirección General del Patrimonio Universitario, el Consejo Académico del Área de las Humanidades y las Artes, el Instituto de Astronomía, la Escuela Nacional Preparatoria, Planteles 9 “Pedro de Alba”, 2 “Erasmus Castellanos Quinto” y 7 “Ezequiel A. Chávez”, la Unidad Coordinadora de Servicios de Apoyo Administrativo a los Consejos Académicos de Área, la Facultad de Estudios Superiores Iztacala, la Facultad de Medicina Veterinaria y Zootecnia, la Coordinación de Vinculación con el Consejo Universitario, la Secretaría Administrativa, el Instituto de Investigaciones Estéticas, el Centro de Investigaciones Interdisciplinarias en Ciencias y Humanidades, el Programa Universitario de Bioética, la Dirección General de Bibliotecas y Servicios Digitales de Información, el Centro de Enseñanza para Extranjeros, el Instituto de Ciencias Aplicadas y Tecnología, el Centro de Investigaciones sobre América Latina y el Caribe, la Facultad de Estudios Superiores Aragón, la Coordinación Universitaria para la Sustentabilidad, el Tribunal Universitario, la Escuela Nacional Preparatoria, Plantel 1 “Gabino Barreda”, la Escuela Nacional de Estudios Superiores, Unidad León, la Dirección General de Administración Escolar y la Oficina de la Abogacía General, clasificaron como información reservada, por un periodo de **cinco años**, la relativa al **Análisis de Riesgo**, al **Análisis de Brecha** y al **Plan de Trabajo**, conforme a lo expuesto en el antecedente VII de la presente resolución, por actualizarse el supuesto establecido en los artículos 113, fracción VII y 110, fracción VII de las Leyes General y Federal de Transparencia y Acceso a la Información Pública, respectivamente.

Ahora bien, los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, establecen lo siguiente:

“... Como información reservada podrá clasificarse aquella cuya publicación:



COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/528/2022

[...]

VII. Obstruya la prevención o persecución de los delitos;

[...]”.

En correlación con los artículos antes mencionados, el numeral Vigésimo Sexto de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas, establece los parámetros para la procedencia de la causal de reserva prevista en el artículo 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública:

“Vigésimo sexto. De conformidad con el artículo 113, fracción VII de la Ley General, podrá considerarse como información reservada, **aquella que obstruya la prevención de delitos al obstaculizar las acciones implementadas por las autoridades para evitar su comisión, o menoscabar o limitar la capacidad de las autoridades para evitar la comisión de delitos.**

...”.

Énfasis añadido.

De lo anterior se desprende, entre otras cuestiones, que podrá clasificarse como reservada aquella información que obstruya la prevención de delitos, ya sea por obstaculizar las acciones implementadas para evitar la comisión de los mismos, o bien, por menoscabar o limitar la capacidad para evitarlos.

Al respecto, cabe tener en consideración lo establecido en el documento de trabajo del 12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal de la Organización de las Naciones Unidas, en el cual se define la prevención del delito de la siguiente manera: “*La prevención del delito engloba toda la labor realizada para reducir el riesgo de que se cometan delitos y sus efectos perjudiciales en las personas y la sociedad...*”.

Por otro lado, las Directrices para la prevención del delito de la Organización de las Naciones Unidas enumeran tres enfoques, a saber, la prevención social, la prevención basada en la comunidad y la prevención de situaciones propicias al delito; este último tiene por objeto reducir las oportunidades y los incentivos para delinquir, maximizar el riesgo de ser aprehendido y reducir al mínimo los beneficios del delito. En este sentido, el enfoque de prevención de situaciones está orientada en formas específicas de delincuencia.

Desde el punto de vista criminológico, prevenir es conocer con anticipación la probabilidad de una conducta criminal disponiendo de los medios necesarios para evitarla. Es decir, no permitir que alguna situación llegue a darse cuando ésta se estima inconveniente.



COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/528/2022

Ahora bien, cabe destacar que conforme a las Directrices de la Organización para la Cooperación y el Desarrollo Económico, sobre protección de la privacidad y flujos transfronterizos de datos personales, los sectores público y privado, como principio básico, deben emplear salvaguardas razonables de seguridad para proteger los datos personales contra riesgos, tales como pérdida, acceso no autorizado, destrucción, uso, modificación o divulgación de los mismos; asimismo, se establece el principio de responsabilidad que recae sobre todo controlador de datos y su deber en el cumplimiento de las medidas que hagan efectivos los principios señalados anteriormente.

Asimismo, el artículo 7 del Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal, adoptado en Estrasburgo, Francia, el 28 de enero de 1981, publicado mediante Decreto de fecha 28 de septiembre de 2018 en el Diario Oficial de la Federación, establece que los Estados miembros deberán tomar medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados.

Por su parte, el artículo 30, fracción V de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, dispone como uno de los mecanismos que deberá adoptar el responsable para cumplir con el principio de responsabilidad establecido en dicha Ley General, contar con un sistema de supervisión y vigilancia, interna y/o externa, incluidas auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales.

De igual forma, de conformidad con el artículo 33, fracción VII de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, para establecer y mantener las medidas de seguridad para la protección de los datos personales, el Sujeto Obligado deberá monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales, para lo cual en términos del numeral 63 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, el responsable deberá monitorear, entre otras cuestiones, lo siguiente:

- Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas;
- La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;
- Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;
- El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo, y
- Los incidentes y vulneraciones de seguridad ocurridas.

De conformidad con lo anterior, con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, para establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y



COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/528/2022

disponibilidad, el responsable deberá monitorear y revisar de manera periódica dichas medidas, donde no podrá pasar inadvertidas las nuevas amenazas, las posibles vulnerabilidades, los riesgos en conjunto, los incidentes y las vulneraciones de seguridad ocurridas, entre otras.

En ese sentido, el artículo 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, establece que los sujetos obligados deben elaborar un documento de seguridad, entendiéndose como tal, el instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

Ahora bien, de conformidad con los artículos 33 y 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, en relación con los numerales 55 al 64 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, el documento de seguridad deberá contener, cuando menos, el inventario de datos personales y de los sistemas de tratamiento; las funciones y obligaciones de las personas que traten datos personales; **el análisis de riesgos, el análisis de brecha, el plan de trabajo**, los mecanismos de monitoreo y revisión de las medidas de seguridad y el programa general de capacitación. Dicho documento deberá actualizarse cuando se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio de nivel de riesgo; como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión; como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida; así como con la implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

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

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

Por ende, de difundirse la información contenida en los apartados relativos al **Análisis de Riesgos, al Análisis de Brecha, al Plan de Trabajo**, así como a **toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados o que revele vulnerabilidades en la protección de los datos personales en poder de las Áreas Universitarias**, se haría del conocimiento público la falta o debilidad de seguridad en un activo o grupo de activos, físicos o electrónicos, que puede ser explotada por una o más amenazas, lo que conllevaría a la materialización de las mismas y ocasionar la pérdida, destrucción no autorizada o



COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/528/2022

incluso la sustracción de los datos personales en posesión de la Universidad, así como el robo, extravío o copia no autorizada de los mismos, su uso, acceso o tratamiento no autorizado, además del daño, alteración o modificación no autorizada, incluso impidiendo su recuperación, vulnerando así la seguridad de los datos personales.

Bajo estos argumentos se advierte que la clasificación de la información contenida en el **Análisis de Riesgos**, en el **Análisis de Brecha**, en **Plan de Trabajo**, así como de **toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados o que revele vulnerabilidades en la protección de los datos personales en poder de las Áreas Universitarias**, tiene como propósito evitar o prevenir la comisión de conductas ilícitas, tales como el acceso ilícito a equipos y sistema de informática, la cual se encuentra prevista en el Título Noveno, Revelación de Secretos y Acceso Ilícito a sistemas y equipos de informática, Capítulo II, Acceso Ilícito a sistemas y equipos de informática, del Código Penal Federal en el cual se dispone lo siguiente:

“Artículo 211 bis 1.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa”.

“Artículo 211 bis 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

...”

De la normativa señalada se advierte que comete el **delito de acceso ilícito a sistemas y equipos de informática** todo aquel que **sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, sean o no propiedad del Estado**, o bien, conozca o copie dicha información; conductas que de igual manera se pueden materializar en los archivos físicos, ya que es factible **sustraer, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente, los datos personales contenidos en los documentos bajo custodia de las Áreas Universitarias**, por lo que la misma protección deberá otorgarse a los sistemas electrónicos, así como a los archivos físicos con los que se cuenta.



COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/528/2022

Por lo que de darse a conocer la información relativa al **Análisis de Riesgos**, al **Análisis de Brecha**, al **Plan de Trabajo**, así como a **toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados o revele vulnerabilidades en la protección de los datos personales en poder de las Áreas Universitarias**, la cual se encuentra contenida en los documentos de seguridad remitidos por las Áreas Universitarias, se darían a conocer las acciones implementadas o por implementar, de acuerdo con el análisis de riesgos y de brecha, priorizando las medidas de seguridad más relevantes e inmediatas a establecer, así como las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser: hardware, software, personal del responsable, manejo de documentos físicos y/o electrónicos, entre otros, lo que representa para las Áreas Universitarias un riesgo evidente para la estabilidad de la ejecución de las medidas de seguridad adoptadas para resguardar los datos en su poder, en tanto la publicación de esa información revelaría elementos que de manera concatenada con otra información que pudiera generarse o que se haya generado, evidenciaría vulnerabilidades que pudieran ser aprovechadas por personas dedicadas a la comisión de conductas ilícitas y con ello poner en riesgo la seguridad de los datos personales tratados en el desempeño y/o ejercicio de sus competencias, facultades y/o funciones.

De esta forma, se colige que con la publicidad de la información referida, se generaría un riesgo potencial tanto para la documentación física como para la infraestructura tecnológica de las Áreas Universitarias, ya que la información relativa a las medidas físicas, administrativas y técnicas puede ser utilizada para propiciar, entre otros, actos vandálicos, o bien, ataques informáticos de diversa índole, al hacerse identificables las vulnerabilidades que pueden ser explotadas y causar un daño a los documentos físicos y/o electrónicos que obran en los archivos, así como a la infraestructura informática, programas y desarrollos tecnológicos de las Áreas Universitarias, lo que limitaría severamente su capacidad para prevenir conductas ilícitas, tales como las relacionadas en párrafos anteriores.

Por lo anterior, se concluye que la información solicitada actualiza la causal de reserva prevista en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, así como en el numeral Vigésimo Sexto de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas.

Así, en términos del artículo 104 de la Ley General de Transparencia y Acceso a la Información Pública, se analiza la siguiente prueba de daño:

“Artículo 104. En la aplicación de la prueba de daño, el sujeto obligado deberá justificar que:

I. La divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público o a la seguridad nacional;



COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/528/2022

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

III. La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio”.

I. La divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público.

De difundirse la información contenida en el **análisis de riesgos**, en el **análisis de brecha** y en el **plan de trabajo**, así como **toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados o revele vulnerabilidades en la protección de los datos personales en poder de las Áreas Universitarias**, representa un riesgo potencial para las Áreas Universitarias, pues a través de dicha información se podrían identificar vulnerabilidades que pueden ser aprovechadas para realizar conductas contrarias a derecho, tales como actos vandálicos, o bien, ataques informáticos de diversa índole, disminuyendo la capacidad de las Áreas Universitarias para responder ante posibles amenazas.

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

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

El perjuicio que en su caso ocasionaría al interés público la divulgación de la información en cuestión, supera al perjuicio que se ocasionaría al no publicarla, pues con la difusión de la información contenida en el **análisis de riesgos**, en el **análisis de brecha** y en el **plan de trabajo**, así como **toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados o revele vulnerabilidades en la protección de los datos personales en poder de las Áreas Universitarias**, se limitaría la capacidad de las Áreas Universitarias para prevenir la comisión de conductas ilícitas.

De ahí resulta evidente que el riesgo de perjuicio que supondría la divulgación de la información solicitada, supera el interés público general de que se difunda.

III. La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio.

Se considera que la limitación de acceso a la información solicitada se ajusta al principio de proporcionalidad, toda vez que se justifica negar su acceso, a cambio de garantizar la capacidad de las Áreas Universitarias para implementar todas aquellas medidas y acciones tendientes a reducir el riesgo de que se cometa una conducta ilícita que pudiera vulnerar los datos personales cuyo tratamiento realizan las Áreas Universitarias, en el desempeño y/o ejercicio de sus competencias, facultades o funciones.



COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/528/2022

En ese sentido, se considera que la limitación representa el medio menos restrictivo disponible para evitar el perjuicio ya que únicamente se restringirá el acceso a la información por un periodo de **cinco años**, el cual se computará a partir de la fecha en que se emite la presente resolución y hasta la fecha de término del periodo, o bien, se interrumpirá antes si desaparecen las causas que originaron la reserva de la información, lo que suceda primero. De tal forma que no se afecte la capacidad de este sujeto obligado para prevenir la comisión de conductas ilícitas, pero tampoco se prive de manera trascendente el acceso a la información, en su momento, ya que éste no se verá restringido por un periodo mayor al previsto por la norma.

Por lo antes mencionado, se colman las hipótesis de las fracciones I, II y III, dispuestas en el artículo 104 de la Ley General de Transparencia y Acceso a la Información Pública, por lo que es procedente **CONFIRMAR** la reserva total de una parte de la información para la elaboración de la versión pública propuesta por el **Programa Universitario de Estudios del Desarrollo**, la **Dirección General de Actividades Cinematográficas**, la **Dirección General de Publicaciones y Fomento Editorial**, el **Instituto de Ciencias Físicas**, la **Coordinación de Relaciones y Asuntos Internacionales**, el **Programa Universitario de Estudios sobre Asia y África**, la **Dirección General del Patrimonio Universitario**, el **Consejo Académico del Área de las Humanidades y las Artes**, el **Instituto de Astronomía**, la **Escuela Nacional Preparatoria, Planteles 9 “Pedro de Alba”, 2 “Erasmus Castellanos Quinto” y 7 “Ezequiel A. Chávez”**, la **Unidad Coordinadora de Servicios de Apoyo Administrativo a los Consejos Académicos de Área**, la **Facultad de Estudios Superiores Iztacala**, la **Facultad de Medicina Veterinaria y Zootecnia**, la **Coordinación de Vinculación con el Consejo Universitario**, la **Secretaría Administrativa**, el **Instituto de Investigaciones Estéticas**, el **Centro de Investigaciones Interdisciplinarias en Ciencias y Humanidades**, el **Programa Universitario de Bioética**, la **Dirección General de Bibliotecas y Servicios Digitales de Información**, el **Centro de Enseñanza para Extranjeros**, el **Instituto de Ciencias Aplicadas y Tecnología**, el **Centro de Investigaciones sobre América Latina y el Caribe**, la **Facultad de Estudios Superiores Aragón**, la **Coordinación Universitaria para la Sustentabilidad**, el **Tribunal Universitario**, la **Escuela Nacional Preparatoria, Plantel 1 “Gabino Barreda”**, la **Escuela Nacional de Estudios Superiores, Unidad León**, la **Dirección General de Administración Escolar** y por la **Oficina de la Abogacía General**, por un periodo de **cinco años**, que se computarán a partir de la fecha de la presente resolución, de conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

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

- Deberán testar las secciones o información correspondientes al “Análisis de Riesgo”, al “Análisis de Brecha”, al “Plan de Trabajo”, así como toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados o revele vulnerabilidades en la protección de los datos personales en su poder; para lo cual deberán emplear un medio que no permita la visualización de la misma y que no impida la



COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/528/2022

lectura de aquella información que no es considerada como reservada. Al respecto, es importante precisar que **no deberán suprimirse las secciones** donde se contenga la información objeto de reserva.

- Deberán insertar un cuadro de texto en el cual se indiquen:
 - Las partes o secciones reservadas.
 - El fundamento legal que sustenta la reserva, así como el plazo de ésta, mismos que se encuentran indicados en el último párrafo de la consideración **TERCERA** de la presente resolución.

Lo anterior, de conformidad con lo dispuesto en los numerales Quincuagésimo Noveno, Sexagésimo y Sexagésimo Primero de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas.

Por lo expuesto, y con fundamento en lo dispuesto por los artículos 6, apartado A de la Constitución Política de los Estados Unidos Mexicanos; 1, 6, 7, 8, 23, 44, fracción II, 113, fracción VII, 137 inciso a) de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, 110, fracción VII, y 140, fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública; 1, 15, fracción X, 38, último párrafo del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, este Comité de Transparencia:

RESUELVE

PRIMERO. Con fundamento en lo dispuesto en los artículos 1, 10, 11, 15 fracción X y 31, fracción I del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, 137, inciso a) de la Ley General de Transparencia y Acceso a la Información Pública y 140, fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública, este Comité de Transparencia **CONFIRMA** la **CLASIFICACIÓN** de **RESERVA** total de una parte la información para la elaboración de la versión pública de los Documentos de Seguridad, propuesta por el **Programa Universitario de Estudios del Desarrollo**, la **Dirección General de Actividades Cinematográficas**, la **Dirección General de Publicaciones y Fomento Editorial**, el **Instituto de Ciencias Físicas**, la **Coordinación de Relaciones y Asuntos Internacionales**, el **Programa Universitario de Estudios sobre Asia y África**, la **Dirección General del Patrimonio Universitario**, el **Consejo Académico del Área de las Humanidades y las Artes**, el **Instituto de Astronomía**, la **Escuela Nacional Preparatoria**, **Planteles 9 “Pedro de Alba”, 2 “Erasmus Castellanos Quinto” y 7 “Ezequiel A. Chávez”**, la **Unidad Coordinadora de Servicios de Apoyo Administrativo a los Consejos Académicos de Área**, la **Facultad de Estudios Superiores Iztacala**, la **Facultad de Medicina Veterinaria y Zootecnia**, la **Coordinación de Vinculación con el Consejo Universitario**, la **Secretaría Administrativa**, el **Instituto de Investigaciones Estéticas**, el **Centro de Investigaciones Interdisciplinarias en Ciencias y Humanidades**, el **Programa Universitario de Bioética**, la **Dirección General de Bibliotecas y Servicios Digitales de Información**, el **Centro de**



COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/528/2022

Enseñanza para Extranjeros, el Instituto de Ciencias Aplicadas y Tecnología, el Centro de Investigaciones sobre América Latina y el Caribe, la Facultad de Estudios Superiores Aragón, la Coordinación Universitaria para la Sustentabilidad, el Tribunal Universitario, la Escuela Nacional Preparatoria, Plantel 1 “Gabino Barreda”, la Escuela Nacional de Estudios Superiores, Unidad León, la Dirección General de Administración Escolar y por la Oficina de la Abogacía General, en relación con el Análisis de Riesgos, el Análisis de Brecha y el Plan de Trabajo, así como toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados o revele vulnerabilidades en la protección de los datos personales en poder de las Áreas Universitarias, por un periodo de **cinco años**, contados a partir de la fecha de la presente resolución, o bien, hasta en tanto se extingan las causas que dieron origen a la reserva de la información.

Lo anterior, en términos de la consideración **TERCERA** de la presente resolución.

SEGUNDO. Se instruye a las Áreas Universitarias a efecto de que elaboren la versión pública en términos de lo dispuesto en la consideración **CUARTA**.

TERCERO. Con fundamento en los artículos 45, fracción V y 137, último párrafo de la Ley General de Transparencia y Acceso a la Información Pública: así como 53, fracción VI, inciso c) del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, notifíquese la presente resolución por correo institucional al **Programa Universitario de Estudios del Desarrollo**, a la **Dirección General de Actividades Cinematográficas**, a la **Dirección General de Publicaciones y Fomento Editorial**, al **Instituto de Ciencias Físicas**, a la **Coordinación de Relaciones y Asuntos Internacionales**, al **Programa Universitario de Estudios sobre Asia y África**, a la **Dirección General del Patrimonio Universitario**, al **Consejo Académico del Área de las Humanidades y las Artes**, al **Instituto de Astronomía**, a la **Escuela Nacional Preparatoria, Planteles 9 “Pedro de Alba”, 2 “Erasmus Castellanos Quinto” y 7 “Ezequiel A. Chávez”**, a la **Unidad Coordinadora de Servicios de Apoyo Administrativo a los Consejos Académicos de Área**, a la **Facultad de Estudios Superiores Iztacala**, a la **Facultad de Medicina Veterinaria y Zootecnia**, a la **Coordinación de Vinculación con el Consejo Universitario**, a la **Secretaría Administrativa**, al **Instituto de Investigaciones Estéticas**, al **Centro de Investigaciones Interdisciplinarias en Ciencias y Humanidades**, al **Programa Universitario de Bioética**, a la **Dirección General de Bibliotecas y Servicios Digitales de Información**, al **Centro de Enseñanza para Extranjeros**, al **Instituto de Ciencias Aplicadas y Tecnología**, al **Centro de Investigaciones sobre América Latina y el Caribe**, a la **Facultad de Estudios Superiores Aragón**, a la **Coordinación Universitaria para la Sustentabilidad**, al **Tribunal Universitario**, a la **Escuela Nacional Preparatoria, Plantel 1 “Gabino Barreda”**, a la **Escuela Nacional de Estudios Superiores, Unidad León**, a la **Dirección General de Administración Escolar**, a la **Oficina de la Abogacía General**, así como a la **Unidad de Transparencia** de esta Universidad, para los efectos procedentes.



COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/528/2022

Así lo resolvió por unanimidad de votos de sus integrantes, el Comité de Transparencia de la Universidad Nacional Autónoma de México, en términos de los artículos 1, 11, 15, 20 y 53, fracción VI del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

**POR MI RAZA HABLARÁ EL ESPÍRITU”
Ciudad Universitaria, Cd. Mx., 24 de agosto de 2022**

Archivo	02-ctunam-528-2022-docto-seg-3.pdf		
Identificador único (hash)	07de6833b5dddfbc06d59dfe05ffc9ae1d6e0e12f253c84b4590303ce195d20cd		
Fecha y hora de cierre	24/08/2022 19:14:44	Fecha y hora de emisión	24/08/2022 19:35:48
Número de páginas	18	Firmantes	5



Firmantes

Nombre	Lic. MARIA ELENA GARCIA MELENDEZ	Fecha y hora de firma	24/08/2022 16:01:41
Directora General para la Prevención y Mejora de la Gestión Institucional y Suplente del Contralor			
Hash Firma	a5b9499d7fd52fa3c184565d34d68700d725eea53a83224d5cb7a84fc5e3e39e1d35df5ae8294a7d46ae8e8b731e1394		

Nombre	Dra. Guadalupe Barrena Nájera	Fecha y hora de firma	24/08/2022 16:36:33
Titular de la Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género			
Hash Firma	730f1857908c13c686920a2766995f4f29d88309feb74c45dcb8753ce300799dd8962ec4863776556b971bd808c63e3f		

Nombre	Ing. Ricardo Ramírez Ortiz	Fecha y hora de firma	24/08/2022 15:52:42
Director General de Servicios Generales y Movilidad			
Hash Firma	d56f4af1a2aa91be862c6200037618c973a7a494330be4015b65e14ba73b7f814dd8e8c370d1f428753896438442afcd		

Nombre	JOSE MELJEM MOCTEZUMA	Fecha y hora de firma	24/08/2022 17:57:01
Titular de la Unidad de Transparencia			
Hash Firma	ee57713fb4e324026815ba61dec8c010cbbe4089ba52a484dff0d1953af31654d371b4b621a363f2c110c521fe492397		

Nombre	Dra. Jacqueline Peschard Mariscal	Fecha y hora de firma	24/08/2022 19:14:44
Especialista			
Hash Firma	6c01e40a8ac66d63d19efa430d0cc5a32750a74bd853ee40d2d3d8571a5c6ed4e483274029997b22c3c45cd4ba2dc82c		

ANEXO II. FORMATO UNIVERSITARIO DE “SOLICITUD DE EJERCICIO DE DERECHOS ARCO”



Formato de solicitud de ejercicio de derechos Acceso, Rectificación, Cancelación y Oposición (ARCO)

Con fundamento en el artículo 54 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, esta área universitaria le solicita llenar el presente formato para ejercer sus derechos de Acceso, Rectificación, Cancelación y Oposición.

1. Datos del Área Universitaria de la UNAM responsable de tratar los datos personales*:

2. Datos del Titular de los Datos Personales*:

Primer apellido:	Segundo apellido:	Nombre(s):
CURP (para evitar homónimos):		

3. Datos del solicitante:

Primer apellido:	Segundo apellido:	Nombre(s):
Indicar si los datos corresponden a:		
☐ Titular		
☐ Menor de edad		
☐ Persona que se encuentren en estado de interdicción o incapacidad establecida por ley.		
☐ Fallecida		
Datos de identidad y representación legal (opcional, solo si usted no es el titular de los datos personales)		
☐ Persona física:		
☐ Nombre completo del representante:		
☐ Representación de un menor de edad:		
☐ Representación de una persona que se encuentren en estado de interdicción o incapacidad establecida por ley.		
☐ Persona moral:		
☐ Nombre o razón social del representante:		
Registro Federal de Contribuyentes (RFC):		
Documento con el que acredita la representación:		
☐ Poder notarial		
☐ Carta poder simple signada ante dos testigos (con copia de los documentos que acrediten la identidad de los testigos y titular)		
☐ Declaración en comparecencia del Titular (en las instalaciones del área universitaria).		

4. Documento oficial de identificación del titular o solicitante (sólo originales) *:

☐ Credencial para votar (INE)	☐ Pasaporte	☐ Licencia de conducir
☐ Cédula profesional	☐ Cartilla del Servicio militar nacional	☐ Documento migratorio
☐ Acta de nacimiento	☐ Acta de defunción	☐ Otra identificación con fotografía (especifique):

5. Medio por el cual prefiere que le sea notificada la puesta a disposición de la respuesta*:

☐ Acudir al área universitaria donde presentó este formato	☐ Correo electrónico (especificar):
---	--

6. Modalidad en la cual prefiere le sean entregados los datos, en caso de ser procedente. *

☐ Copia simple	☐ Correo electrónico
☐ Copia certificada	☐ Otro medio electrónico como USB/CD ROOM/ DVD (previo depósito de ficha de pago):
☐ Consultas directas	☐ Yo proporciono el medio magnético o electrónico para reproducir los datos personales.

7. Tipo de solicitud de ejercicio de Derechos Acceso, Rectificación, Cancelación y Oposición (ARCO) a datos personales*:

☐ ACCESO

Describir la información datos personales que obran en posesión del área universitaria y a los que requiere tener acceso*:

Señalar el nombre y ubicación del archivo o registro de datos personales*: _____ _____ _____
RECTIFICACIÓN
☐ Son inexactos.
☐ Son incompletos.
☐ Requieren ser actualizados
Justificación y documentación original que acompaña para motivar su petición*: _____ _____
CANCELACIÓN (supresión o eliminación)
Causas que motivan la cancelación*: _____
OPOSICIÓN (cese del tratamiento)
Causas que motivan la oposición (daño o perjuicio que le causa la persistencia del tratamiento de sus datos)*: _____
Señalar si es para una finalidad específica o para todos los sistemas de información que obren en el área universitaria*. _____
Documentación original que acompaña para motivar su petición*: _____
Señalar la referencia o documento que facilite la localización de sus datos personales*
_____ _____

Leí el Aviso de privacidad del área universitaria a la que acudo y en este acto otorgo el consentimiento para que mis datos personales sean tratados conforme al mismo.

Firma o huella dactilar*

Plazos y procedimiento para la atención de las solicitudes de ejercicio de derechos ARCO:

Una vez que se presentó la solicitud, esta área universitaria cuenta con:

- Un plazo de 20 días hábiles, contados a partir del día siguiente a la recepción de la solicitud, para informarle si procede o no el ejercicio del derecho solicitado.
- Un plazo de 15 días hábiles, contados a partir del día siguiente en el que le haya notificado la respuesta anterior, en caso de que haya procedido el ejercicio del derecho, deberá llevar a cabo las acciones necesarias para hacerlo efectivo.

El ejercicio de los derechos ARCO será sencillo y gratuito, siempre que no rebase las 20 hojas simples, por lo que las áreas universitarias realizarán el cobro del costo de reproducción de acuerdo con los Lineamientos para la determinación de los costos de reproducción y envío en el marco de solicitudes de acceso a Información y entrega de datos personales en la Universidad Nacional Autónoma de México.

ANEXO III. CARTA DE CONFIDENCIALIDAD



Carta compromiso de confidencialidad, no divulgación, reserva y resguardo de información y datos personales

(Este documento debe firmarse por todas aquellas personas que por su empleo, cargo o comisión en la Universidad reciban y traten información confidencial de otras personas)

CIUDAD DE _____, A (DD-MM-AAAA)

(Nombre completo), (cargo), adscrita(o) *(dependencia/entidad de adscripción)* de la Universidad Nacional Autónoma de México (en adelante la UNAM) acepto los términos y condiciones, que se describen más adelante, de resguardo, reserva, custodia y protección de la seguridad y confidencialidad de la información, datos personales y de todo tipo de documentos propiedad de la UNAM de los que tenga conocimiento, con motivo de las funciones que desempeño en la Universidad.

El presente compromiso me responsabiliza respecto de la información que me sea proporcionada por la UNAM, ya sea de forma oral, escrita, impresa, sonora, visual, electrónica, informática u holográfica, contenida en cualquier tipo de documento, que puede consistir en: expedientes, reportes, estudios, actas, resoluciones, oficios, correspondencia, acuerdos, directivas, directrices, circulares, contratos, convenios, instructivos, notas, memorandos, estadísticas, o bien, cualquier otro registro en medio conocido o por conocer que documente el ejercicio de las facultades, funciones y competencias del área universitaria y de los servidores universitarios, sin importar su fuente o fecha de elaboración.

La información que me sea proporcionada podría ser considerada, según el caso, como reservada, privilegiada y confidencial, en los términos de las leyes aplicables, por lo que me obligo a protegerla, reservarla, resguardarla y no divulgarla, utilizándola única y exclusivamente para llevar a cabo y cumplir con las actividades y obligaciones que expresamente me sean conferidas por la Universidad.

Es mi responsabilidad no reproducir, hacer pública o divulgar a terceros la información objeto de la presente Carta, y de cumplir con las medidas de seguridad adecuadas al tipo de documento con el que se trabaje.

Mi obligación de confidencialidad no es aplicable en los siguientes casos:

- a) Cuando la información se encuentre en el dominio público en el momento en que me sea suministrada o, una vez suministrada, ésta se haga pública.
- b) Cuando la legislación vigente o un mandato judicial exija su divulgación.
- c) Cuando la información se desarrolle o reciba legítimamente de terceros, de forma totalmente independiente a mi relación con la Universidad.

A t e n t a m e n t e

Firma o huella dactilar

ANEXO IV. RUTA CRÍTICA PARA CUMPLIMIENTO DE LAS MEDIDAS DE SEGURIDAD TÉCNICAS (MST)

A continuación, se presentan los requisitos técnicos para sistemas de información, descritos en las MST del capítulo II de las Normas Complementarias, por orden de prioridad, esto es: de los mínimos indispensables para asegurar los datos personales hasta los necesarios para incrementar la protección de dichos datos.

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 esta guía 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) **Etapas 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) **Etapas 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) **Etapas 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.

Instrucciones

- Para cada MST se ha diseñado un formato, el cual está numerado en correspondencia con la ruta crítica de cumplimiento.
- Se deberán completar todos los formatos aplicables por cada uno de los sistemas de información a cargo del Área Universitaria.
- Todos los formatos deberán integrar el anexo del documento de seguridad de datos personales.
- En el caso de los sistemas que estén en desarrollo al momento de la publicación de las Normas complementarias, deberán cumplir con el 100% de las MST, previo a su publicación como sistema en producción.
- Es requisito indispensable el cumplimiento de las MST para conservar el registro dominio institucional **.unam.mx** en el caso de servicios Web.

Núm. formato	Etapas	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
ETAPA 1			
Anexo I, numerales 1 y 2	1	Un día hábil	Generar el inventario de sistemas de tratamiento de datos personales y la Estructura de descripción de los sistemas de tratamiento de datos personales.
			A) Integrar la información correspondiente a todos los sistemas que dan tratamiento de datos personales en el área universitaria. B) Llenar formatos y colocar nombre y firma de quien realizó la acción.

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
1	1	Un día hábil	Artículo 18. I. c) Utilizar datos no personales durante el desarrollo y pruebas de los sistemas.
			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 1 con nombre y firma de quien realizó la acción, fecha de inicio y de conclusión.
2	1	Un día hábil	Artículo 18. I. e) Asignar o revocar los privilegios de acceso para los usuarios teniendo como base el principio del menor privilegio.
			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 2 con nombre y firma de quien realizó la acción, fecha de inicio y de conclusión.
3	1	Tres días hábiles	Artículo 18. I. g) Instalar y mantener vigentes certificados de comunicación segura SSL en el caso de servicios basados en Web.
			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. E) Llenar formato 3 y colocar nombre y firma de quien realizó la acción.
4	1	Dos días hábiles	Artículo 18. I. h) Definir el plan de respaldos de la información, incluyendo periodicidad y alcance.
			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.

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			- 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: <i>Recovery Time Objective</i>. Tiempo objetivo de recuperación. - RPO: <i>Recovery Point Objective</i>: Punto objetivo de recuperación. D) Concluir este documento, adjuntarlo a SGDP, llenar formato 4 y colocar nombre y firma de quien realizó la acción.
5	1	Un día hábil	Artículo 18. I. i) Definir el procedimiento para el borrado seguro.
			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 SGDP, llenar formato 5 y colocar nombre y firma de quien realizó la acción.
6	1	Un día hábil	Artículo 18. II. a) Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM
			A) Realizar la verificación y configuración con privilegio de administrador del sistema operativo. B) En función del sistema operativo, acceder a la configuración de servidor de tiempo (NTP) en interfaz gráfica o por medio de línea de comandos. <u>Por ejemplo</u>, en el caso del sistema operativo Linux: - Verificar la existencia del archivo <code>/etc/ntp.conf</code> - Editar el archivo <code>ntp.conf</code> incluyendo en la primera línea: <code>server ntpdgctic.redunam.unam.mx ó</code> <code>server 132.247.169.17</code> - Reiniciar el demonio del cliente NTP con el comando <code>sudo service ntp reload</code>. 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 formato 6 y colocar nombre y firma de quien realizó la acción.
7	1	Dos días hábiles	Artículo 18. II. b) Instalar y mantener actualizado el software antimalware.
			A) En función del sistema operativo, instalar uno o varios programas para la contención de malware. <u>Por ejemplo</u>, para el caso del sistema operativo Linux existen herramientas de

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			código abierto y uso libre como <i>chkrootkit</i>, <i>rootkit hunter</i>, <i>bothunter</i>, <i>clamAV</i>, <i>avast</i>, 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. <u>Por ejemplo</u>, para el caso de Linux, se recomienda usar el comando <i>grep</i> para la detección de cadenas regulares de texto en las invocaciones al <i>shell</i>. C) Una vez instalada la solución, verificar periódicamente su actualización. D) Llenar formato 7 y colocar nombre y firma de quien realizó la acción.
8	1	Cuatro días hábiles	Artículo 18. II. c) Instalar las actualizaciones de seguridad más recientes disponibles. A) En función del sistema operativo, se debe revisar la vigencia y actualización de las herramientas de seguridad de la información. <u>Por ejemplo</u>, en el sistema operativo Linux ejecutar <i>apt-get update</i> para obtener la lista de actualizaciones, especialmente en el repositorio <i>security</i> 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 formato 8 y colocar nombre y firma de quien realizó la acción.
			Artículo 19. I. a) Aplicar un mecanismo de autenticación para las personas autorizadas con base en el principio del menor privilegio. 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. <u>Por ejemplo</u>: 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 formato 9 y colocar nombre y firma de quien realizó la acción.
10	1	Dos días hábiles	Artículo 19. II. b) Evitar la instalación de cualquier elemento de software que implique algún riesgo para el tratamiento de datos personales. A) Dependiendo del sistema operativo, configurar las actualizaciones solamente para versiones maduras o revisiones certificadas de las aplicaciones. <u>Por ejemplo</u>: en sistemas Linux desactivar la instalación de versiones <i>beta</i>, <i>test</i>, <i>debug</i>, <i>non-official</i>. B) De la lista de software instalado, verificar el consumo de recursos de aplicaciones <i>TSR (Terminal and Stay Resident)</i>. Identificar demonios que ocupen excesiva RAM o tiempo de

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			ejecución en el procesador. <i>Por ejemplo:</i> 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. <i>Por ejemplo,</i> si el servidor Linux no proporcionará direcciones IP, el demonio o servicio <i>dchpd</i> no debe estar instalado. D) Llenar formato 10 y colocar nombre y firma de quien realizó la acción.
11	1	Dos días hábiles	Artículo 19. III. a) Establecer las medidas físicas de seguridad que controlen el acceso a los equipos. 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. <i>Por ejemplo;</i> 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 formato 11 y colocar nombre y firma de quien realizó la acción.
			Artículo 19. III. b) Restringir la salida de equipos de las instalaciones de cada área universitaria. 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 12 y colocar nombre y firma de quien realizó la acción.
13	1	Tres días hábiles	Artículo 19. IV. a) Realizar la transmisión de datos personales a través de un canal cifrado. A) Identificar, mediante el administrador de aplicaciones que corresponda al sistema operativo, los protocolos y aplicaciones instalados para comunicación cifrada. <i>Por ejemplo:</i> 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. <i>Por ejemplo,</i> en el caso de requerir ejecutar

Núm. formato	Etap	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			comandos de forma remota en un servidor Linux, instalarlo con el comando <i>apt-get install openssh-server</i> . C) Activar los protocolos de comunicación encriptada en el servidor. <i>Por ejemplo:</i> en Linux con el comando <i>sudo systemctl enable ssh</i> . D) Llenar formato 13 y colocar nombre y firma de quien realizó la acción.
14	1	Tres días hábiles	Artículo 20. Aplicar el procedimiento de borrado seguro que impida la recuperación en las bases de datos y todos sus respaldos.
			A) Realizar una copia integral del sistema de información y colocarla en un servicio temporal. <i>Por ejemplo:</i> máquina virtual o 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. <i>Por ejemplo:</i> en Linux se dispone de <i>shred</i> , <i>wipe</i> , <i>secure-delete</i> , <i>srm</i> , <i>sfill</i> , <i>sswap</i> , <i>sdmem</i> , que se pueden instalar desde el administrador de aplicaciones. D) Llenar formato 14 y colocar nombre y firma de quien realizó la acción.
ETAPA 2			
15	2	Hito	Artículo 18. I. a) Utilizar los datos personales preexistentes que estén disponibles, de acuerdo con sus respectivas políticas de uso y acceso, en bases de datos a cargo de otras áreas universitarias.
			A) Disponer del inventario de datos del sistema de información, esto es: documento con la descripción de tablas, campos, tipo de datos, relaciones y consultas. B) Con el Área Universitaria que esté identificada como la instancia autoritativa en materia de datos personales, comparar el inventario de datos. <i>Por ejemplo:</i> La Dirección General de Administración Escolar es la dependencia autoritativa en materia de datos personales de estudiantes. C) Establecer el acuerdo por escrito para el uso de campos específicos de datos personales de la instancia autoritativa. D) Establecer el mecanismo de comunicación entre el sistema de información y el de la instancia autoritativa. <i>Por ejemplo:</i> <i>Webservices</i> , transferencia <i>SFTP</i> . E) Llenar 15 y colocar nombre y firma de quien realizó la acción.
16	2	Ocho días hábiles	Artículo 18. I. d) Permitir el acceso al código fuente de los sistemas exclusivamente a la administración del sistema y personal para el desarrollo.
			A) Recopilar el código fuente y documentación del sistema de información en todas sus versiones disponibles. B) Depositar en un equipo central de desarrollo todas las versiones de código fuente y su documentación (inventario de datos, manual de administración, manual de programador).

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			C) Establecer control de acceso por usuario y contraseña hacia el equipo central de desarrollo. D) Activar bitácoras de acceso (<i>log</i>) hacia el equipo central de desarrollo. E) Proporcionar las credenciales de acceso al equipo central de desarrollo exclusivamente al personal a cargo de programación y mantenimiento de código y manuales. F) Llenar formato 16 y colocar nombre y firma de quien realizó la acción.
17	2	Cuatro días hábiles	Artículo 19. I. b) Establecer las medidas de seguridad en los periodos de inactividad o mantenimiento. A) Elaborar documento con las medidas necesarias de seguridad para periodos vacacionales, contingencias y ventanas de mantenimiento, incluyendo: control de acceso físico y lógico a los equipos, ejecución de respaldos, sistemas de alta disponibilidad (redundancia). B) Incluir en el documento la descripción de los procedimientos en caso de contingencia por falla de servicio de red, falla de equipo de cómputo, falla lógica en sistema operativo. C) Incluir en el documento el directorio de responsables de cada uno de los puntos a atender: apagado seguro, apagado fortuito, apagado programado, verificación de integridad de información, activación de servicios locales o de respaldo. D) Llenar formato 17 y colocar nombre y firma de quien realizó la acción.
			Artículo 19. I. c) Generar respaldos y aplicar los mecanismos de control y protección para su resguardo. A) De acuerdo con el plan de respaldos establecido, ejecutar la secuencia de respaldos. B) Designar responsables de respaldos y responsables de verificación de respaldos. C) Completar bitácora de control de los respaldos, indicando fecha, hora, tipo de respaldo (integral, total, parcial de registros), ejecutor y revisor del respaldo, ubicación del respaldo, medio y etiqueta. D) Llenar formato 18 y colocar nombre y firma de quien realizó la acción.
18	2	Ocho días hábiles	
19	2	Veinte días hábiles	Artículo 19. I. d) Impedir el uso de cuentas y servicios gestionados por personas físicas para el tratamiento de los datos personales. A) Realizar revisión integral del sistema de información en materia de accesos, cuentas y servicios. <i>Por ejemplo:</i> En caso de consultar vía un <i>Webservice</i> a un sistema autoritativo de datos personales en la DGAE, identificar la cuenta de acceso a ese sistema. B) Determinar si las cuentas de acceso a servicios locales o remotos están bajo el control de la administración del sistema. <i>Por ejemplo:</i> Si la cuenta de acceso a un <i>Webservice</i> – su usuario y contraseña – está bajo el control del administrador del sistema, o si un respaldo que se realiza en un equipo remoto es con una cuenta y contraseña controlada por el administrador del sistema.

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			C) Si las cuentas de acceso a servicios locales o remotos pertenecen a personas del Área Universitaria, cambiarlas por cuentas institucionales dentro del control de la instancia universitaria. <i>Por ejemplo:</i> si la identificación para acceder a un respaldo remoto es del tipo xxx@google.com, deberá cambiarse por una cuenta del tipo xxxx@unam.mx. D) Llenar formato 19 y colocar nombre y firma de quien realizó la acción.
20	2	Cuatro días hábiles	Artículo 19. II. a) Proteger ante manipulaciones indebidas y accesos no autorizados las bitácoras y los dispositivos donde se almacenan. A) Elaborar una lista de las bitácoras relacionadas con el sistema de información, tanto en medio digital como físico. <i>Por ejemplo:</i> En el equipo de cómputo las bitácoras de acceso de usuarios al sistema operativo y al sistema de información (<i>logs</i>), de forma física las bitácoras de acceso al área donde está el equipo de cómputo. B) Junto a la lista elaborar el cronograma de revisión de integridad y respaldo de las bitácoras. <i>Por ejemplo:</i> diario, semanal, mensual. C) Establecer en el documento el procedimiento de resguardo de las bitácoras. <i>Por ejemplo:</i> respaldo y protección de <i>logs</i> en el caso de equipo de cómputo o zonas seguras de almacenamiento de bitácoras en papel, digitalización de registros. D) Llenar formato 20 y colocar nombre y firma de quien realizó la acción.
			Artículo 19. IV. b) Supervisar los controles de seguridad en la red de datos donde opere el sistema para tratamiento de datos personales. A) Identificar los equipos activos de red que permiten la conexión del equipo de cómputo con el sistema de información, incluyendo marca, modelo, versión de software, vigencia de mantenimiento y capacidades de protección de las comunicaciones. B) Determinar las reglas de seguridad físicas (acceso restringido, cuartos de telecomunicaciones) y lógicas (cuentas de acceso, puertos activos, protocolos activos) para el equipo de red. C) Incluir en las acciones para aseguramiento de la red de datos aquellas que sean necesarias en función de los controles actuales. Definir un plan de regularización de la seguridad en caso de ser aplicable. D) Mantener actualizados los equipos activos de red y con un programa de mantenimiento. E) Identificar y en su caso programar la instalación de equipo para seguridad perimetral de la red de datos. D) Llenar formato 21 y colocar nombre y firma de quien realizó la acción.
22	2	Cuatro días hábiles	Artículo 19. IV. c) Proporcionar el acceso exclusivamente desde redes y servicios autorizados. A) Revisar los puertos de comunicación (<i>TCP</i> y <i>UDP</i>) que requiera el sistema de información para su operación. <i>Por</i>

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			<u>ejemplo</u>: para servicios <i>Web</i> los puertos 80 y 8080 son los convencionales. B) Activar en el sistema operativo la herramienta correspondiente para el control de puertos de comunicación. <u>Por ejemplo</u>, en Linux puede tratarse de un <i>firewall</i> a nivel de software o las herramientas que para tal efecto contenga la distribución correspondiente del sistema operativo. C) Dejar activos solamente los puertos necesarios para la operación del sistema. D) Activar el filtrado de la comunicación por direccionamiento IP en caso de ser posible para la operación del sistema. <u>Por ejemplo</u>: Permitir el acceso al puerto de <i>SSH</i> solamente a direcciones IP en una subred de la UNAM (132.248.x.y) o a un grupo de direcciones IP específicas. E) Llenar formato 22 y colocar nombre y firma de quien realizó la acción.
ETAPA 3			
23	3	Veinte días hábiles	Artículo 18. I. b) Contar con entornos para desarrollo, pruebas y operación. A) Instalar y configurar equipos similares en características, preferentemente virtuales, a los equipos donde se instalará el sistema de información en su nueva o actualizada versión. B) Crear un repositorio en un equipo central de desarrollo para el resguardo de códigos, documentación, inventarios de datos y manuales de usuario, administrador y programador. C) Ejecutar las pruebas de nuevas versiones o actualizaciones del sistema de información en el equipo dispuesto para tal efecto. Nunca usar -equipos físicos o virtuales con el sistema actualmente en producción como las plataformas para evaluación de versiones en desarrollo. D) Llenar formato 23 y colocar nombre y firma de quien realizó la acción.
24	3	Veinte días hábiles	Artículo 18. I. f) Cumplir con las especificaciones de seguridad informática previo a la puesta en operación. A) Una vez concluido el desarrollo o actualización de un sistema de información, solicitar al área de seguridad del Área Universitaria la revisión de seguridad informática del sistema, lo que incluye: pruebas de penetración, pruebas de estabilidad, pruebas de carga y endurecimiento de la seguridad. En caso de no contar con esa área, requerirlo a UNAM CERT al correo seguridad.tic@unam.mx. B) Una vez recibido el reporte del área de seguridad, aplicar las medidas de corrección que incluya el reporte. Regresar al punto A. C) Habiendo resuelto los hallazgos y sugerencias de mejora de la seguridad señalados por el área especializada, realizar la instalación del sistema en la plataforma definitiva de cómputo, extrayéndolo del entorno de desarrollo. D) Llenar formato 24 y colocar nombre y firma de quien realizó la acción.
25	3	Hito	Artículo 18. III. a) Utilizar equipos con componentes actualizados, protegidos con garantías y soporte, y con la

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			capacidad suficiente para atender la demanda del servicio y de los usuarios. A) Elaborar una lista del inventario de los equipos de cómputo, periféricos y de almacenamiento necesarios para la ejecución del sistema de información. B) Determinar la razón por la que el sistema de información requerirá estar localizado en un equipo físico y no en un servidor virtual. Con ello justificar una adquisición o actualización. Por ejemplo: por incompatibilidad con hipervisores, necesidades de comunicación exclusivamente locales en la entidad y dependencia o el no necesitar de un entorno de alta disponibilidad automática. C) Identificar en el inventario versiones, introducción en el mercado, vida útil, contratos de mantenimiento y soporte para todos y cada uno de los componentes, en el caso de emplear equipo físico. D) Adquirir los componentes y elementos necesarios para la actualización, vigencia de soporte y capacidad para atención a los usuarios en el equipo de cómputo físico. E) Llenar formato 25 y colocar nombre y firma de quien realizó la acción.
26	3	Hito	Artículo 18. III. b) Definir el programa de mantenimiento preventivo. A) De la lista de equipo de cómputo físico necesario para la operación del sistema de información, extraer las vigencias de mantenimiento. B) En caso de no estar en posibilidad de aplicar el mantenimiento preventivo por el personal del Área Universitaria, cotizar pólizas de mantenimiento de acuerdo con el tipo de componente, preferentemente una sola póliza para el conjunto del equipo físico. C) Adquirir las pólizas de mantenimiento preventivo y observar su vigencia. La vigencia no podrá ser menor de un año. D) Llenar formato 26 y colocar nombre y firma de quien realizó la acción.
27	3	Seis días hábiles	Artículo 19. III. c) Aplicar el programa de mantenimiento preventivo a los equipos. A) En caso de que el personal del Área Universitaria pueda realizar el mantenimiento preventivo, definir el calendario de inactividad del sistema de información, notificar a los usuarios y aplicar el plan en caso de mantenimiento o inactividad. B) En caso de que sea a través de un proveedor que se proporcione el mantenimiento al equipo de cómputo, ejecutar el calendario de acciones preventivas en un período no superior a cada 3 meses hasta la conclusión del contrato o póliza respectivo. C) Llenar formato 27 y colocar nombre y firma de quien realizó la acción.
28	3	Hito	Artículo 21. Solo se permitirá el uso de servicios de nube pública para el resguardo de archivos cifrados que contengan respaldos de la información.

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			A) Identificar los respaldos que se tengan resguardados en servicios de nube pública. B) Verificar el cifrado en cada uno de los respaldos que se almacenen en nube pública. El cifrado no deberá ser de menor capacidad al equivalente a AES de 128 bits. C) Llenar formato 28 y colocar nombre y firma de quien realizó la acción.

ANEXO V. FORMATOS PARA CUMPLIMIENTO DE LAS MST

(Nombre del sistema A1)		Identificador único A1	
Formato	1	Verificación anual	Acción concluida ()
Medida de seguridad técnica:	Artículo 18. I. c) Utilizar datos no personales durante el desarrollo y pruebas de los sistemas.		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Un día hábil.		
Importancia de la acción:	Evitar usar datos personales mientras se está desarrollando, actualizando o modificando el código fuente de un sistema de información.		
Proceso recomendado:	A) Realizar respaldo completo de la base de datos. B) Ejecutar consulta en el sistema de información, por medio de formato o comandos. C) Verificar que los datos usados en el desarrollo no correspondan a personas identificables. D) Si se usan datos de personas identificables, cambiar por datos genéricos o datos ficticios y regresar al punto B. E) Si no se usan datos de personas identificables, llenar formato con nombre y firma de quien realizó la acción, fecha de inicio y de conclusión.		
Mejores prácticas, referencias:	1.- Se recomienda al desarrollar un sistema de información no usar datos personales sino ficticios. 2.- Se sugiere incluir en la documentación del desarrollo de un sistema de información el inventario de datos y el tipo de información de prueba.		
Conocimientos requeridos:	Administración de bases de datos. Consulta y actualización de tablas.		
Ejecución		Fecha inicio	
Nombre y firma		Fecha término	
Programador, desarrollador o diseñador del sistema de información			
Observaciones / anotaciones			

I.

(Nombre del sistema A1)		Identificador único A1	
Formato:	2	Verificación anual	Acción concluida ()
Medidas de seguridad técnicas:	Artículo 18. I. e) Asignar o revocar los privilegios de acceso para los usuarios teniendo como base el principio del menor privilegio.		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Un día hábil.		
Importancia de la acción:	No se deben asignar privilegios de acceso a los usuarios en niveles que no estén relacionados con su responsabilidad en el tratamiento de datos.		
Proceso recomendado:	A) Realizar respaldo completo de la base de datos. B) Ejecutar consulta en el sistema de información de la lista de usuarios y sus niveles o privilegios de acceso. C) Validar que los niveles de acceso son acordes a la relación del usuario con el tratamiento de datos personales.		

	D) Si hay usuarios con privilegios mayores a los que les son necesarios, cambiar al mínimo indispensable e informarlo al usuario. Regresar al punto B. E) Si los privilegios de acceso son correctos para los usuarios, llenar formato con nombre y firma de quien realizó la acción, fecha de inicio y de conclusión.
Mejores prácticas, referencias:	1.- Definir niveles de acceso adecuados para cada perfil o tipo de usuario. 2.- Tener un mínimo de administradores o usuarios con altos privilegios en el sistema.
Conocimientos requeridos:	Administración de bases de datos. Consulta y actualización de usuarios.
Ejecución	
Fecha inicio	
Nombre y firma	
Administrador del sistema de información	
Fecha término	
Observaciones / anotaciones	

(Nombre del sistema A1)			Identificador único A1	
Formato:	3	Verificación anual	Acción concluida	()
Medidas de seguridad técnicas:	Artículo 18. I. g) Instalar y mantener vigentes certificados de comunicación segura SSL en el caso de servicios basados en Web.			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Tres días hábiles.			
Importancia de la acción:	El instalar un certificado SSL en servidores web incrementa la seguridad al encriptar la transferencia de datos y la unicidad del sitio para los usuarios.			
Proceso recomendado:	A) En caso de no tener un certificado SSL vigente, enviar correo electrónico al Departamento de Firma Electrónica de DGTIC a firma.tic@unam.mx solicitando la asignación. B) El Departamento de Firma Electrónica Avanzada envía procedimiento para obtención de CSR del servidor, formato de la solicitud y costos de recuperación en función del tipo de certificado requerido (organizacional, comodín o corporativo). C) Completar documentación, proceso y pago de costo de recuperación. Enviar comprobantes a firma.tic@unam.mx. D) Al recibir el certificado SSL, instalarlo en el servidor de acuerdo con las instrucciones recibidas junto con el certificado.			
Mejores prácticas, referencias:	1.- Los certificados SSL deben tener una vigencia de al menos un año. 2.- En caso de tener varios sistemas de información bajo un mismo dominio, se recomienda obtener un certificado SSL del tipo comodín (<i>wildcard</i>). 3.- Se debe realizar el proceso de renovación del certificado al menos 10 días hábiles antes de su vencimiento.			
Conocimientos requeridos:	Administración de sistema operativo. Administración de servicios Web.			
Ejecución			Fecha inicio	

Nombre y firma Administrador del sistema de información o servidor		Fecha término
Observaciones / anotaciones		

(Nombre del sistema A1)		Identificador único A1	
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: <i>Recovery Time Objective</i>. Tiempo objetivo de recuperación. - RPO: <i>Recovery Point Objective</i>: 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	
Nombre y firma Administrador del sistema de información o servidor		Fecha término	
Observaciones / anotaciones			

(Nombre del sistema A1)		Identificador único A1	
Formato:	5	Verificación anual	Acción concluida ()
Medidas de seguridad técnicas:	Artículo 18. I. i) Definir el procedimiento para el borrado seguro.		

Aplicable en:	I. Bases de datos y sistemas de tratamiento.
Tiempo estimado:	Un día hábil.
Importancia de la acción:	Al igual que el procedimiento de respaldo, el borrado seguro de la información debe estar definido en cualquier sistema de información.
Proceso recomendado:	A) Elaborar documento con el procedimiento y la herramienta para borrado seguro en función del tipo de base de datos para registros, tablas y base de datos. B) Incluir en el documento de borrado seguro el proceso de verificación de la no existencia del dato, generalmente por medio de consultas y de copias de respaldo. C) El borrado seguro debe incluirse en los respaldos incrementales y totales y en cualquiera de los medios de respaldo, así como máquinas virtuales o contenedores. D) Concluir este documento, adjuntarlo a SGDP, 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 <i>DOD-5220.22-M</i>.
Conocimientos requeridos:	Administración de sistema operativo. Comandos de borrado.
Ejecución	
Fecha inicio	
Nombre y firma	
Administrador del sistema de información o servidor	
Fecha término	
Observaciones / anotaciones	

(Nombre del sistema A1)		Identificador único A1	
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. <i>Por ejemplo</i>, en el caso del sistema operativo Linux: - Verificar la existencia del archivo <i>/etc/ntp.conf</i> - Editar el archivo <i>ntp.conf</i> incluyendo en la primera línea: <code>server ntpdgtic.redunam.unam.mx ó</code> <code>server 132.247.169.17</code> - Reiniciar el demonio del cliente NTP con el comando <i>sudo service ntp reload</i>.		

	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	
Nombre y firma	
Administrador del sistema de información o servidor	
Fecha término	
Observaciones / anotaciones	

(Nombre del sistema A1)			Identificador único A1	
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 <i>malware</i> (<i>rootkits</i> , <i>backdoors</i> 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. <u>Por ejemplo</u>, para el caso del sistema operativo Linux existen herramientas de código abierto y uso libre como <i>chkrootkit</i>, <i>rootkit hunter</i>, <i>bothunter</i>, <i>clamAV</i>, <i>avast</i>, 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. <u>Por ejemplo</u>, para el caso de Linux, se recomienda usar el comando <i>grep</i> para la detección de cadenas regulares de texto en las invocaciones al <i>shell</i>. 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 <i>anti malware</i> más adecuadas para el servidor donde se aloje el sistema de información. Contactar al correo seguridad.tic@unam.mx.			
Conocimientos requeridos:	Administración de sistema operativo. Instalación de aplicaciones.			
Ejecución			Fecha inicio	
Nombre y firma			Fecha término	
Administrador del sistema de información o servidor				

Observaciones / anotaciones	
-----------------------------	--

(Nombre del sistema A1)			Identificador único A1	
Formato:	8	Verificación anual	Acción concluida	()
Medidas de seguridad técnicas:		Artículo 18. II. c) Instalar las actualizaciones de seguridad más recientes disponibles.		
Aplicable en:		II. Sistemas operativos y servicios.		
Tiempo estimado:		Cuatro días hábiles.		
Importancia de la acción:		El servidor que hospede el sistema de información debe tener vigentes todas las actualizaciones de seguridad proporcionadas por el fabricante o desarrollador del sistema operativo.		
Proceso recomendado:		A) En función del sistema operativo, se debe revisar la vigencia y actualización de las herramientas de seguridad de la información. <i>Por ejemplo</i> , en el sistema operativo Linux ejecutar <i>apt-get update</i> para obtener la lista de actualizaciones, especialmente en el repositorio <i>security</i> de la respectiva distribución. B) Realizar un respaldo del sistema para garantizar retorno a versión anterior en caso de incompatibilidad con alguna aplicación de las actualizaciones de seguridad. C) Instalar las actualizaciones en el sistema operativo. D) Llenar y firmar formato.		
Mejores prácticas, referencias:		1.- Debe verificarse la actualización de seguridad del sistema operativo al menos una vez a la semana y configurar la actualización o notificación inmediata en caso de complementos de seguridad urgentes.		
Conocimientos requeridos:		Administración de sistema operativo. Instalación de aplicaciones.		
Ejecución			Fecha inicio	
Nombre y firma			Fecha término	
Administrador del sistema de información o servidor				
Observaciones / anotaciones				

(Nombre del sistema A1)		Identificador único A1	
Formato:	9	Verificación anual	Acción concluida ()
Medidas de seguridad técnicas:	Artículo 19. I. a) Aplicar un mecanismo de autenticación para las personas autorizadas con base en el principio del menor privilegio.		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Cuatro días hábiles.		
Importancia de la acción:	Partiendo de la asignación o niveles de acceso a la información con el principio del menor privilegio, debe haber en operación en el sistema al menos un mecanismo para la validación de los usuarios autorizados.		
Proceso recomendado:	A) Verificar el tipo de control de acceso al sistema, esto es: a través de contraseñas, claves, identificadores, nombres de usuario, nombres de dominio, entre otros. Según sea aplicable al sistema de		

	información en lo particular. En caso de no tener un control de acceso establecer al menos uno como: usuarios de sistema operativo, cuenta y contraseña de sistema. B) Revisar que los privilegios de acceso sean los adecuados en función del rol del usuario. <i>Por ejemplo:</i> 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 (<i>Active Directory</i>), <i>LDAP</i> u <i>OpenAIM</i>. 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	
Nombre y firma	
Administrador del sistema de información o servidor	
Observaciones / anotaciones	

(Nombre del sistema A1)		Identificador único A1	
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. <i>Por ejemplo:</i> en sistemas Linux desactivar la instalación de versiones <i>beta</i>, <i>test</i>, <i>debug</i>, <i>non-official</i>. B) De la lista de software instalado, verificar el consumo de recursos de aplicaciones <i>TSR (Terminal and Stay Resident)</i>. Identificar demonios que ocupen excesiva RAM o tiempo de ejecución en el procesador. <i>Por ejemplo:</i> 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. <i>Por ejemplo,</i> si el servidor Linux no proporcionará direcciones IP, el demonio o servicio <i>dchpd</i> 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	
Nombre y firma	
Administrador del sistema de información o servidor	
Observaciones / anotaciones	

(Nombre del sistema A1)			Identificador único A1	
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. <i>Por ejemplo;</i> cámaras de videovigilancia, bitácoras, vigilantes, cuartos cerrados, racks con puerta y chapa, candados en equipos, bloqueo o desconexión física de puertos USB, alarmas y sensores, según sea lo más conveniente como mínimo para la protección de los datos. D) Llenar y firmar formato.			
Mejores prácticas, referencias:	1.- Las medidas físicas de seguridad deben revisarse regularmente y formar parte de plan de continuidad de operaciones, así como ser del conocimiento de la Comisión local de seguridad.			
Conocimientos requeridos:	Administración de bases de datos. Consulta y actualización de usuarios.			
Ejecución			Fecha inicio	
Nombre y firma			Fecha término	
Administrador del sistema de información o servidor				
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
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 <i>flash</i>, 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	
Nombre y firma	
Administrador del sistema de información o servidor	
Observaciones / anotaciones	

(Nombre del sistema A1)			Identificador único A1	
Formato:	13	Verificación anual	Acción concluida	()
Medidas de seguridad técnicas:	Artículo 19. IV. a) Realizar la transmisión de datos personales a través de un canal cifrado.			
Aplicable en:	IV. Red de datos.			
Tiempo estimado:	Tres días hábiles.			
Importancia de la acción:	La comunicación del sistema de información con otros sistemas o servicios, así como el acceso de administración para ejecución de procesos por comandos, debe estar encriptada para evitar el envío o recepción de datos susceptibles de ser interceptados en tránsito.			
Proceso recomendado:	A) Identificar, mediante el administrador de aplicaciones que corresponda al sistema operativo, los protocolos y aplicaciones instalados para comunicación cifrada. <i>Por ejemplo:</i> SFTP (<i>Secure File Transfer Protocol</i>), SSH (<i>Secure Shell</i>), SCP (<i>Secure Copy</i>). 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. <i>Por ejemplo,</i> en el caso de requerir ejecutar comandos de forma remota en un servidor Linux, instalarlo con el comando <i>apt-get install openssh-server</i>. C) Activar los protocolos de comunicación encriptada en el servidor. <i>Por ejemplo:</i> en Linux con el comando <i>sudo systemctl enable ssh</i>.			

	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	
Nombre y firma	
Administrador del sistema de información o servidor	
Observaciones / anotaciones	

(Nombre del sistema A1)			Identificador único A1	
Formato:	14	Verificación anual	Acción concluida	()
Medidas de seguridad técnicas:	Artículo 20. Aplicar el procedimiento de borrado seguro que impida la recuperación en las bases de datos y todos sus respaldos.			
Aplicable en:	Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Tres días hábiles.			
Importancia de la acción:	Se debe verificar que el procedimiento de borrado seguro es funcional y que el dato no persiste en función del tipo de borrado (registro, tabla, base, sistema).			
Proceso recomendado:	A) Realizar una copia integral del sistema de información y colocarla en un servicio temporal. <i>Por ejemplo:</i> 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. <i>Por ejemplo:</i> en Linux se dispone de <i>shred</i> , <i>wipe</i> , <i>secure-delete</i> , <i>srm</i> , <i>sfill</i> , <i>sswap</i> , <i>sdmem</i> , que se pueden instalar desde el administrador de aplicaciones. D) Llenar y firmar este formato.			
Mejores prácticas, referencias:	1.- Se recomienda usar al menos un comando a nivel de sistema operativo para el borrado seguro de conformidad con el procedimiento establecido.			
Conocimientos requeridos:	Administración de sistema operativo. Instalación de aplicaciones. Gestión de archivos.			
Ejecución			Fecha inicio	
Nombre y firma			Fecha término	
Administrador del sistema de información o servidor				
Observaciones / anotaciones				

(Nombre del sistema A1)		Identificador único A1	
Formato:	15	Verificación anual	Acción concluida ()
Medidas de seguridad técnicas	Artículo 18. I. a) Utilizar los datos personales preexistentes que estén disponibles, de acuerdo con sus respectivas políticas de uso y acceso en bases de datos a cargo de otras áreas universitarias.		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Hito.		
Importancia de la acción:	Optimizar y consolidar el uso y la protección de datos personales al hacer referencia a instancias universitarias que sean las principales responsables de su obtención, resguardo y protección.		
Proceso recomendado:	A) Disponer del inventario de datos del sistema de información, esto es: documento con la descripción de tablas, campos, tipo de datos, relaciones y consultas. B) Con la Área Universitaria que esté identificada como la instancia autoritativa en materia de datos personales, comparar el inventario de datos. <i>Por ejemplo:</i> La Dirección General de Administración Escolar es la dependencia autoritativa en materia de datos personales de estudiantes. C) Establecer el acuerdo por escrito para el uso de campos específicos de datos personales de la instancia autoritativa. D) Establecer el mecanismo de comunicación entre el sistema de información y el de la instancia autoritativa. <i>Por ejemplo:</i> Webservices, transferencia SFTP. E) Llenar y firmar formato.		
Mejores prácticas, referencias:	1.- El hacer referencia a instancias a cargo de la obtención de los datos personales y su protección se garantiza la homogeneidad de la información.		
Conocimientos requeridos:	Administración de sistema de información. Gestión de bases de datos.		
Ejecución		Fecha inicio	
Nombre y firma		Fecha término	
Administrador del sistema de información o servidor			
Observaciones / anotaciones			

(Nombre del sistema A1)		Identificador único A1	
Formato:	16	Verificación anual	Acción concluida ()
Medidas de seguridad técnicas:	Artículo 18. I. d) Permitir el acceso al código fuente de los sistemas exclusivamente a la administración del sistema y personal para el desarrollo.		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Ocho días hábiles.		
Importancia de la acción:	Evitar el uso de códigos originales de los sistemas de información que posteriormente implique un riesgo a la seguridad de estos.		
Proceso recomendado:	A) Recopilar el código fuente y documentación del sistema de información en todas sus versiones disponibles. B) Depositar en un equipo central de desarrollo todas las versiones de código fuente y su documentación (inventario de datos, manual de administración, manual de programador).		

	C) Establecer control de acceso por usuario y contraseña hacia el equipo central de desarrollo D) Activar bitácoras de acceso (<i>log</i>) hacia el equipo central de desarrollo. E) Proporcionar las credenciales de acceso al equipo central de desarrollo exclusivamente al personal a cargo de programación y mantenimiento de código y manuales. F) Llenar y firmar formato.
Mejores prácticas, referencias:	1.- Se debe documentar todo el proceso de desarrollo y actualización de un sistema de información.
Conocimientos requeridos:	Administración de sistema de información. Gestión de bases de datos.
Ejecución	
Nombre y firma	
Administrador del sistema de información o servidor	
Observaciones / anotaciones	

(Nombre del sistema A1)			Identificador único A1	
Formato:	17	Verificación anual	Acción concluida	()
Medidas de seguridad técnicas:	Artículo 19. I. b) Establecer las medidas de seguridad en los periodos de inactividad o mantenimiento.			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Cuatro días hábiles.			
Importancia de la acción:	Garantizar la continuidad de la operación y disponibilidad de los sistemas de información especialmente durante períodos vacacionales, contingencias o ciclos de mantenimiento.			
Proceso recomendado:	A) Elaborar documento con las medidas necesarias de seguridad para períodos vacacionales, contingencias y ventanas de mantenimiento, incluyendo: control de acceso físico y lógico a los equipos, ejecución de respaldos, sistemas de alta disponibilidad (redundancia). B) Incluir en el documento la descripción de los procedimientos en caso de contingencia por falla de servicio de red, falla de equipo de cómputo, falla lógica en sistema operativo. C) Incluir en el documento el directorio de responsables de cada uno de los puntos a atender: apagado seguro, apagado fortuito, apagado programado, verificación de integridad de información, activación de servicios locales o de respaldo. D) Llenar y firmar formato.			
Mejores prácticas, referencias:	1.- Las medidas de seguridad durante períodos de mantenimiento deben formar parte de un plan de continuidad de operaciones y de recuperación ante desastres (DRP).			
Conocimientos requeridos:	Administración de sistema de información. Administración de sistema operativo.			
Ejecución			Fecha inicio	
Nombre y firma			Fecha término	
Administrador del sistema de información o servidor				

Observaciones / anotaciones	
-----------------------------	--

(Nombre del sistema A1)		Identificador único A1	
Formato:	18	Verificación anual	Acción concluida ()
Medidas de seguridad técnica:	Artículo 19. I. c) Generar respaldos y aplicar los mecanismos de control y protección para su resguardo.		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Ocho días hábiles.		
Importancia de la acción:	Verificar que el plan de respaldos opera adecuadamente para su utilización en caso de contingencia.		
Proceso recomendado:	A) De acuerdo con el plan de respaldos establecido, ejecutar la secuencia de respaldos. B) Designar responsables de respaldos y responsables de verificación de respaldos. C) Completar bitácora de control de los respaldos, indicando fecha, hora, tipo de respaldo (integral, total, parcial de registros), ejecutor y revisor del respaldo, ubicación del respaldo, medio y etiqueta. D) Llenar y firmar formato.		
Mejores prácticas, referencias:	1.- La generación de respaldos, su control y protección deben formar parte de un plan de continuidad de operaciones y de recuperación ante desastres (DRP).		
Conocimientos requeridos:	Administración de sistema de información. Administración de sistema operativo.		
Ejecución		Fecha inicio	
Nombre y firma		Fecha término	
Administrador del sistema de información o servidor			
Observaciones / anotaciones			

(Nombre del sistema A1)		Identificador único A1	
Formato:	19	Verificación anual	Acción concluida ()
Medidas de seguridad técnicas:	Artículo 19. I. d) Impedir el uso de cuentas y servicios gestionados por personas físicas para el tratamiento de los datos personales.		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Veinte días hábiles.		
Importancia de la acción:	Debe evitarse el riesgo que implica el depender de cuentas de control personal para acceder a servicios, fuentes de información o cualquier elemento del sistema de información que ponga en riesgo su estabilidad y confiabilidad.		
Proceso recomendado:	A) Realizar revisión integral del sistema de información en materia de accesos, cuentas y servicios. <i>Por ejemplo:</i> En caso de consultar vía un <i>Webservice</i> a un sistema autoritativo de datos personales en la DGAE, identificar la cuenta de acceso a ese sistema. B) Determinar si las cuentas de acceso a servicios locales o remotos están bajo el control de la administración del sistema. <i>Por ejemplo:</i> Si la cuenta de acceso a un <i>Webservice</i> – su usuario y contraseña –		

	está bajo el control del administrador del sistema, o si un respaldo que se realiza en un equipo remoto es con una cuenta y contraseña controlada por el administrador del sistema. C) Si las cuentas de acceso a servicios locales o remotos pertenecen a personas del Área Universitaria, cambiarlas por cuentas institucionales dentro del control de la instancia universitaria. <i>Por ejemplo:</i> si la identificación para acceder a un respaldo remoto es del tipo xxx@google.com, deberá cambiarse por una cuenta del tipo xxxx@unam.mx D) Llenar y firmar formato.
Mejores prácticas, referencias:	1.- Nunca deben usarse cuentas, servicios, suscripciones, licencias o cualquier otro elemento informático cuyo control dependa de una sola persona.
Conocimientos requeridos:	Administración de sistema de información. Gestión de bases de datos.
Ejecución	
Fecha inicio	
Nombre y firma	
Administrador del sistema de información o servidor	
Observaciones / anotaciones	

(Nombre del sistema A1)		Identificador único A1	
Formato:	20	Verificación anual	Acción concluida ()
Medidas de seguridad técnicas:	Artículo 19. II. a) Proteger ante manipulaciones indebidas y accesos no autorizados las bitácoras y los dispositivos donde se almacenan.		
Aplicable en:	II. Sistemas operativos.		
Tiempo estimado:	Cuatro días hábiles.		
Importancia de la acción:	Las bitácoras son un elemento esencial para determinar acciones que atentan contra la estabilidad del sistema de información y la protección de los datos personales.		
Proceso recomendado:	A) Elaborar una lista de las bitácoras relacionadas con el sistema de información, tanto en medio digital como físico. <i>Por ejemplo:</i> En el equipo de cómputo las bitácoras de acceso de usuarios al sistema operativo y al sistema de información (<i>logs</i>), de forma física las bitácoras de acceso al área donde está el equipo de cómputo. B) Junto a la lista elaborar el cronograma de revisión de integridad y respaldo de las bitácoras. <i>Por ejemplo:</i> diario, semanal, mensual. C) Establecer en el documento el procedimiento de resguardo de las bitácoras. <i>Por ejemplo:</i> respaldo y protección de <i>logs</i> en el caso de equipo de cómputo o zonas seguras de almacenamiento de bitácoras en papel, digitalización de registros. D) Llenar y firmar formato.		
Mejores prácticas, referencias:	1.- Las bitácoras digitales y en papel deben resguardarse preferentemente en una zona independiente de la ubicación del sistema de información.		
Conocimientos requeridos:	Administración de sistema de información. Administración de sistema operativo.		
Ejecución		Fecha inicio	

Nombre y firma		Fecha término
Administrador del sistema de información o servidor		
Observaciones / anotaciones		

(Nombre del sistema A1)			Identificador único A1	
Formato:	21	Verificación anual	Acción concluida	()
Norma Complementaria Técnica		Artículo 19. IV. b) Supervisar los controles de seguridad en la red de datos donde opere el sistema para tratamiento de datos personales.		
Aplicable en:		IV. Red de datos.		
Tiempo estimado:		Cuatro días hábiles.		
Importancia de la acción:		El control de seguridad de los equipos activos de red que suministran la conectividad al sistema de información es un elemento básico para la protección de los datos.		
Proceso recomendado:		A) Identificar los equipos activos de red que permiten la conexión del equipo de cómputo con el sistema de información, incluyendo marca, modelo, versión de software, vigencia de mantenimiento y capacidades de protección de las comunicaciones. B) Determinar las reglas de seguridad físicas (acceso restringido, cuartos de telecomunicaciones) y lógicas (cuentas de acceso, puertos activos, protocolos activos) para el equipo de red. C) Incluir en las acciones para aseguramiento de la red de datos aquellas que sean necesarias en función de los controles actuales. Definir un plan de regularización de la seguridad en caso de ser aplicable. D) Mantener actualizados los equipos activos de red y con un programa de mantenimiento. E) Identificar y en su caso programar la instalación de equipo para seguridad perimetral de la red de datos. D) Llenar y firmar formato.		
Mejores prácticas, referencias:		1.- Las ubicaciones físicas de los equipos activos de red deben estar protegidas con cerraduras y controles de acceso, cumplir las normas de operación y no emplearse para ningún otro equipo o uso.		
Conocimientos requeridos:		Administración de redes de datos.		
Ejecución			Fecha inicio	
Nombre y firma			Fecha término	
Administrador del sistema de información o servidor				
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	22	Verificación anual	Acción concluida	()
Medidas de seguridad técnicas:	Artículo 19. IV. c) Proporcionar exclusivamente el acceso desde redes y servicios autorizados.			
Aplicable en:	IV. Red de datos.			
Tiempo estimado:	Cuatro días hábiles.			

Importancia de la acción:	Es necesario reducir el mínimo necesario los puertos de comunicación para el funcionamiento del sistema de información.		
Proceso recomendado:	A) Revisar los puertos de comunicación (<i>TCP</i> y <i>UDP</i>) que requiera el sistema de información para su operación. <i>Por ejemplo:</i> para servicios <i>Web</i> los puertos 80 y 8080 son los convencionales. B) Activar en el sistema operativo la herramienta correspondiente para el control de puertos de comunicación. <i>Por ejemplo,</i> en Linux puede tratarse de un <i>firewall</i> a nivel de software o las herramientas que para tal efecto contenga la distribución correspondiente del sistema operativo. C) Dejar activos solamente los puertos necesarios para la operación del sistema. D) Activar el filtrado de la comunicación por direccionamiento IP en caso de ser posible para la operación del sistema. <i>Por ejemplo:</i> Permitir el acceso al puerto de <i>SSH</i> solamente a direcciones IP en una subred de la UNAM (132.248.x.y) o a un grupo de direcciones IP específicas. E) Llenar y firmar formato.		
Mejores prácticas, referencias:	1.- No se deben tener activos accesos que no son necesarios vía la red de datos.		
Conocimientos requeridos:	Administración de sistema de información. Administración de sistema operativo.		
Ejecución		Fecha inicio	
Nombre y firma		Fecha término	
Administrador del sistema de información o servidor			
Observaciones / anotaciones			

(Nombre del sistema A1)		Identificador único A1	
Formato:	23	Verificación anual	Acción concluida ()
Medidas de seguridad técnicas:	Artículo 18. I. b) Contar con entornos para desarrollo, pruebas y operación.		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Veinte días hábiles.		
Importancia de la acción:	Para evitar riesgos innecesarios a la información, el desarrollo y actualización de los mismos deberá ser realizado siempre en una plataforma y ambientes por separado.		
Proceso recomendado:	A) Instalar y configurar equipos similares en características, preferentemente virtuales, a los equipos donde se instalará el sistema de información en su nueva o actualizada versión. B) Crear un repositorio en un equipo central de desarrollo para el resguardo de códigos, documentación, inventarios de datos y manuales de usuario, administrador y programador. C) Ejecutar las pruebas de nuevas versiones o actualizaciones del sistema de información en el equipo dispuesto para tal efecto. Nunca usar -equipos físicos o virtuales con el sistema actualmente en producción como las plataformas para evaluación de versiones en desarrollo. D) Llenar y firmar formato.		

Mejores prácticas, referencias:	1.- Se deben realizar respaldos de la información en los sistemas en desarrollo del mismo modo que como se realicen con el sistema en producción.	
Conocimientos requeridos:	Administración de sistema de información. Desarrollo de aplicaciones.	
Ejecución		Fecha inicio
Nombre y firma		Fecha término
Administrador del sistema de información o servidor		
Observaciones / anotaciones		

(Nombre del sistema A1)			Identificador único A1	
Formato:	24	Verificación anual	Acción concluida	()
Medidas de seguridad técnicas:		Artículo 18. I. f) Cumplir con las especificaciones de seguridad informática previo a la puesta en operación.		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Veinte días hábiles.		
Importancia de la acción:		Solo los sistemas de información revisados integralmente en su seguridad y estabilidad pueden ser publicados bajo el dominio .unam.mx .		
Proceso recomendado:		A) Una vez concluido el desarrollo o actualización de un sistema de información, solicitar al área de seguridad del Área Universitaria la revisión de seguridad informática del sistema, lo que incluye: pruebas de penetración, pruebas de estabilidad, pruebas de carga y endurecimiento de la seguridad. En caso de no contar con esa área, requerirlo a UNAM CERT al correo seguridad.tic@unam.mx . B) Una vez recibido el reporte del área de seguridad, aplicar las medidas de corrección que incluya el reporte. Regresar al punto A. C) Habiendo resuelto los hallazgos y sugerencias de mejora de la seguridad señalados por el área especializada, realizar la instalación del sistema en la plataforma definitiva de cómputo, extrayéndolo del entorno de desarrollo. D) Llenar y firmar formato.		
Mejores prácticas, referencias:		1.- El equipo de UNAM CERT puede asesorar a las entidades y dependencias en la aplicación de las medidas de corrección y mitigación a partir de los resultados de la revisión de seguridad.		
Conocimientos requeridos:		Administración de aplicaciones. Administración de sistema operativo.		
Ejecución			Fecha inicio	
Nombre y firma			Fecha término	
Administrador del sistema de información o servidor				
Observaciones / anotaciones				

(Nombre del sistema A1)	Identificador único A1
-------------------------	------------------------

Formato:	25	Verificación anual	Acción concluida	()
Medidas de seguridad técnicas:	Artículo 18. III. a) Utilizar equipos con componentes actualizados, protegidos con garantías y soporte, y con la capacidad suficiente para atender la demanda del servicio y de los usuarios.			
Aplicable en:	III. Equipos de cómputo.			
Tiempo estimado:	Hito.			
Importancia de la acción:	Mantener en adecuada condición de operación el equipo de cómputo incrementa la estabilidad y seguridad del sistema de información.			
Proceso recomendado:	A) Elaborar una lista del inventario de los equipos de cómputo, periféricos y de almacenamiento necesarios para la ejecución del sistema de información. B) Determinar la razón por la que el sistema de información requerirá estar localizado en un equipo físico y no en un servidor virtual. Con ello justificar una adquisición o actualización. Por ejemplo: por incompatibilidad con hipervisores, necesidades de comunicación exclusivamente locales en la entidad y dependencia o el no necesitar de un entorno de alta disponibilidad automática. C) Identificar en el inventario versiones, introducción en el mercado, vida útil, contratos de mantenimiento y soporte para todos y cada uno de los componentes, en el caso de emplear equipo físico. D) Adquirir los componentes y elementos necesarios para la actualización, vigencia de soporte y capacidad para atención a los usuarios en el equipo de cómputo físico. E) Llenar y firmar formato.			
Mejores prácticas, referencias:	1.- El mantenimiento preventivo debe contar con medidas de verificación.			
Conocimientos requeridos:	Administración de infraestructura.			
Ejecución			Fecha inicio	
Nombre y firma			Fecha término	
Administrador del sistema de información o servidor				
Observaciones / anotaciones				

(Nombre del sistema A1)		Identificador único A1		
Formato:	26	Verificación anual	Acción concluida	()
Medidas de seguridad técnicas:	Artículo 18. III. b) Definir el programa de mantenimiento preventivo.			
Aplicable en:	III. Equipos de cómputo.			
Tiempo estimado:	Hito.			
Importancia de la acción:	Garantizar que el plan de mantenimiento de equipo se realiza en tiempo y forma.			
Proceso recomendado:	A) De la lista de equipo de cómputo físico necesario para la operación del sistema de información, extraer las vigencias de mantenimiento. B) En caso de no estar en posibilidad de aplicar el mantenimiento preventivo por el personal del Área Universitaria, cotizar pólizas de mantenimiento de acuerdo con el tipo de componente, preferentemente una sola póliza para el conjunto del equipo físico.			

	C) Adquirir las pólizas de mantenimiento preventivo y observar su vigencia. La vigencia no podrá ser menor de un año. D) Llenar y firmar formato.
Mejores prácticas, referencias:	1.- El programa de mantenimiento debe considerar los costos de contratos, refacciones, partes, actualizaciones y reemplazos.
Conocimientos requeridos:	Administración de infraestructura.
Ejecución	
Nombre y firma	
Administrador del sistema de información o servidor	
Fecha inicio	
Fecha término	
Observaciones / anotaciones	

(Nombre del sistema A1)			Identificador único A1	
Formato:	27	Verificación anual	Acción concluida	()
Medidas de seguridad técnicas:	Artículo 19. III. c) Aplicar el programa de mantenimiento preventivo a los equipos.			
Aplicable en:	III. Equipos de cómputo.			
Tiempo estimado:	Seis días hábiles.			
Importancia de la acción:	Garantizar que el plan de mantenimiento de equipo se realiza en tiempo y forma.			
Proceso recomendado:	A) En caso de que el personal del Área Universitaria pueda realizar el mantenimiento preventivo, definir el calendario de inactividad del sistema de información, notificar a los usuarios y aplicar el plan en caso de mantenimiento o inactividad. B) En caso de que sea a través de un proveedor que se proporcione el mantenimiento al equipo de cómputo, ejecutar el calendario de acciones preventivas en un período no superior a cada 3 meses hasta la conclusión del contrato o póliza respectivo. C) Llenar y firmar formato.			
Mejores prácticas, referencias:	1.- Debe actualizarse el equipo de cómputo de manera suficiente para continuar la operación del sistema y considerar en el mantenimiento preventivo sistemas paralelos de manera temporal hasta la conclusión de los trabajos.			
Conocimientos requeridos:	Administración de infraestructura.			
Ejecución			Fecha inicio	
Nombre y firma			Fecha término	
Administrador del sistema de información o servidor				
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	28	Verificación anual	Acción concluida	()

Medidas de seguridad técnicas:	Artículo 21. Solo se permitirá el uso de servicios de nube pública para el resguardo de archivos cifrados que contengan respaldos de la información.	
Aplicable en:	Servicios en la nube pública.	
Tiempo estimado:	Hito.	
Importancia de la acción:	No pueden conservarse o usarse datos personales que sean tratados por la UNAM en servicios de nube pública. Estos servicios sólo se permiten para el respaldo de archivos cifrados, no en producción.	
Proceso recomendado:	A) Identificar los respaldos que se tengan resguardados en servicios de nube pública. B) Verificar el cifrado en cada uno de los respaldos que se almacenen en nube pública. El cifrado no deberá ser de menor capacidad al equivalente a AES de 128 bits.	
Mejores prácticas, referencias:	1.- La DGTIC proporciona el servicio de respaldos en el Centro de Datos, por lo que se sugiere utilizarlo en lugar de respaldos en la nube pública.	
Conocimientos requeridos:	Administración de respaldos. Administración de sistema operativo.	
Ejecución		Fecha inicio
Nombre y firma		Fecha término
Administrador del sistema de información o servidor		
Observaciones / anotaciones		