Documento de Seguridad de Datos Personales

Diciembre 2023

FACULTAD DE MEDICINA
VETERINARIA Y ZOOTECNIA

FACULTAD DE MEDICINA VETERINARIA ZOOTECNIA

PRESENTACIÓN

Este documento tiene el objetivo de documentar las actividades realizadas para integrar el Sistema de Gestión de la Seguridad de la información en la Facultad de Medicina Veterinaria y Zootecnia. En el presente documento se presentan mejoras ante los nuevos retos en tecnología, así como el trabajo constante en la prevención de riesgos potenciales para los sistemas, y se lleven a cabo las verificaciones pertinentes que se manejan dentro de la Facultad de Medicina Veterinaria y Zootecnia.

El alcance de este proceso se centra en la seguridad de la información tanto de datos personales como datos personales sensibles que recabe y trate la Facultad de Medicina Veterinaria y Zootecnia, de accesos no autorizados ni de tratamientos distintos a los fines para los que fueron recabados.

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Dentro de la Facultad de Medicina Veterinaria y Zootecnia, se cuenta con sistemas para el registro de estudiantes para la rotación de prácticas que se llevan en la Facultad y sus Centros de Enseñanza.

Es en este sistema donde se solicita información que contenga o no datos personales para la coordinación de las prácticas a realizarse en los centros de enseñanza.

A este sistema tiene acceso el personal de la Coordinación de Enseñanza Práctica y el Departamento de Tecnología Educativa, quienes se encargan de verificar que el sistema se encuentre en condiciones para procesar los registros de los estudiantes garantizando la protección de sus datos.

La información es recopilada y resguardada en este sistema en el área de Servidores de la Facultad de Medicina Veterinaria y Zootecnia para su consulta y tratamiento por la Coordinación de Enseñanza Práctica.

Para apoyar estas actividades, en el Departamento de Educación Tecnológica se cuenta con el siguiente sistema:

En el Anexo 1. Inventario de sistemas de tratamiento de datos personales

ROLES Y RESPONSABILIDADES DE LOS INVOLUCRADOS EN LA SEGURIDAD DE LA INFORMACIÓN.

Los perfiles de puestos del personal que participa en el tratamiento de datos personales son los siguientes:

Titular de la Dependencia. Responsable de designar al personal responsable para el resguardo, tratamiento e implementación de medidas en seguridad de datos personales.

Coordinador de Seguridad de la Información. Responsable de establecer las medidas y políticas a fin de garantizar la protección de datos personales en la Dependencia.

Encargado de Seguridad de la Información. Responsable de implementar y verificar el cumplimiento de las medidas de seguridad para la protección de datos personales. Responsable de informar el estado de la implementación al Coordinador de Seguridad de la Información.

Personal de Unidad Administrativa. Encargado de resguardar el archivo físico de la FMVZ.

Responsable de sistemas. Encargados de desarrollar, elaborar respaldos, actualizar y mantener en operación los sistemas y servidores de la FMVZ.

En el Anexo 2 se detallan las funciones y obligaciones de quienes traten datos personales.

ANÁLISIS DE RIESGO.

Para poder realizar el análisis de riesgos, el Departamento de Tecnología Educativa, considera el Análisis FODA (Fortalezas, Oportunidades, Debilidades y Amenazas), así como las partes interesadas, involucradas en el proceso de la Seguridad de la Información.

En el Anexo 3 se detalla el Análisis de Riesgos.

ANÁLISIS DE BRECHA.

Una vez identificado los controles necesarios para mitigar los riesgos encontrados en nuestros activos de información, se hace un Análisis de Brecha por medio del cual se identifica lo siguiente:

1. Las medidas de seguridad existentes y efectivas;
2. El nivel óptimo de medidas de seguridad y
3. Las medidas de seguridad adicionales a las existentes para alcanzar el nivel óptimo.

Anexo 4 Análisis de Brecha.

PLAN DE TRABAJO.

Una vez realizado el análisis de riesgos y haber identificado los controles faltantes para mitigar cada riesgo, se hace un plan para implementar los controles de seguridad faltantes, en el cual se identifican estos controles, las actividades a realizar para implementar el control, el tiempo estimado para completar las actividades, la prioridad que se dará a dicho control y finalmente, las áreas responsables de su implementación.

En el Anexo 5 se detalla el Plan de trabajo.

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

Dada la complejidad de diversos sistemas en la UNAM, se ha dispuesto la ruta crítica para el cumplimiento de las MST en tres etapas para los sistemas de información que a la fecha de publicación de 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 fmvz.unam.mx.

Etapa 1. Corto plazo. Requisitos de misión crítica y mínimos indispensables para la protección de datos personales y datos personales sensibles. Cumplimiento obligatorio en menos de treinta días hábiles.

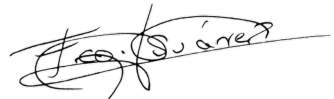
Etapa 2. Mediano plazo. Requisitos importantes para garantizar la protección de datos personales y datos personales sensibles. Ejecución estimada entre un mes y seis meses.

Etapa 3. Largo plazo. Requisitos necesarios para reforzar la seguridad en la protección de datos personales y datos personales sensibles. Ejecución estimada entre seis y doce meses.

En el Anexo 6 Formatos para el cumplimiento de las MST.

En esta versión del documento solo se listan los formatos de las actividades realizadas para cumplir con lo dispuesto en la etapa 1, 2 y 3.

APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

		Nombre y firma de quienes revisaron el presente documento
Desarrolló	**Eric Martínez Paredes** **Responsable de Seguridad de Datos Personales** **Tel. 555556225987** **eric.martinez@unam.mx**	 **Eric Martínez Paredes**
Desarrolló	**Myriam Beltrán Zavaleta** **Responsable de administrativo de Seguridad de Datos Personales** **Tel. 5556225959** **myriambz@fmvz.unam.mx**	 **Myriam Beltrán Zavaleta**
Autorizó	**Francisco Suárez Güemes** **Titular de la Facultad de Medicina Veterinaria y Zootecnia** **Tel. 5556225962 y 5556225884** **direccionfmvz@unam.mx**	 **Francisco Suárez Güemes**
Fecha de Aprobación		**19/05/2022**
Fecha de Actualización		**14/12/2023**

ANEXOS

Diciembre 2023

FACULTAD DE MEDICINA
VETERINARIA Y ZOOTECNIA

ANEXO 1

Inventario de sistemas de tratamiento de datos personales

Diciembre 2023

Coordinación de Enseñanza Práctica	
Identificador único*	**FMVZ-SIS-038**
(Nombre del sistema A1) *	**Moodle de la COEPA**
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre del Alumno y Número de Cuenta para identificarlos; Fecha de nacimiento, para su ingreso y cambio de contraseña.
Responsable*:	Coordinador de Enseñanza Práctica
Nombre*:	**Javier Flores Covarrubias**
Cargo*:	**Responsable Administrativo de Sistemas**
Funciones*:	Designación de los Encargados de Sistema, Funciones y Obligaciones, implementación de Medidas de Seguridad, Capacitar al personal, revisión de documentos y estar presente en Auditorias.
Obligaciones*:	Verificar que se cumplan con los lineamientos y Normas Complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la Universidad.
	Encargados:
(Nombre del Encargado 1*)	**Gabriela García Beltrán**
Cargo*:	**Responsable de Seguridad**
Funciones*:	Solicitar datos de las generaciones que entran a Hemi-semestre Práctico al Departamento de Tecnología Educativa y dar de alta a los titulares en el sistema.
Obligaciones*:	Mantener los datos recabados sin alteración, apoyo para el cambio de contraseña en caso de que el titular así lo requiera.
(Nombre del Encargado 2*)	**José Iván López Pelcastre**
Cargo*:	**Responsable Técnico**
Funciones*:	Cargar datos (Nombre y No de Cuenta) de las generaciones que sean solicitados por la Responsable de Seguridad y Apoyo con las medidas de seguridad técnicas del Sistema.
Obligaciones*:	Cumplir con lo establecido en los lineamientos y en las Normas Complementarias correspondiente al área Técnica
	Usuarios:
(Nombre del Usuario 1*)	**Gabriela García Beltrán**
Cargo*:	**Responsable de Seguridad**
Funciones*:	Bajar informes y reportes de prácticas y evaluación de los profesores, actualizar archivos que contienen la información de las prácticas.
Obligaciones*:	Cumplir con lo establecido en los lineamientos y en las Normas Complementarias correspondiente al área Administrativa.
(Nombre del Usuario 2*)	**Javier Flores Covarrubias**
Cargo*:	**Usuario**
Funciones*:	Revisar los archivos que se encuentran en el Sistema de Moodle de la COEPA
Obligaciones*:	Mantener informada a la Encargada del sistema, de cualquier falla en los archivos que se encuentran o cambios en ellos (cuenta no permite cambios ni ver datos personales)
(Nombre del Usuario 3*)	**Myriam Beltrán Zavaleta**

Cargo*:	**Usuario**
Funciones*:	Revisar los archivos que se encuentran en el Sistema de Moodle de la COEPA
Obligaciones*:	Mantener informada a la Encargada del sistema, de cualquier falla en los archivos que se encuentran o cambios en ellos (cuenta no permite cambios ni ver datos personales)

Identificador único*	**FMVZ-SIS-069**
Sistema (Nombre del A2)*:	**Sistema de Estancias dentro de la FMVZ y CEIES de la misma**
Datos personales contenidos en el sistema*:	Nombre, teléfono, correo electrónico, universidad de procedencia, si es extranjero pasaporte y lugar donde realizará su estancia
Responsable:	Coordinador de Enseñanza Práctica
Nombre*:	**Javier Flores Covarrubias**
Cargo*:	**Responsable Administrativo de Sistemas**
Funciones*:	Designación de los Encargados del Sistema, Funciones y Obligaciones, implementación de Medidas de Seguridad, Capacitar al personal, revisión de documentos y estar presente en Auditorias.
Obligaciones*:	Verificar que se cumplan con los lineamientos y Normas Complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la Universidad.
	Encargados:
(Nombre del Encargado 1*)	**Javier Flores Covarrubias**
Cargo*:	**Encargado de Seguridad**
Funciones*:	Recibir el formulario con los datos recabados, hacérselos llegar a Usuario 1.
Obligaciones*:	Verificar que se cumplan con los lineamientos y Normas Complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la Universidad.
	Usuarios
(Nombre del Usuario 1*)	**Gabriela García Beltrán**
Cargo*:	**Encargado de Seguridad**
Funciones*:	Recibir los datos, y recabarlos en un archivo de Excel, hacer el oficio de aceptación de estancia. Regresarlo al Coordinador de Enseñanza Práctica
Obligaciones*:	Recabar los datos sin modificarlos, resguardar los datos recopilados.
Identificador único*	**FMVZ-SIS-068**
Sistema (Nombre del A3)*:	**Sistema de Registro a Guardias Voluntarias a Centros de la Facultad (SIRGE)**
Datos personales contenidos en el sistema*:	Datos de identificación del alumno: Nombre, número de cuenta, teléfono celular, correo electrónico.
Responsable:	Coordinador de Enseñanza Práctica
Nombre*:	**Javier Flores Covarrubias**
Cargo*:	**Responsable Administrativo de Sistemas**
Funciones*:	Designación de los Encargados del Sistema, Funciones y Obligaciones, implementación de Medidas de Seguridad,

	Capacitar al personal, revisión de documentos y estar presente en Auditorias.
Obligaciones*:	Verificar que se cumplan con los lineamientos y Normas Complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la Universidad.
	Encargados:
(Nombre del Encargado 1)	**Myriam Beltrán Zavaleta**
Cargo*:	**Encargado de Seguridad**
Funciones*:	Solicitar la carga de los datos (Nombre y número de cuenta) al DTE, de manera anual, ingresar datos al sistema (teléfono y correo), modificar datos en caso de que así lo solicite el titular
Obligaciones*:	Proteger los datos de los alumnos que se encuentran registrados en el SIRGE. Solicitar cambios de USUARIOS, proteger el equipo de computo donde se abra el SIRGE, mantener contraseña única e intransferible
(Nombre del Encargado 2)	**José Iván López Pelcastre**
Cargo*:	**Responsable Técnico**
Funciones*:	Cargar datos (Nombre y No de cuenta) de las generaciones que se soliciten por la COEPA, Apoyo técnico en cuanto al SIRGE
Obligaciones*:	Proteger a nivel técnico el SIRGE, cumpliendo con lo establecido en los lineamientos para la protección de datos personales en posesión de la UNAM así como las establecidas en las Normas Complementarias sobre medidas de Seguridad Técnicas para protección de datos.
(Nombre del Encargado 3)*	**Miguel Ángel Sandoval Texcahuac**
Cargo*:	**Responsable Técnico**
Funciones*:	Realizar cambios en el SIRGE a solicitud de la COEPA, en cuanto al Sistema.
Obligaciones*:	Proteger a nivel técnico el SIRGE, cumpliendo con lo establecido en los lineamientos para la protección de datos personales en posesión de la UNAM así como las establecidas en las Normas Complementarias sobre medidas de Seguridad Técnicas para protección de datos.
	Usuarios:
(Nombre del Usuario 1*)	**Myriam Beltrán Zavaleta**
Cargo*:	**Responsable de Seguridad**
Funciones*:	Ingresar datos de los alumnos, modificar los datos cuando sea solicitado por los mismos.
Obligaciones*:	Proteger los datos de los alumnos que se encuentran registrados en el SIRGE. Solicitar cambios de USUARIOS, proteger el equipo de computo donde se abra el SIRGE, mantener contraseña única e intransferible
(Nombre del Usuario 2*)	**Eric Martínez Paredes**
Cargo*:	**Usuario**
Funciones*:	Hacer pruebas para el correcto funcionamiento de las adecuaciones solicitadas por la COEPA, dentro del SIRGE
Obligaciones*:	Cumplir con lo establecido en los lineamientos y en las Normas Complementarias sobre medidas de Seguridad Técnica para protección de datos.

Identificador único*	**FMVZ-SIS-084**

Sistema (Nombre del A4)*:	**Sistema de Registro para Seguro de Vida del Patronato**
Datos personales contenidos en el sistema*:	Datos de identificación del alumno: Nombre, número de cuenta, número de ISS, dirección particular, firma. Datos de beneficiario. Nombre completo. En caso de ser menor de edad, copia de una credencial.
Responsable:	Coordinador de Enseñanza Práctica
Nombre*:	**Javier Flores Covarrubias**
Cargo*:	**Responsable Administrativo de Sistemas**
Funciones*:	Designación de los Encargados del Sistema, Funciones y Obligaciones, implementación de Medidas de Seguridad, Capacitar al personal, revisión de documentos y estar presente en Auditorias.
Obligaciones*:	Verificar que se cumplan con los lineamientos y Normas Complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la Universidad.
	Encargados:
(Nombre del Encargado 1*)	**Myriam Beltrán Zavaleta**
Cargo*:	**Encargado de Seguridad**
Funciones*:	Solicitar al alumno, que lo solicite, llenar el formato de Prácticas de Campo del Patronato de la UNAM, realizar el pago correspondiente.
Obligaciones*:	Envío de Oficio con el formato de Prácticas de Campo y pago correspondiente al responsable del Patronato de la UNAM. Resguardo de una copia del oficio en digital.
	Usuarios:
(Nombre del Usuario 1*)	**LC. Ismael Yáñez**
Cargo*:	**Gestión de Seguros del Patronato**
Funciones*:	Recepción de oficios y dar de alta en la aseguradora.
Obligaciones*:	Mantener los datos sin alteraciones, cumplir con los establecido en los lineamientos y en las Normas Complementarias sobre medidas de Seguridad Administrativa para protección de datos

Departamento de Medicina y Zootecnia de Aves	
Identificador único*	**FMVZ-SIS-004**
Nombre del sistema*	**Servicio de diagnóstico**
Datos personales con justificación (sensibles o no) contenidos en el sistema*:	Nombre del propietario Domicilio donde se encuentran las aves Teléfono celular Correo electrónico Firma RFC Régimen fiscal
Responsable*:	Jefe de Departamento
Nombre*:	**Cecilia Rosario Cortés**
Cargo*:	**Jefe de departamento**
Funciones*:	Controlar, coordinar y organizar el seguimiento y cumplimiento de los procesos de enseñanza, servicio y formación de recursos humanos en el DMZA que son sustantivos para la FMVZ.

	Firmar la carta de confidencialidad correspondiente.
Obligaciones*:	Designar al personal responsable de las áreas de diagnóstico y de calidad. Vigilar el proceso de la entrega de resultados Firmar la carta de confidencialidad correspondiente. Dar cumplimiento con lo establecido en las Normas Complementarias sobre medidas de Seguridad Técnica, Administrativas y Físicas para la protección de datos personales en posesión de la Universidad.
	Encargados:
Nombre del Encargado *	**Teresa Olivares Hernández**
Cargo*:	**Responsable de calidad**
Funciones*:	Coordinar el área de diagnóstico para asegurar el cumplimiento del proceso de diagnóstico conforme los lineamientos y requisitos acordados en Sistema de Gestión de Calidad del DMZA.
Obligaciones*:	Revisar y verificar la escritura correcta de los datos proporcionados por el usuario al realizar la historia clínica. Supervisar el envío por correo electrónico de las constancias de resultados al usuario. Resguardar la información que el usuario proporcionó así como los resultados que se obtuvieron por el proceso de las muestras. Firmar la carta de confidencialidad correspondiente. Dar cumplimiento con lo establecido en las Normas Complementarias sobre medidas de Seguridad Técnica, Administrativas y Físicas para la protección de datos personales en posesión de la Universidad
(Nombre del Encargado 2*)	**Juan Carlos Morales Luna**
Cargo*:	**Responsable del área de diagnóstico y recepción de muestras**
Funciones*:	Recopilar la información del usuario
Obligaciones*:	Resguardar la información del usuario, protección de los datos proporcionados en el formato de historia clínica y bitácora de diagnóstico y constancia de resultados. Firmar la carta de confidencialidad correspondiente. Dar cumplimiento con lo establecido en las Normas Complementarias sobre medidas de Seguridad Técnica, Administrativas y Físicas para la protección de datos personales en posesión de la Universidad
	Usuarios:
(Nombre del Encargado 3*)	**Ayudantes de diagnóstico**
Cargo*:	**Ayudantes de diagnóstico**
Funciones*:	Recopilación de información y utilización de los datos del usuario para la elaboración de formatos y constancias de resultados
Obligaciones*:	Resguardar la información del usuario Completar correctamente el llenado de formatos, bitácoras y registros. Enviar al correo electrónico del propietario la constancia de resultados o entregarla en forma física. Firmar la carta de confidencialidad correspondiente. Dar cumplimiento con lo establecido en las Normas Complementarias sobre medidas de Seguridad Técnica, Administrativas y Físicas para la protección de datos personales en posesión de la Universidad
(Nombre del Usuario 1*)	**Servicio social**

Cargo*:	**Servicio social**
Funciones*:	Participar en la captura y registro de los datos del usuario al momento de solicitar el servicio de diagnóstico
Obligaciones*:	Resguardar la información proporcionada por el usuario y utilizarla únicamente para la colaboración en la elaboración de los formatos, constancia de resultados y envío de correos electrónicos de los usuarios. Firmar la carta de confidencialidad correspondiente. Dar cumplimiento con lo establecido en las Normas Complementarias sobre medidas de Seguridad Técnica, Administrativas y Físicas para la protección de datos personales en posesión de la Universidad
(Nombre del Usuario 2*)	**Responsables de las áreas de diagnóstico**
Cargo*:	**Responsables de las áreas de diagnóstico**
Funciones*:	Emitir los resultados de las pruebas diagnósticas.
Obligaciones*:	Resguardar la información del usuario a la que tendrá acceso para emitir el diagnóstico correspondiente. Firmar la carta de confidencialidad correspondiente. Dar cumplimiento con lo establecido en las Normas Complementarias sobre medidas de Seguridad Técnica, Administrativas y Físicas para la protección de datos personales en posesión de la Universidad.

Departamento de Patología	
Identificador único*	**FMVZ-SIS-066**
Nombre del sistema*	**Servicio de diagnóstico**
Datos personales con justificación (sensibles o no) contenidos en el sistema*:	Nombre, teléfono y correo electrónico (del propietario y del médico veterinario)
Responsable*:	
Nombre*:	**Dra. Luary Carolina Martínez Chavarría**
Cargo*:	**Jefa del Departamento de Patología**
Funciones*:	Coordinar y supervisar el servicio de diagnóstico con base en la misión y visión del Departamento de Patología
Obligaciones*:	Vigilar que los datos obtenidos en el servicio de diangóstico estén protegidos Dar cumplimiento con lo establecido en las Normas Complementarias sobre medidas de Seguridad Técnica, Administrativas y Físicas para la protección de datos personales en posesión de la Universidad
	Encargados:
Nombre del Encargado *	**Dr. Isaac Martínez Racine (anatomopatología)**
Cargo*:	**Responsable del área de diagnóstico de anatomopatología**
Funciones*:	Coordinar y supervisar el servicio de diagnóstico de anatomopatología
Obligaciones*:	Establecer las medidas de seguridad y control para proteger la información del servicio de diangóstico
(Nombre del Encargado 2*)	**Dra. Karla Mollinedo Beltrán (patología clínica)**
Cargo*:	**Responsable del área de diagnóstico de patología clínica**
Funciones*:	Coordinar servicio de diagnóstico de anatomopatología y patología clínica
Obligaciones*:	Establecer las medidas de seguridad y control para proteger la información del servicio de diangóstico.

(Nombre del Encargado 2*)	**Maricarmen Zúñiga**
Cargo*:	**Recepcionista**
Funciones*:	Atender a usuarios del servicio de diagnóstico
Obligaciones*:	Brindar información a los usuario del servicio de diagnóstico sobre el uso el tratamiento de sus datos personales
	Usuarios:
(Nombre del Usuario 1*)	Anexo
Cargo*:	
Funciones*:	
Obligaciones*:	

Identificador único*	**SIS-FMVZ-013**
Sistema (Nombre del A2)*:	**Sistema de registro de asistencia**
Datos personales contenidos en el sistema*:	Nombre y huella dactilar
	Responsable:
Nombre*:	**Dra. Luary Carolina Martínez Chavarría**
Cargo*:	**Jefa del Departamento de Patología**
Funciones*:	Coordinar y supervisar el registro de huella dactilar
Obligaciones*:	Dar cumplimiento con lo establecido en las Normas Complementarias sobre medidas de Seguridad Técnica, Administrativas y Físicas para la protección de datos personales en posesión de la Universidad
	Encargados:
(Nombre del Encargado 1*)	**Dr. Isaac Martínez Racine (anatomopatología)**
Cargo*:	**Responsable del registro de huella dactilar en el área de anatomopatología**
Funciones*:	Administrar el registro de huella dactilar
Obligaciones*:	Resguardar la información obtenida
(Nombre del Encargado 2*)	**Dr. Luis Enrirque García Ortuño**
Cargo*:	**Responsable del registro de huella dactilar en el área de patología clínica**
Funciones*:	Administrar el registro de huella dactilar
Obligaciones*:	Resguardar la información obtenida.

Departamento de Nutrición Animal y Bioquímica	
Identificador único*	**FMVZ-SIS-014**
Nombre del sistema*	**Servicios de Laboratorio de Bromatología I y II**
Datos personales con justificación (sensibles o no) contenidos en el sistema*:	Nombre, correo electrónico (personal o institucional), procedencia
Responsable*:	Departamento de Nutrición Animal y Bioquímica
Nombre*:	**Dr. Luis Corona Gochi**
Cargo*:	**Jefe del Departamento de Nutrición Animal y Bioquímica**
Funciones*:	Decidir sobre el tratamiento automatizado de los datos personales, así como el contenido, finalidad y uso del sistema
Obligaciones*:	Las establecidas en los lineamientos para la Protección de Datos Personales en Posesión de la UNAM para responsables del tratamiento de datos personales en las áreas universitarias.
	Encargados:
Nombre del Encargado *	**QA. Águeda García Pérez**

Cargo*:	**Encargada de Datos Personales**
Funciones*:	Recabar información de los usuarios
Obligaciones*:	Proteger los datos personales en el proceso mediante la implementación de estrategias y mecanismos de seguridad en su desarrollo y mantenimiento.
	Usuarios:
(Nombre del Usuario 1*)	**MVZ Juana de Dios Becerril De la Cruz**
Cargo*:	**Dar seguimiento de llenado de Bitácoras**
Funciones*:	Recabar información de muestras
Obligaciones*:	Proteger la privacidad de los datos personales a los que accede mediante el uso del sistema
(Nombre del Usuario 2*)	**Servicio Social en turno y Ayudante de Profesor**
Cargo*:	**Encargados de llenar Bitácoras**
Funciones*:	Recabar información de muestras
Obligaciones*:	Proteger la privacidad de los datos personales a los que accede mediante el uso del sistema
(Nombre del Usuario 3*)	**Laboratoristas en turno**
Cargo*:	**Laboratorista**
Funciones*:	Procesamiento de Muestras
Obligaciones*:	Cumplir con lo establecido en las normas complementarias de medidas técnicas administrativas y físicas en materia de datos personales en posesión de la UNAM.

Secretaría de Planeación	
Identificador único*	**FMVZ-SIS-026**
(Nombre del sistema A1) *	**Informe de Labores.**
Datos personales (sensibles o no) contenidos en el sistema*:	Datos de identificación: Nombre, correo electrónico, RFC, idioma o lengua, Datos laborales: Nombramiento o puesto. Datos académicos: Trayectoria educativa, títulos, certificados y reconocimientos, entre otros.
Responsable*:	
Nombre*:	**Verónica Caballero Gutiérrez**
Cargo*:	**Secretaria de Planeación**
Funciones*:	Es responsable de dirigir, administrar el sistema y de garantizar que el tratamiento de los datos personales se realice de conformidad con la ley.
Obligaciones*:	Debe establecer medidas de seguridad adecuadas para la protección de los datos personales y asegurarse de que los usuarios y encargados del sistema cumplan con las políticas de protección de datos.
	Encargados:
(Nombre del Encargado 1*)	**Roberto Gallegos Carreño**
Cargo*:	**Asistente de Procesos**
Funciones*:	Encargado de administrar y dar mantenimiento al sistema Informe de Labores.
Obligaciones*:	Garantizar la seguridad y privacidad de los datos personales contenidos en el sistema y mantener actualizado el software del sistema.
(Nombre del Encargado 2*)	**José Iván López Pelcastre**
Cargo*:	**Administrador del Área de Servidores**
Funciones*:	Encargado de brindar soporte técnico al servidor.

Obligaciones*:	Garantizar la seguridad de los datos personales contenidos en el servidor y mantener actualizado el software y hardware del servidor.
	Usuarios:
(Nombre del Usuario 1*)	**Profesores de asignatura, Profesores de tiempo completo y Técnicos académicos.**
Cargo*:	**Académicos**
Funciones*:	Ingresar sus actividades laborales y administrativas en el sistema Informe de Labores
Obligaciones*:	Garantizar la veracidad y exactitud de los datos personales que ingrese en el sistema, así como el cumplimiento de los lineamientos y políticas establecidos por la institución en materia de protección de datos personales.

Departamento de Medicina, Cirugía y Zootecnia de Équidos	
Identificador único*	**FMVZ-SIS-027**
(Nombre del sistema A1) *	**Procesos del Hospital del Departamento de medicina cirugía y zootecnia para équidos (DMCZE)**
Datos personales (sensibles o no) contenidos en el sistema*:	Datos personales, no sensibles. (nombre, primer apellido, número telefónico, correo electrónico y domicilio). Datos personales sensibles: (“Datos fiscales” ejemplo: RFC, CURP, nombre completo. Actividad económica ejemplo: “asalariado, alquiler de vivienda, intereses por inversiones, intereses por deposito, socio o accionista”. Datos de domicilio ejemplo: código postal, nombre de vialidad, numero interior, numero exterior, calle, nombre de la colonia, municipio y colonia”).
Responsable*:	
Nombre*:	**MSc. Alejandro Rodríguez Monterde**
Cargo*:	**Jefe del departamento del DMCZE, MSc. Alejandro Rodríguez Monterde**
Funciones*:	Definir el alcance del proceso, también definir roles y responsabilidades del personal involucrado en el sistema.
Obligaciones*:	Dar cumplimiento con lo establecido en los lineamientos sobre medidas de protección de datos UNAM.
	Encargados:
(Nombre del Encargado 1*)	**Lic. Karim Ulises Salazar García**
Cargo*:	**Seguridad de datos personales, Técnico académico del DMCZE**
Funciones*:	Resguardar los record´s de la clínica después de haber sido llenado por los alumnos del hospital del departamento. Asegurar los record´s de los pacientes una vez llenados y solo dar el uso de los documentos resguardados para fines académicos
Obligaciones*:	Dar cumplimiento de las MTS establecidos en las normas complementarias por DGETIC y, establecer comunicación con él DTE además de la unidad jurídica.
(Nombre del Encargado 2*)	**Admin. Diego Emmanuel González**
Cargo*:	**Delegado Administrativo del DMCZE**
Funciones*:	Resguardar los datos personales con los alineamientos de la UNAM, también tener comunicación con la jefatura, así como el responsable del área de datos personales.
Obligaciones*:	Dar cumplimiento con lo establecido en los lineamientos sobre

	medidas de protección de datos UNAM.
Nombre del Encargado 3*)	**Residentes (MVZ- maestría).**
cargo	**Residentes del Hospital para équidos del DMCZE.**
funciones	Sin acceso a datos personales, no hacer cambios en los mismos y únicamente a expedientes del paciente.
obligaciones	Dar cumplimiento con lo establecido en los lineamientos sobre medidas de protección de datos UNAM.
Nombre del encargado 4*	**Internos (MVZ titulados).**
Cargo	**Internos del Hospital para équidos del DMCZE**
Funciones	Sin acceso a datos personales, no hacer cambios en los mismos y únicamente a expedientes del paciente.
Obligaciones	Dar cumplimiento con lo establecido en los lineamientos sobre medidas de protección de datos UNAM.
	Usuarios:
(Nombre del Usuario 1*)	**Alumnos de la FMVZ, también servicio social y trabajo profesional, por otro lado, estancias e Internado del DMCZE y finalmente, estudiantes del programa de Posgrado del DMCZE.**
.Cargo*:	**Estudiantes de licenciatura y posgrado de igual forma, pasantes de la FMVZ del DMCZE.**
Funciones*:	Sin acceso a datos personales, no hacer cambios en los mismos y únicamente a expedientes del paciente.
Obligaciones*:	Dar cumplimiento con lo establecido en los lineamientos sobre medidas de protección de datos UNAM.
(Nombre del Usuario 2, profesores):	**Profesores de la FMVZ-UNAM del DMCZE.**
Cargo:	**Catedráticos del DMCZE de la FMVZ-UNAM.**
Funciones:	Sin acceso a datos personales, no hacer cambios en los mismos y únicamente a expedientes del paciente.
Obligaciones*:	Dar cumplimiento con lo establecido en los lineamientos sobre medidas de protección de datos UNAM.

Identificador único*	**FMVZ-SIS-028**
Sistema:	**Internado, Estancia y voluntarios del departamento de medicina cirugía y zootecnia para équidos (DMCZE) hospital para équidos.**
Datos personales contenidos en el sistema	Nombre, apellido, número telefónico, nombre de la universidad donde residen (internos-estancias) y correo electrónico (datos personales no sensibles).
	Responsable:
Nombre*:	**Alejandro Rodríguez Monterde**
Cargo*:	**Responsable del área.**
Funciones*:	Definir el alcance del proceso, concretar los roles y responsabilidades del personal involucrado en el sistema
Obligaciones*:	Dar cumplimiento con lo establecido en los lineamientos sobre medidas de protección de datos UNAM.
	Encargados:
(Nombre del Encargado 1*)	**Salazar García Karim Ulises**
Cargo*:	**Seguridad de datos personales**
Funciones*:	Tener comunicación con las diferentes áreas que estén en contacto o manejen datos personales, para dar información sobre las mejoras, para llevar los procesos.

Obligaciones*:	Dar cumplimiento de las MTS establecidos en las normas complementarias por DGETIC y, establecer comunicación
(Nombre del Encargado 2*)	**Yasmin Esperanza López García**
Cargo*:	**Responsable del programa de internado, estancias y voluntarios del hospital para équidos.**
Funciones*:	Recibir los datos personales no sensibles, de los alumnos de internado, estancia y voluntarios del hospital del DMCZE. Por otro lado, establecer comunicación con el encargado de área del DMCZE y encargado de los datos personales del DMCZE y, así mismo, con el departamento de jurídico de la FMVZ.
Obligaciones*:	Dar cumplimiento con lo establecido en los lineamientos sobre medidas de protección de datos de la UNAM.
	Usuarios:
(Nombre del Usuario 1*)	**Hospital de équidos del DMCZE.**
Cargo*:	**Sitio de enseñanza.**
Funciones*:	Establecer comunicación con el responsable del área del DMCZE y, a su vez, con el responsable de datos personales del DMCZE.
Obligaciones*:	Dar cumplimiento con lo establecido en los lineamientos sobre medidas de protección de datos UNAM

Departamento de Publicaciones	
Identificador único*	**FMVZ-SIS-060 Revista Clínica Veterinaria (revistas.fmvz.unam.mx/index.php/Clinica-Veterinaria)**
Nombre del sistema*	**Open Journal System (OJS)**
Datos personales con justificación (sensibles o no) contenidos en el sistema*:	Nombre completo; Correo electrónico; Adscripción laboral. País de origen; ORCID iD.
Responsable*:	Jefe del Departamento de Publicaciones
Nombre*:	Dr. Enrique Jesús Delgado Suárez
Cargo*:	**Jefe del Departamento de Publicaciones**
Funciones*:	Designación de las personas autorizadas para tener acceso a los datos personales de los autores y usuarios.
Obligaciones*:	Dar cumplimiento al acuerdo por el que se establecen los lineamientos para la protección de datos personales en posesión de la Universidad Nacional Autónoma de México.
	Encargados:
Nombre del Encargado técnico*	**Ing José Iván López Pelcastre**
Cargo*:	**Administrador del área de servidores**
Funciones*:	A solicitud del responsable o primer encargado: actualizar, corregir o dar servicio a la plataforma para su óptimo funcionamiento.
Obligaciones*:	Dar cumplimiento al acuerdo por el que se establecen los lineamientos para la protección de datos personales en posesión de la Universidad Nacional Autónoma de México.
(Nombre del Encargado 1*)	**Mtra. Elizabeth Sarmiento de la Huerta**
Cargo*:	**Gestión Editorial**
Funciones*:	Responsable de los artículos, desde su ingreso hasta su publicación.
Obligaciones*:	Dar cumplimiento al acuerdo por el que se establecen los lineamientos para la protección de datos personales en posesión

	de la Universidad Nacional Autónoma de México.
(Nombre del Encargado 2*)	**MVZ Silvia M. Ibañez Zavala**
Cargo*:	**Gestión Editorial**
Funciones*:	**Responsable de los artículos, desde su ingreso hasta su publicación.**
Obligaciones*:	Dar cumplimiento al acuerdo por el que se establecen los lineamientos para la protección de datos personales en posesión de la Universidad Nacional Autónoma de México.
	Usuarios:
(Nombre del Usuario 1*)	**DGV Firely Avril Braulio Ortiz**
Cargo*:	**Diseño Gráfico y Editorial de Libros y Revistas Electrónicas**
Funciones*:	**Formación de las galeras del artículo a publicarse**
Obligaciones*:	Dar cumplimiento al acuerdo por el que se establecen los lineamientos para la protección de datos personales en posesión de la Universidad Nacional Autónoma de México.
(Nombre del Usuario 2*)	**Pendientes**
Cargo*:	**Editores de sección (por definir)**
Funciones*:	Entre sus funciones se encuentran, pero no se limitan: Evaluar el mérito académico de los artículos, antes de asignar un revisor. Integrar las evaluaciones de los revisores y emitir una recomendación para el Editor de la Revista.
Obligaciones*:	Dar cumplimiento al acuerdo por el que se establecen los lineamientos para la protección de datos personales en posesión de la Universidad Nacional Autónoma de México.

Identificador único*	**FMVZ-SIS-061 Revista Veterinaria México (veterinariamexico.unam.mx)**
Nombre del sistema*	**Open Journal System (OJS)**
Datos personales con justificación (sensibles o no) contenidos en el sistema*:	Nombre completo; Correo electrónico; Adscripción laboral País de origen; ORCID iD.
	Responsables:
Nombre*:	Dr. Enrique Jesús Delgado Suárez
Cargo*:	**Jefe del Departamento de Publicaciones**
Funciones*:	Designación de las personas autorizadas para tener acceso a los datos personales de los autores y usuarios.
Obligaciones*:	Dar cumplimiento al acuerdo por el que se establecen los lineamientos para la protección de datos personales en posesión de la Universidad Nacional Autónoma de México.
	Encargados:
Nombre del Encargado técnico*	**Ing. Miguel Ángel Mejía Argueta**
Cargo*:	**DGTIC, Responsable de Acervos Digitales**
Funciones*:	A solicitud del responsable o primer encargado: actualizar, corregir o dar servicio a la plataforma para su óptimo funcionamiento.
Obligaciones*:	Dar cumplimiento al acuerdo por el que se establecen los lineamientos para la protección de datos personales en posesión de la Universidad Nacional Autónoma de México.

Nombre del Encargado técnico*	**Ing José Iván López Pelcastre**
Cargo*:	**Administrador del área de servidores**
Funciones*:	A solicitud del responsable o primer encargado: actualizar, corregir o dar servicio a la plataforma para su óptimo funcionamiento.
Obligaciones*:	Dar cumplimiento al acuerdo por el que se establecen los lineamientos para la protección de datos personales en posesión de la Universidad Nacional Autónoma de México.
Nombre del Encargado 1*	**MVZ Nora Lucía Galván Ochoa**
Cargo*:	**Gestión de Revistas Electrónicas; Gestión Editorial**
Funciones*:	**Responsable de los artículos, desde su ingreso hasta publicación**
Obligaciones*:	Dar cumplimiento al acuerdo por el que se establecen los lineamientos para la protección de datos personales en posesión de la Universidad Nacional Autónoma de México.
(Nombre del Encargado 2*)	**MVZ Miguel Ángel Cuevas Díaz**
Cargo*:	**Gestión Editorial**
Funciones*:	**Responsable de los artículos, desde su ingreso hasta publicación**
Obligaciones*:	Dar cumplimiento al acuerdo por el que se establecen los lineamientos para la protección de datos personales en posesión de la Universidad Nacional Autónoma de México.
	Usuarios:
(Nombre del Usuario 1*)	**DGV Firely Avril Braulio Ortiz**
Cargo*:	**Diseño Gráfico y Editorial de Libros y Revistas Electrónicas**
Funciones*:	**Formación de las galeras del artículo a publicarse**
Obligaciones*:	Dar cumplimiento al acuerdo por el que se establecen los lineamientos para la protección de datos personales en posesión de la Universidad Nacional Autónoma de México.
(Nombre del Usuario 2*)	**Mtra. Elizabeth Sarmiento de la Huerta**
Cargo*:	**Corrección de Estilo**
Funciones*:	Revisión del texto aprobado por el Comité Editorial y revisión de galeras.
Obligaciones*:	Dar cumplimiento al acuerdo por el que se establecen los lineamientos para la protección de datos personales en posesión de la Universidad Nacional Autónoma de México.
(Nombre del Usuario 3*)	**Ariadne Hernández Pérez** **Daniel Díaz Espinosa de los Monteros** **Einar Vargas Bello Pérez** **Elein Hernández Trujillo** **Enrique Jesús Delgado Suárez** **Ernesto Orozco Lucero** **Hugo Montaldo Valdenegro** **Hugo Oswaldo Toledo Alvarado** **José Ángel Gutiérrez Pabello** **María Salud Rubio Lozano** **Rafael Trueta Santiago**
Cargo*:	**Editores de sección**
Funciones*:	Entre sus funciones se encuentran, pero no se limitan: Evaluar el mérito académico de los artículos, antes de asignar un revisor. Integrar las evaluaciones de los revisores y emitir una recomendación para el Editor de la Revista.

Obligaciones*:	Dar cumplimiento al acuerdo por el que se establecen los lineamientos para la protección de datos personales en posesión de la Universidad Nacional Autónoma de México.

Identificador único*	**FMVZ-SIS-029**
Nombre del sistema*	**Libros - Facultad de Medicina Veterinaria y Zootecnia, UNAM (publicaciones.fmvz.unam.mx/index.php/fmvz) Open Monograph Press (OMP)**
Datos personales con justificación (sensibles o no) contenidos en el sistema*:	Nombre completo; Correo electrónico; Adscripción laboral, País de origen.
Responsable*:	Jefe del Departamento de Publicaciones
Nombre*:	Dr. Enrique Jesús Delgado Suárez
Cargo*:	**Jefe del Departamento de Publicaciones**
Funciones*:	Designación de las personas autorizadas para tener acceso a los datos personales de los autores y usuarios.
Obligaciones*:	Dar cumplimiento al acuerdo por el que se establecen los lineamientos para la protección de datos personales en posesión de la Universidad Nacional Autónoma de México.
	Encargados:
Nombre del Encargado técnico*	**Ing Jorge Pérez García**
Cargo*:	**Jefe del Departamento de Soporte Técnico de Sistemas Editoriales, Dirección de Fomento Editorial.**
Funciones*:	A solicitud del responsable o primer encargado (1): actualizar, corregir o dar servicio a la plataforma para su óptimo funcionamiento.
Obligaciones*:	Dar cumplimiento al acuerdo por el que se establecen los lineamientos para la protección de datos personales en posesión de la Universidad Nacional Autónoma de México.
Nombre del Encargado técnico*	**Ing. José Iván López Pelcastre**
Cargo*:	**Administrador del área de servidores, Facultad de Medicina Veterinaria y Zootecnia.**
Funciones*:	A solicitud del responsable o primer encargado: actualizar, corregir o dar servicio a la plataforma para su óptimo funcionamiento.
Obligaciones*:	Dar cumplimiento al acuerdo por el que se establecen los lineamientos para la protección de datos personales en posesión de la Universidad Nacional Autónoma de México.
(Nombre del Encargado 1*)	**MVZ Nora Lucía Galván Ochoa**
Cargo*:	**Gestión de Revistas Electrónicas**
Funciones*:	Carga de material y configuración general de la plataforma.
Obligaciones*:	Dar cumplimiento al acuerdo por el que se establecen los lineamientos para la protección de datos personales en posesión de la Universidad Nacional Autónoma de México.
(Nombre del Encargado 2*)	**MVZ Silvia M. Ibañez Zavala**
Cargo*:	**Gestión Editorial**
Funciones*:	Responsable de las obras, desde su ingreso hasta su publicación.
Obligaciones*:	Dar cumplimiento al acuerdo por el que se establecen los lineamientos para la protección de datos personales en posesión de la Universidad Nacional Autónoma de México.
(Nombre del Encargado 3*)	**MVZ Laura Edith Martínez Álvarez**

Cargo*:	**Gestión Editorial**
Funciones*:	Responsable de las obras, desde su ingreso hasta su publicación.
Obligaciones*:	Dar cumplimiento al acuerdo por el que se establecen los lineamientos para la protección de datos personales en posesión de la Universidad Nacional Autónoma de México.
(Nombre del Encargado 4*)	**MVZ Enrique Basurto Argueta**
Cargo*:	**Jefe del Departamento de Diseño Gráfico y Editorial**
Funciones*:	Formación y diseño editorial
Obligaciones*:	Dar cumplimiento al acuerdo por el que se establecen los lineamientos para la protección de datos personales en posesión de la Universidad Nacional Autónoma de México.
	Usuarios:
(Nombre del Usuario 1*)	**Mtra. Elizabeth Sarmiento de la Huerta**
Cargo*:	**Corrección de Estilo**
Funciones*:	Revisión del texto aprobado por el Comité Editorial y revisión de galeras.
Obligaciones*:	Dar cumplimiento al acuerdo por el que se establecen los lineamientos para la protección de datos personales en posesión de la Universidad Nacional Autónoma de México.
(Nombre del Usuario 2*)	**Alberto Fouilloux Morales** **Alejandro Cervantes Arias** **Eligio Gabriel Salgado Hernández** **Enrique Basurto Argueta** **Francisco Suárez Güemes** **Itzcóatl Felipe Aquino Díaz** **Javier Gutiérrez Molotla** **Jorge Hernández Espinosa** **José Angel Guadalupe Gutiérrez Pabello** **María de Guadalupe Ramírez Díaz** **Marina Guadalupe Tamara Guadarrama Olhovich** **Néstor Ledesma Martínez** **Orbelín Soberanis Ramos** **Victoria Yukie Tachika Ohara**
Cargo*:	**Comité Editorial**
Funciones*:	Son los responsables de dictaminar sobre las obras que se proponen para publicar en la Facultad de Medicina Veterinaria y Zootecnia, entre sus funciones se incluyen, pero no se limitan: Establecer los lineamientos para la selección de proyectos editoriales, tomando en consideración los objetivos de la Facultad de Medicina Veterinaria y Zootecnia, los factores de naturaleza académica, el mercado editorial, las necesidades de difusión y las disposiciones del Consejo Editorial de la UNAM. Autorizar la edición de libros, catálogos y otras publicaciones Autorizar las coediciones con instituciones y editoriales externas. Autorizar las colaboraciones en materia editorial con dependencias y entidades universitarias. Autorizar las reimpresiones y reediciones de las publicaciones que se encuentren agotadas o por agotarse.
Obligaciones*:	Dar cumplimiento al acuerdo por el que se establecen los lineamientos para la protección de datos personales en posesión de la Universidad Nacional Autónoma de México.
(Nombre del Usuario 3*)	**Firely Avril Braulio Ortiz** **Rosalinda Meza Contreras**

	Edgar Emmanuel Herrera López **Carlos Iván Sánchez Sánchez**
Cargo*:	**Diseñadores del Departamento de Diseño Gráfico y Editorial**
Funciones*:	Formación y diseño editorial
Obligaciones*:	Dar cumplimiento al acuerdo por el que se establecen los lineamientos para la protección de datos personales en posesión de la Universidad Nacional Autónoma de México.

Identificador único*	**FMVZ-SIS-030**
Nombre del sistema*	**Trámite ISBN**
Datos personales con justificación (sensibles o no) contenidos en el sistema*:	Nombre completo, fecha de nacimiento, lugar de nacimiento, RFC con homoclave, nacionalidad, domicilio completo, teléfono particular y para autores externos (no UNAM), se solicita INE o Pasaporte o un documento oficial de identidad de su país que sea claro el número de registro, nombre de la persona y nombre del documento.
	Responsables:
Nombre*:	Dr. Enrique Jesús Delgado Suárez
Cargo*:	**Jefe del Departamento de Publicaciones**
Funciones*:	Designación de las personas autorizadas para tener acceso a los datos personales de los autores.
Obligaciones*:	Dar cumplimiento al acuerdo por el que se establecen los lineamientos para la protección de datos personales en posesión de la Universidad Nacional Autónoma de México.
	Encargados:
Nombre del Encargado 1*	**MVZ Laura Martínez Álvarez**
Cargo*:	**Coordinadora editorial**
Funciones*:	Realiza las gestiones necesarias entre las diferentes instancias de la Dirección General de Asuntos Jurídicos, para el trámite de cesión de derechos a favor de la UNAM, registro y depósito de instrumentos jurídicos, gestión de ISBN y registro legal de obra, responsabilidades que se realizan en el área de publicaciones de la FMVZ-UNAM.
Obligaciones*:	Dar cumplimiento al acuerdo por el que se establecen los lineamientos para la protección de datos personales en posesión de la Universidad Nacional Autónoma de México.
Nombre del Encargado 2*	**MVZ. Silvia M. Ibáñez Zavala**
Cargo*:	**Coordinadora editorial**
Funciones*:	Realiza las gestiones necesarias entre las diferentes instancias de la Dirección General de Asuntos Jurídicos, para el trámite de cesión de derechos a favor de la UNAM, registro y depósito de instrumentos jurídicos, gestión de ISBN y registro legal de obra, responsabilidades que se realizan en el área de publicaciones de la FMVZ-UNAM.
Obligaciones*:	Dar cumplimiento al acuerdo por el que se establecen los lineamientos para la protección de datos personales en posesión de la Universidad Nacional Autónoma de México.
Usuarios:	Dirección General de Asuntos Jurídicos
Nombre del Encargado *	**Lic. Daniel Enrique Álvarez Ochoa**
Cargo*:	**Abogado** **Departamento de Derechos de Autor**

	DGAJ-UNAM
Funciones*:	Responsable de los trámites jurídicos necesarios para el “Registro Legal de Obra”
Obligaciones*:	Dar cumplimiento al acuerdo por el que se establecen los lineamientos para la protección de datos personales en posesión de la Universidad Nacional Autónoma de México.

Departamento de Medicina Preventiva y Salud Pública	
Identificador único*	**FMVZ-SIS-033**
Nombre del sistema*	**Laboratorio de Servicios**
Datos personales con justificación (sensibles o no) contenidos en el sistema*:	Datos: nombre (completo), domicilio (particular o empresa), número telefónico (empresarial o particular), correo electrónico, constancia de situación fiscal.
Responsable*:	**Departamento de Medicina Preventiva y Salud Pública (DMPSP)**
Nombre*:	**Juan Ramón Ayala Torres**
Cargo*:	**Jefe de Departamento / Responsable Administrativo de Sistemas**
Funciones*:	Establecer los alcances del Sistema de Gestión de Seguridad en el DMPSP, así como del personal insertado en el proceso. Supervisar el contenido y uso del sistema de tratamiento de datos personales, así como la finalidad en su uso.
Obligaciones*:	Dar cumplimiento en lo establecido en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, el Acuerdo por el que se establecen los Lineamientos para la Protección de Datos Personales en Posesión de la UNAM y las Normas Complementarias sobre Medidas de Seguridad Técnicas, Administrativas y Físicas para la Protección de Datos Personales en Posesión de la Universidad.
	Encargados:
Nombre del Encargado *	**José Antonio Romero López**
Cargo*:	**Encargado de Seguridad del DMPYSP**
Funciones*:	Colaborar como enlace entre el Departamento de Tecnología Educativa y el DMPSP
Obligaciones*:	Identificar los sistemas de tratamiento de activos de información, riesgos de vulneración, así como la interpretación del marco regulatorio, para la mitigación de amenaza inherente. Dar cumplimiento en lo establecido en: la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, el Acuerdo por el que se establecen los Lineamientos para la Protección de Datos Personales en Posesión de la UNAM y las Normas Complementarias sobre Medidas de Seguridad Técnicas, Administrativas y Físicas para la Protección de Datos Personales en Posesión de la Universidad.
Nombre del Encargado *	**Jocelin Ledesma López**
Cargo*:	**Encargada del Laboratorio de Servicios y calidad**
Funciones*:	Subir los datos personales sistema, en su caso modificación de datos de los clientes. Atender las necesidades administrativas del Laboratorio de Servicios del DMPSP, mediante el seguimiento en la captación, contención y el tratamiento de activos de información
Obligaciones*:	Implementar y mantener las medidas de seguridad para la mitigación de riesgo y protección de activos de información ante la eventualidad de vulneraciones, mediante el control de usuarios y sistemas de tratamiento de datos. Dar cumplimiento en lo

	establecido en: la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, el Acuerdo por el que se establecen los Lineamientos para la Protección de Datos Personales en Posesión de la UNAM y las Normas Complementarias sobre Medidas de Seguridad Técnicas, Administrativas y Físicas para la Protección de Datos Personales en Posesión de la Universidad.
	Usuarios:
(Nombre de Usuarios*)	**Claudia Alcázar Montañez** **Bertha Lucila Velázquez Camacho** **Rosa Helia Vite Pedroza**
Cargo*:	**Analistas**
Funciones*:	Consulta, resguardo y contención de datos, seguimiento del proceso analítico y emisión de formato de resultados
Obligaciones*:	Implementar y mantener las medidas de seguridad para la mitigación de riesgo y protección de activos de información ante la eventualidad de vulneraciones, mediante el control de usuarios y sistemas de tratamiento de datos. Dar cumplimiento en lo establecido en: la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, el Acuerdo por el que se establecen los Lineamientos para la Protección de Datos Personales en Posesión de la UNAM y las Normas Complementarias sobre Medidas de Seguridad Técnicas, Administrativas y Físicas para la Protección de Datos Personales en Posesión de la Universidad.
(Nombre del Usuario *)	**Trabajo Profesional** **Servicio Social (en turno)**
Cargo*:	**Apoyo**
Funciones*:	Personal de apoyo para la logística y seguimiento del proceso analítico, durante su Trabajo Profesional o SS
Obligaciones*:	Implementar y mantener las medidas de seguridad para la mitigación de riesgo y protección de activos de información ante la eventualidad de vulneraciones, mediante el control de usuarios y sistemas de tratamiento de datos. Dar cumplimiento en lo establecido en: la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, el Acuerdo por el que se establecen los Lineamientos para la Protección de Datos Personales en Posesión de la UNAM y las Normas Complementarias sobre Medidas de Seguridad Técnicas, Administrativas y Físicas para la Protección de Datos Personales en Posesión de la Universidad.

Identificador único*	**FMVZ-SIS-041**
Nombre del sistema*	**Laboratorio de Investigación**
Datos personales con justificación (sensibles o no) contenidos en el sistema*:	Datos: nombre (completo), número telefónico (institucional/particular/celular), correo electrónico, firma.
Responsable*:	**Departamento de Medicina Preventiva y Salud Pública (DMPSP)**
Nombre*:	**Juan Ramón Ayala Torres**
Cargo*:	**Jefe de Departamento / Responsable Administrativo de Sistemas**
Funciones*:	Establecer los alcances del Sistema de Gestión de Seguridad en

	el DMPSP, así como del personal insertado en el proceso. Supervisar el contenido y uso del sistema de tratamiento de datos personales, así como la finalidad en su uso.
Obligaciones*:	Dar cumplimiento en lo establecido en: la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, el Acuerdo por el que se establecen los Lineamientos para la Protección de Datos Personales en Posesión de la UNAM y las Normas Complementarias sobre Medidas de Seguridad Técnicas, Administrativas y Físicas para la Protección de Datos Personales en Posesión de la Universidad
	Encargados:
Nombre del Encargado *	**José Antonio Romero López**
Cargo*:	**Encargado de Seguridad del DMPYSP**
Funciones*:	Colaborar como enlace entre el Departamento de Tecnología Educativa y el DMPSP
Obligaciones*:	Identificar los sistemas de tratamiento de activos de información, riesgos de vulneración, así como la interpretación del marco regulatorio, para la mitigación de amenaza inherente. Dar cumplimiento en lo establecido en: la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, el Acuerdo por el que se establecen los Lineamientos para la Protección de Datos Personales en Posesión de la UNAM y las Normas Complementarias sobre Medidas de Seguridad Técnicas, Administrativas y Físicas para la Protección de Datos Personales en Posesión de la Universidad.
(Nombre del Encargado 2*)	**Enrique Jesús Delgado Suárez**
Cargo*:	**Encargado del Laboratorio de Investigación**
Funciones*:	Atender y coordinar las necesidades de investigación de la FMVZ mediante la infraestructura del Laboratorio de Investigación del DMPSP, procurando la supervisión para la mitigación de riesgo en los sistemas de tratamiento de activos de información
Obligaciones*:	Implementar y mantener las medidas de seguridad para la mitigación de riesgo y protección de activos de información ante la eventualidad de vulneraciones, mediante el control de usuarios y sistemas de tratamiento de datos. Dar cumplimiento en lo establecido en: la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, el Acuerdo por el que se establecen los Lineamientos para la Protección de Datos Personales en Posesión de la UNAM y las Normas Complementarias sobre Medidas de Seguridad Técnicas, Administrativas y Físicas para la Protección de Datos Personales en Posesión de la Universidad.
(Nombre del Encargado 3*)	**Luz Del Carmen Sierra Gómez Pedroso**
Cargo*:	**Encargada del Laboratorio de Investigación**
Funciones*:	Atender las necesidades administrativas del Laboratorio de Servicios del DMPSP, gestionando el seguimiento en la captación, contención y el tratamiento de activos de información.
Obligaciones*:	Implementar y mantener las medidas de seguridad para la mitigación de riesgo y protección de activos de información ante la eventualidad de vulneraciones, mediante el control de usuarios y sistemas de tratamiento de datos. Dar cumplimiento en lo establecido en: la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, el Acuerdo por el que se establecen los Lineamientos para la Protección de Datos Personales en Posesión de la UNAM y las Normas

	Complementarias sobre Medidas de Seguridad Técnicas, Administrativas y Físicas para la Protección de Datos Personales en Posesión de la Universidad.
	Usuarios:
(Nombre del Usuario 1*)	Este sistema no requiere de usuarios para su funcionamiento

Secretaría General de la FMVZ	
Identificador único*	**FMVZ-SIS-009**
Nombre del sistema*	**Control de asistencias**
Datos personales con justificación (sensibles o no) contenidos en el sistema*:	Nombre, Nombramiento o cargo, No. de trabajador, Área de adscripción, RFC.
Responsable*:	**Secretaría General de la Facultad de Medicina Veterinaria y Zootecnia**
Nombre*:	**Dr. Jorge Hernández Espinosa**
Cargo*:	**Secretario General**
Funciones*:	Decidir sobre el alcance, contenido y tratamiento de los datos personales y uso del sistema.
Obligaciones*:	Las establecidas en los Lineamientos para la Protección de Datos Personales en posesión de la UNAM para responsables del tratamiento de datos personales en las áreas universitarias.
	Encargados:
Nombre del Encargado *	**Mario Arturo Rodríguez Mendoza**
Cargo*:	**Encargado de Seguridad de datos en la Secretaría General.**
Funciones*:	Capacitar y compartir a los usuarios del sistema información sobre las normativas vigentes en materia de protección de datos personales.
Obligaciones*:	Procurar la protección de datos personales contenidos en el sistema mediante la implementación de estrategias y mecanismos de seguridad en su desarrollo y mantenimiento.
	Usuarios:
(Nombre del Usuario 1*)	**Gabriel Pantoja Medina**
Cargo*:	**Colaborador de la Secretaría General**
Funciones*:	Supervisión de la información recabada por el sistema durante el semestre para realizar el análisis de cumplimiento de asistencias. Brindar seguimiento a la solicitud de información por parte de los interesados.
Obligaciones*:	Procurar la privacidad de los datos personales a los que accede mediante el uso del sistema.

Identificador único*	**FMVZ-SIS-012**
Nombre del sistema*	**Comisiones FMVZ**
Datos personales con justificación (sensibles o no) contenidos en el sistema*:	Nombre, edad, RFC, CURP, nacionalidad, fecha de nacimiento, idiomas, correo electrónico, estado civil, nombramiento académico, formación académica, correo institucional, capacitación, títulos, cédula profesional, certificados, reconocimientos, trayectoria académica, promociones, estímulos, sanciones, firmas.

Responsable*:	**Secretaría General de la Facultad de Medicina Veterinaria y Zootecnia**
Nombre*:	**Dr. Jorge Hernández Espinosa**
Cargo*:	**Secretario General**
Funciones*:	Decidir sobre el alcance, contenido y tratamiento de los datos personales y uso del sistema.
Obligaciones*:	Las establecidas en los Lineamientos para la Protección de Datos Personales en posesión de la UNAM para responsables del tratamiento de datos personales en las áreas universitarias.
	Encargados:
Nombre del Encargado *	**Mario Arturo Rodríguez Mendoza**
Cargo*:	**Encargado de Seguridad de datos en la Secretaría General.**
Funciones*:	Capacitar y compartir a los usuarios del sistema información sobre las normativas vigentes en materia de protección de datos personales.
Obligaciones*:	Procurar la protección de datos personales contenidos en el sistema mediante la implementación de estrategias y mecanismos de seguridad en su desarrollo y mantenimiento.
Nombre del Encargado *	**María Magdalena Escamilla Guerrero**
Cargo*:	**Jefa del Departamento de Asuntos del Personal Académico de la FMVZ**
Funciones*:	Solicitar el acceso al sistema de los nuevos integrantes de las Comisiones. Recabar y resguardar cartas de confidencialidad de los integrantes de las Comisiones. Subir información al sistema.
Obligaciones*:	Procurar la protección de datos contenidos en el sistema mediante la implementación de estrategias y mecanismos de seguridad.
Nombre del Encargado *	**Laura Méndez Olvera**
Cargo*:	**Colaboradora de la Secretaría General**
Funciones*:	Subir información al sistema. Recabar firmas.
Obligaciones*:	Procurar la privacidad de los datos personales a los que accede mediante el uso del sistema.
Nombre del Encargado *	**Cinthia Monserrat Godínez Ramírez**
Cargo*:	**Colaboradora de la Secretaría General**
Funciones*:	Subir información al sistema. Recabar firmas.
Obligaciones*:	Procurar la privacidad de los datos personales a los que accede mediante el uso del sistema.
	Usuarios:
(Nombre del Usuario 1*)	**(Anexo 1)**
Cargo*:	**Integrantes de Comisiones del H. Consejo Técnico de la Facultad de Medicina Veterinaria y Zootecnia.**
Funciones*:	Revisar y dictaminar la información que le proporciona el sistema.
Obligaciones*:	Resguardar sus claves de acceso al sistema. Procurar la privacidad de los datos personales a los que accede y no compartir con nadie ajeno a los Cuerpos Colegiados.
(Nombre del Usuario 2*)	**(Anexo 2)**
Cargo*:	**Integrantes de Comisiones dictaminadoras en la Facultad de Medicina Veterinaria y Zootecnia.**
Funciones*:	Revisar y dictaminar la información que le proporciona el sistema.
Obligaciones*:	Resguardar sus claves de acceso al sistema. Procurar la privacidad de los datos personales a los que accede y no compartir con nadie ajeno a la Comisión a la que pertenece.

Identificador único*	**FMVZ-SIS-022**
Nombre del sistema*	**Contrataciones FMVZ**
Datos personales con justificación (sensibles o no) contenidos en el sistema*:	Nombre, Domicilio, Teléfono de casa, Teléfono celular, correo electrónico, estado civil, firma, RFC, CURP, lugar y fecha de nacimiento, nacionalidad, edad, nombre de familiares, dependientes económicos, beneficiarios de prestaciones, fotografía, situación migratoria. Nombramiento académico, puesto o cargo, área de adscripción, correo institucional, teléfono institucional, promociones, estímulos, licencias, antigüedad, bajas. Ingresos, cuentas bancarias, seguro de vida institucional, pago de marcha, modalidad de pago. Trayectoria educativa, títulos, cédulas profesionales, certificados, reconocimientos, capacitaciones. Otros empleos.
Responsable*:	**Secretaría General de la Facultad de Medicina Veterinaria y Zootecnia**
Nombre*:	**Dr. Jorge Hernández Espinosa**
Cargo*:	**Secretario General**
Funciones*:	Decidir sobre el alcance, contenido y tratamiento de los datos personales y uso del sistema.
Obligaciones*:	Las establecidas en los Lineamientos para la Protección de Datos Personales en posesión de la UNAM para responsables del tratamiento de datos personales en las áreas universitarias.
	Encargados:
Nombre del Encargado *	**Mario Arturo Rodríguez Mendoza**
Cargo*:	**Encargado de Seguridad de datos en la Secretaría General.**
Funciones*:	Capacitar y compartir a los usuarios del sistema información sobre las normativas vigentes en materia de protección de datos personales.
Obligaciones*:	Procurar la protección de datos personales contenidos en el sistema mediante la implementación de estrategias y mecanismos de seguridad en su desarrollo y mantenimiento.
	Usuarios:
(Nombre del Usuario 1*)	**Elia Lizeth Espinosa Rodríguez**
Cargo*:	**Colaboradora de la Secretaría General**
Funciones*:	Recabar información y subirla al sistema. Recabar firmas.
Obligaciones*:	Procurar la privacidad de los datos personales a los que accede mediante el uso del sistema.
(Nombre del Usuario 2*)	**Gabriel Pantoja Medina**
Cargo*:	**Colaborador de la Secretaría General**
Funciones*:	Recabar información y subirla al sistema. Recabar firmas.
Obligaciones*:	Procurar la privacidad de los datos personales a los que accede mediante el uso del sistema.
(Nombre del Usuario 3*)	**Mario Arturo Rodríguez Mendoza**
Cargo*:	**Colaborador de la Secretaría General**
Funciones*:	Recabar información y subirla al sistema. Recabar firmas.
Obligaciones*:	Procurar la privacidad de los datos personales a los que accede mediante el uso del sistema.

Identificador único*	**FMVZ-SIS-046**
Nombre del sistema*	**Permisos**
Datos personales con justificación (sensibles o no) contenidos en el sistema*:	Nombre, RFC, correo electrónico, nombre del jefe de área, correo del jefe de área, fechas solicitadas, motivo del permiso.
Responsable*:	**Secretaría General de la Facultad de Medicina Veterinaria y Zootecnia**
Nombre*:	**Dr. Jorge Hernández Espinosa**
Cargo*:	**Secretario General**
Funciones*:	Decidir sobre el alcance, contenido y tratamiento de los datos personales y uso del sistema.
Obligaciones*:	Las establecidas en los Lineamientos para la Protección de Datos Personales en posesión de la UNAM para responsables del tratamiento de datos personales en las áreas universitarias.
	Encargados:
Nombre del Encargado *	**Mario Arturo Rodríguez Mendoza**
Cargo*:	**Encargado de Seguridad de datos en la Secretaría General.**
Funciones*:	Capacitar y compartir a los usuarios del sistema información sobre las normativas vigentes en materia de protección de datos personales.
Obligaciones*:	Procurar la protección de datos personales contenidos en el sistema mediante la implementación de estrategias y mecanismos de seguridad en su desarrollo y mantenimiento.
	Usuarios:
(Nombre del Usuario 1*)	**Elia Lizeth Espinosa Rodríguez**
Cargo*:	**Colaboradora de la Secretaría General**
Funciones*:	Revisar y elaborar reportes del sistema. Cargar información.
Obligaciones*:	Procurar la privacidad de los datos personales a los que accede mediante el uso del sistema.
(Nombre del Usuario 2*)	**Gabriel Pantoja Medina**
Cargo*:	**Colaborador de la Secretaría General**
Funciones*:	Cargar información.
Obligaciones*:	Procurar la privacidad de los datos personales a los que accede mediante el uso del sistema.
(Nombre del Usuario 3*)	**Mario Arturo Rodríguez Mendoza**
Cargo*:	**Colaborador de la Secretaría General**
Funciones*:	Cargar información.
Obligaciones*:	Procurar la privacidad de los datos personales a los que accede mediante el uso del sistema.

Secretaria De Atención A La Comunidad	
Identificador único*	**FMVZ-SIS-049**
Nombre del sistema*	**SEGUIMIENTO DE EGRESADOS**
Datos personales con justificación (sensibles o no) contenidos en el sistema*:	Nombre, correo, teléfono de casa, teléfono personal y de trabajo, datos patrimoniales
Responsable*:	**Secretaría De Atención A La Comunidad**
Nombre*:	**LILIANA VALDÉS VÁZQUEZ**

Cargo*:	**SECRETARIA DE ATENCIÓN A LA COMUNIDAD**
Funciones*:	Fijar el alcance del sistema, dar cumplimiento con las normas complementarias sobre medidas de seguridad técnica, administrativas y físicas, para la protección de datos personales en posesión de la Universidad.
Obligaciones*:	Garantizar que se dé el cumplimiento con las normas complementaria sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la Universidad.
	Encargados:
Nombre del Encargado *	**Marcella Altamirano Quintana**
Cargo*:	**Jefa del Departamento del Seguimiento a Egresados**
Funciones*:	Realizar llamadas de manera personal para localizar al egresado y/o al empleador para enviar del formulario correspondiente para la obtención de datos solicitados.
Obligaciones*:	Mantener los datos protegidos como lo menciona las normas complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la Universidad.
	Usuarios:
NOTA*	Por necesidades del sistema éste no cuenta con usuarios

Departamento de Economía, Administración y Desarrollo rural – DEADR.	
Identificador único*	**FMVZ-SIS-058**
Nombre del sistema*	**Proyecto – CONACYT. "*Desarrollo de estrategias participativas para el fortalecimiento de redes de producción y consumo de productos lácteos tradicionales orientados a la soberanía alimentaria de territorios del centro-occidente de México".***
Datos personales con justificación (sensibles o no) contenidos en el sistema*:	Nombres, teléfonos, correos electrónicos.
Responsable*:	Responsable principal del proyecto CONACYT.
Nombre*:	**Randy Alexis Jiménez Jiménez.**
Cargo*:	**Responsable Administrativo del Sistema.**
Funciones*:	Delimitar el alcance de los procesos, asignar roles de responsables o encargados.
Obligaciones*:	Cumplir con lo determinado en las normas complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la universidad.
Nombre de Encargados*	**CHÁVEZ PÉREZ LUIS MANUEL** **ESPINOSA ORTIZ VALENTIN** **GIL GONZÁLEZ GRETEL ILIANA** **GÓMEZ ESPINOSA GUILLERMO** **MIGUEL ESTRADA MAURICIO** **RENDÓN RENDÓN MARIA CAMILA**
Cargos*:	**Investigadores asociados.**
Funciones*:	Obtención y resguardo de los datos dentro del Departamento de

	Economía, Administración y Desarrollo Rural.
Obligaciones*:	Cumplir con lo determinado en las normas complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la universidad.
Nombre de Encargados*	**CALÓNICO CASTRO TALIA** **CRUZ VERGARA BEATRIZ**
Cargos*:	**Ayudantes de profesor.**
Funciones*:	Obtención y resguardo de los datos dentro del Departamento de Economía, Administración y Desarrollo Rural.
Obligaciones*:	Cumplir con lo determinado en las normas complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la universidad.
	USUARIO
Nombre del Usuario*	**SERVICIO SOCIAL EN TURNO**
Cargo*:	**Servicio social.**
Funciones*:	Apoyo en las actividades relacionadas a los datos dentro del Departamento de Economía, Administración y Desarrollo Rural.
Obligaciones*:	Cumplir con lo determinado en las normas complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la universidad.

Identificador único*	**FMVZ-SIS-085**
Nombre del sistema*	**Proyecto – SSAFE - IICA**
Datos personales con justificación (sensibles o no) contenidos en el sistema*:	Nombres, direcciones, CURP's - copias de INE, correos electrónicos y teléfonos.
Responsable*:	Jefe del departamento de Economía, Administración y Desarrollo Rural.
Nombre*:	**José Luis Dávalos Flores**
Cargo*:	**Responsable Administrativo de Sistemas**
Funciones*:	Delimitar el alcance de los procesos, asignar roles de responsables o encargados.
Obligaciones*:	Cumplir con lo determinado en las normas complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la universidad.
Nombre del Encargado *	**Lidia Boleaga Rivera**
Cargo*:	**Responsable de la seguridad de la información.**
Funciones*:	Obtención y resguardo de los datos dentro del Departamento de Economía, Administración y Desarrollo Rural.
Obligaciones*:	Cumplir con lo determinado en las normas complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la universidad.
(Nota: Por cuestiones de este proceso no se cuenta con usuarios.)	

Identificador único*	**FMVZ-SIS-086**
Nombre del sistema*	**Proyecto – MARGARITA**
Datos personales con justificación (sensibles o no) contenidos en el sistema*:	Nombres, direcciones, CURP's - copias de INE, correos electrónicos y teléfonos.
Responsable*:	Jefe del departamento de Economía, Administración y Desarrollo Rural.
Nombre*:	**José Luis Dávalos Flores**
Cargo*:	**Responsable Administrativo de Sistemas**
Funciones*:	Delimitar el alcance de los procesos, asignar roles de responsables o encargados.
Obligaciones*:	Cumplir con lo determinado en las normas complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la universidad.
Nombre del Encargado *	**Lidia Boleaga Rivera**
Cargo*:	**Responsable de la seguridad de la información.**
Funciones*:	Obtención y resguardo de los datos dentro del Departamento de Economía, Administración y Desarrollo Rural.
Obligaciones*:	Cumplir con lo determinado en las normas complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la universidad.
(Nota: Por cuestiones de este proceso no se cuenta con usuarios.)	

Biblioteca "MV José de la Luz Gómez"	
Identificador único*	**FMVZ-SIS-011**
Nombre del sistema*	**Aleph, sistema de bibliotecas para el registro de usuarios que requieran acceso a los servicios de biblioteca**
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre, teléfono, cuenta de correo electrónico, domicilio, fotografía, número de cuenta
Responsable*:	
Nombre*:	**Saúl Acuña Paredes**
Cargo*:	**Coordinador de biblioteca**
Funciones*:	Apoyo con las medidas técnicas de seguridad establecidas en las Normas complementarias sobre medidas de Seguridad Técnica, Administrativa y Física para Protección de datos personales en posesión de la Universidad
Obligaciones*:	Dar cumplimiento con lo establecido en las Normas Complementarias sobre medidas de Seguridad Técnica, Administrativas y Físicas para la protección de datos personales en posesión de la Universidad
	Encargados:

Nombre del Encargado *	**José Iván López Pelcastre**
Cargo*:	**Responsable técnico**
Funciones*:	Apoyo con las medidas técnicas de seguridad establecidas en las Normas complementarias sobre medidas de Seguridad Técnica, Administrativa y Física para Protección de datos personales en posesión de la Universidad
Obligaciones*:	Dar cumplimiento con lo establecido en las Normas Complementarias sobre medidas de Seguridad Técnica, Administrativas y Físicas para la protección de datos personales en posesión de la Universidad
(Nombre del Encargado 2*)	**Dirección General de Bibliotecas y Sistemas Digitales de Información (DGBSDI)**
Cargo*:	**Responsables Técnico, Físico y Administrativos**
Funciones*:	Apoyo con las medidas técnicas de seguridad establecidas en las Normas complementarias sobre medidas de Seguridad Técnica, Administrativa y Física para Protección de datos personales en posesión de la Universidad
Obligaciones*:	Dar cumplimiento con lo establecido en las Normas Complementarias sobre medidas de Seguridad Técnica, Administrativas y Físicas para la protección de datos personales en posesión de la Universidad
(Nombre del Encargado 3*)	**Elisa López López**
Cargo*:	**Responsable de área**
Funciones*:	Apoyo con las medidas técnicas de seguridad establecidas en las Normas complementarias sobre medidas de Seguridad Técnica, Administrativa y Física para Protección de datos personales en posesión de la Universidad
Obligaciones*:	Dar cumplimiento con lo establecido en las Normas Complementarias sobre medidas de Seguridad Técnica, Administrativas y Físicas para la protección de datos personales en posesión de la Universidad
(Nombre del Encargado 4*)	**Fabiola Martínez Orobio**
Cargo*:	**Bibliotecario**
Funciones*:	Apoyo con las medidas técnicas de seguridad establecidas en las Normas complementarias sobre medidas de Seguridad Técnica, Administrativa y Física para Protección de datos personales en posesión de la Universidad
Obligaciones*:	Dar cumplimiento con lo establecido en las Normas Complementarias sobre medidas de Seguridad Técnica, Administrativas y Físicas para la protección de datos personales en posesión de la Universidad
	Usuarios:
(Nombre del Usuario 1*)	**Arturo Durazno López, Pedro Luis López Vargas, María Lourdes Mendoza Aguilar, Miriam Mendoza Aguilar, Omar Palacios López, María del Rocío Palomino Ruiz, Mauricio Tonatiuh Pérez Torres**
Cargo*:	**Bibliotecarios**

Funciones*:	Apoyo con las medidas técnicas de seguridad establecidas en las Normas complementarias sobre medidas de Seguridad Técnica, Administrativa y Física para Protección de datos personales en posesión de la Universidad
Obligaciones*:	Dar cumplimiento con lo establecido en las Normas Complementarias sobre medidas de Seguridad Técnica, Administrativas y Físicas para la protección de datos personales en posesión de la Universidad
(Nombre del Usuario 2*)	**Luz Adriana Roldán García, Margarita Sánchez Martínez, Manuela Legaría García, Gerardo Núñez Núñez, José Luis Olivares Villagran, Luis Antonio Alquicira, Guadalupe Díaz García, Israel Fabián Montaño Sternenfels, José Valderrama García, Eduardo Vázquez Fuentes, María Sánchez Arzate, Jovita Carrillo Vázquez**
Cargo*:	**Bibliotecarios**
Funciones*:	Apoyo con las medidas técnicas de seguridad establecidas en las Normas complementarias sobre medidas de Seguridad Técnica, Administrativa y Física para Protección de datos personales en posesión de la Universidad
Obligaciones*:	Dar cumplimiento con lo establecido en las Normas Complementarias sobre medidas de Seguridad Técnica, Administrativas y Físicas para la protección de datos personales en posesión de la Universidad
(Nombre del Usuario 3*)	**Alejandro Noriega Morales, María Teresa Pedraza Saldivar, Adriana Rosas Lazcano, Felipe Guzmán Galicia, Gerardo Núñez Núñez**
Cargo*:	**Bibliotecarios**
Funciones*:	Apoyo con las medidas técnicas de seguridad establecidas en las Normas complementarias sobre medidas de Seguridad Técnica, Administrativa y Física para Protección de datos personales en posesión de la Universidad
Obligaciones*:	Dar cumplimiento con lo establecido en las Normas Complementarias sobre medidas de Seguridad Técnica, Administrativas y Físicas para la protección de datos personales en posesión de la Universidad
Identificador único*	**FMVZ-SIS-088**
Nombre del sistema*	**Bidi Unam, sistema de Acceso Remoto**
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre, número de cuenta, cuenta de correo electrónico, edad, número de cuenta
Responsable*:	
Nombre*:	**Saúl Acuña Paredes**
Cargo*:	**Coordinador de biblioteca**
Funciones*:	Apoyo con las medidas técnicas de seguridad establecidas en las Normas complementarias sobre medidas de Seguridad Técnica, Administrativa y Física para Protección de datos personales en posesión de la Universidad

Obligaciones*:	Dar cumplimiento con lo establecido en las Normas Complementarias sobre medidas de Seguridad Técnica, Administrativas y Físicas para la protección de datos personales en posesión de la Universidad
	Encargados:
Nombre del Encargado *	**Dirección General de Bibliotecas y Sistemas Digitales de Información (DGBSDI)**
Cargo*:	**Responsables Técnico, Físico y Administrativos**
Funciones*:	Apoyo con las medidas técnicas de seguridad establecidas en las Normas complementarias sobre medidas de Seguridad Técnica, Administrativa y Física para Protección de datos personales en posesión de la Universidad
Obligaciones*:	Dar cumplimiento con lo establecido en las Normas Complementarias sobre medidas de Seguridad Técnica, Administrativas y Físicas para la protección de datos personales en posesión de la Universidad
(Nombre del Encargado 2*)	**Ana María Román de Carlos**
Cargo*:	**Responsable de área**
Funciones*:	Apoyo con las medidas técnicas de seguridad establecidas en las Normas complementarias sobre medidas de Seguridad Técnica, Administrativa y Física para Protección de datos personales en posesión de la Universidad
Obligaciones*:	Dar cumplimiento con lo establecido en las Normas Complementarias sobre medidas de Seguridad Técnica, Administrativas y Físicas para la protección de datos personales en posesión de la Universidad
(Nombre del Encargado 2*)	**Cristian López Montelongo**
Cargo*:	**Técnico académico**
Funciones*:	Apoyo con las medidas técnicas de seguridad establecidas en las Normas complementarias sobre medidas de Seguridad Técnica, Administrativa y Física para Protección de datos personales en posesión de la Universidad
Obligaciones*:	Dar cumplimiento con lo establecido en las Normas Complementarias sobre medidas de Seguridad Técnica, Administrativas y Físicas para la protección de datos personales en posesión de la Universidad
	Usuarios:
NOTA	Por cuestiones de éste sistema, no se cuenta con usuarios

Departamento de Tecnología Educativa	
Identificador único*	**FMVZ-SIS-030**
(Nombre del sistema A1) *	**INTRANET (intranet2.fmvz.unam.mx)**
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre, Número cuenta, huella digital.
Responsable*:	
Nombre*:	**Eric Martínez Paredes**
Cargo*:	**Responsable de Sistema del DTE**
Funciones*:	Establecer el alcance del sistema
Obligaciones*:	Cumplir con lo establecido en los Lineamientos y en las Normas Complementarias a nivel Administrativo, Técnico y Físicas para la protección de datos personales en posesión de la UNAM.
	Encargados:
(Nombre del Encargado 1*)	**Miguel Angel Sandoval Texcahuac,** **José Iván López Pelcastre** **Erick Reyes Hernández**
Cargo*:	**Encargados de Sistemas**
Funciones*:	Subir Base de datos de los alumnos de cada generación. Registro de huella y consentimiento de alumno y creación de Usuarios en el Sistema
Obligaciones*:	Mantener sin cambios los mismos, así como proteger y dar cumplimiento a lo establecido en los Lineamientos y en las Normas Complementarias a nivel Técnico para la protección de datos personales en posesión de la UNAM
(Nombre del Encargado 2*)	**José Iván López Pelcastre**
Cargo*:	**Encargado de Seguridad Técnica**
Funciones*:	Cumplir con las medidas técnicas en materia de seguridad de datos personales en los sistemas alojados en los servidores de la DTE
Obligaciones*:	Dar cumplimiento a lo establecido en los Lineamientos y en las Normas Complementarias a nivel Técnico para la protección de datos personales en posesión de la UNAM
(Nombre del Encargado 3*)	**Alicia Vergara Zavala**
Cargo*:	**Encargada de datos personales**
Funciones*:	Apoyo técnico en registro de huella y consentimiento de alumnos.
Obligaciones*:	Mantener sin cambios los mismos, así como proteger y dar cumplimiento a lo establecido en los Lineamientos y en las Normas Complementarias a nivel Técnico para la protección de datos personales en posesión de la UNAM
Usuarios:	
(Nombre del Usuario 1*)	**Alma Julieta Martínez Santillán** **Ignacio Díaz Sevilla** **José Víctor González Moreno**

	Luis Alberto Gutiérrez Mendoza **María Isabel Oropeza Aguilar** **Erick Reyes Hernández** **Alicia Vergara Zavala** **Miguel Ángel Sandoval Texcahuac** **Eric Martínez Paredes** **Myriam Beltrán Zavaleta** **Álvaro Joaquín Ruiz Chora** **Y encargados de laboratorios de cómputo de la FMVZ**
Cargo*:	Registro
Funciones*:	Realizar el registro de alumno y asociarlo a un equipo para préstamo
Obligaciones*:	Dar cumplimiento a lo establecido en los Lineamientos y en las Normas Complementarias a nivel Técnico para la protección de datos personales en posesión de la UNAM

Identificador único*	**FMVZ-SIS-049**
Sistema (Nombre del A2)*:	**Sistema de autenticación para WiFi (iyari.fmvz.unam.mx)**
Datos personales contenidos en el sistema*:	Nombre, No de cuenta, No de trabajador, RFC.
Responsable:	**Departamento de Tecnología Educativa**
Nombre*:	**Eric Martínez Paredes**
Cargo*:	**Responsable de Sistema del DTE**
Funciones*:	Establecer el alcance del sistema
Obligaciones*:	Cumplir con lo establecido en los Lineamientos y en las Normas Complementarias a nivel Administrativo, Técnico y Físicas para la protección de datos personales en posesión de la UNAM.
	Encargados:
(Nombre del Encargado 1*)	**José Iván López Pelcastre**
Cargo*:	**Encargado de Seguridad Técnica**
Funciones*:	Cumplir con las medidas técnicas en materia de seguridad de datos personales en los sistemas alojados en los servidores de la DTE
Obligaciones*:	Dar cumplimiento a lo establecido en los Lineamientos y en las Normas Complementarias a nivel Técnico para la protección de datos personales en posesión de la UNAM
(Nombre del Encargado 2*)	**Eric Martínez Paredes** **Erick Reyes Hernández** **María Isabel Oropeza Aguilar** **Miguel Ángel Sandoval Texahuac**
Cargo*:	**Encargado de Seguridad de Datos Personales**
Funciones*:	Administrar (Crear, modificar y eliminar) usuarios
Obligaciones*:	Mantener sin cambios los mismos, así como proteger y dar cumplimiento a lo establecido en los Lineamientos y en las Normas Complementarias a nivel Técnico para la protección de datos personales en posesión de la UNAM

Usuarios:	**N/A**

Identificador único*	**FMVZ-SIS-010**
Sistema (Nombre del A3)*:	**Plataformas Moodle (aulavirual.fmvz.unam.mx; examenes3.fmvz.unam.mx; fmvzenlinea2-7.fmvz.unam.mx)**
Datos personales contenidos en el sistema*:	Nombre, No. de cuenta, correo.
Responsable:	**Departamento de Tecnología Educativa**
Nombre*:	**Eric Martínez Paredes**
Cargo*:	**Responsable de Sistema del DTE**
Funciones*:	Establecer el alcance del sistema
Obligaciones*:	Cumplir con lo establecido en los Lineamientos y en las Normas Complementarias a nivel Administrativo, Técnico y Físicas para la protección de datos personales en posesión de la UNAM.
	Encargados:
(Nombre del Encargado 1*)	**José Iván López Pelcastre**
Cargo*:	**Encargado de Seguridad Técnica**
Funciones*:	Cumplir con las medidas técnicas en materia de seguridad de datos personales en los sistemas alojados en los servidores de la DTE
Obligaciones*:	Mantener sin cambios los datos, así como proteger y dar cumplimiento a lo establecido en los Lineamientos y en las Normas Complementarias a nivel Técnico para la protección de datos personales en posesión de la UNAM
(Nombre del Encargado 2*)	**María Isabel Oropeza Aguilar**
Cargo*:	Encargada de Datos Personales
Funciones*:	Cargar bases de datos a los Programas Actualización de datos en caso de ser solicitado, así como las contraseñas.
Obligaciones*:	Mantener sin cambios los datos, así como proteger y dar cumplimiento a lo establecido en los Lineamientos y en las Normas Complementarias a nivel Técnico para la protección de datos personales en posesión de la UNAM
(Encargados 3*)	**Miguel Ángel Sandoval Texcahuac** **Eric Martínez Paredes** **Erick Reyes Hernández** **Alicia Vergara Zavala** **María Isabel Oropeza Aguilar** **Álvaro Joaquín Ruiz Chora**
Cargo*:	Consulta y Cambio de contraseña
Funciones*:	Crear cuentas de alumnos que por alguna razón no se encuentran en la base de datos y consultar cambios de contraseña
Obligaciones*:	Dar cumplimiento a lo establecido en los Lineamientos y en las Normas Complementarias a nivel Técnico para la protección de datos personales en posesión de la UNAM

	Usuarios:
(Nombre del Usuario 1*)	**Comunidad académica de la FMVZ**
Cargo*:	Registro
Funciones*:	Crear cuentas de alumnos que por alguna razón no se encuentran en la base de datos
Obligaciones*:	Dar cumplimiento a lo establecido en los Lineamientos y en las Normas Complementarias a nivel Técnico para la protección de datos personales en posesión de la UNAM
(Nombre del Usuario 3*)	**Erick Reyes Hernández**
Cargo*:	Registro
Funciones*:	Cambios de Contraseñas
Obligaciones*:	Dar cumplimiento a lo establecido en los Lineamientos y en las Normas Complementarias a nivel Técnico para la protección de datos personales en posesión de la UNAM

División de Estudios Profesionales	
Identificador único*	**FMVZ-SIS-071**
Nombre del sistema*	**SITEA-SISTEMA DE TRAYECTORIA ESCOLAR DE ALUMNOS**
Datos personales con justificación (sensibles o no) contenidos en el sistema*:	**Alumnos** Número de cuenta Nombre alumno Curp Año de ingreso Lugar Nacimiento Fecha nacimiento Nacionalidad Domicilio Calle y No Col. o población C.P. Delelg. o munic Estado Lada Teléfono casa Celular Lada trabajo Teléfono trabajo Lada familiar Teléfono familiar Correo electrónico 1 Correo electrónico 2 Teléfono para informar en caso de emergencias Grupo sanguíneo Generación Créditos cursados Promedio Modalidad de titulación Situación de titulación Calificaciones del examen de ingles

	RFC Homo clave Curp Nombre del profesores Sexo Número de Trabajador Correo electrónico Nombramientos Departamento asignado Historia Académica Completa Alumno Avance en créditos
Responsable administrativo*	**Laura P. Romero Romero**
Nombre*:	Laura Patricia Romero Romero
Cargo*:	Jefa de la División de Estudios Profesionales
Funciones*:	Supervisar y controlar los procesos administrativos escolares, para procurar el buen uso de los datos
Obligaciones*:	• Vigilar el cumplimiento de las disposiciones contenidas en la Legislación Universitaria, así como de los reglamentos internos de la Facultad. • Planear, organizar, dirigir, controlar y supervisar los procesos de administración escolar • Designación de encargados del sistema • Verificar que cumplan con los lineamientos y Normas Complementarias sobre medidas de seguridad técnica, administrativas y físicas para la protección de datos personales en posesión de la Universidad
Responsable técnico1 *	**Jesús Peña Delgadillo**
Nombre*:	**Jesús Peña Delgadillo**
Cargo*:	Técnico académico
Funciones*:	Uso de los datos con fines estadísticos Resguardar los datos personales
Obligaciones*:	Cumplir con lo establecido en los lineamientos y en las Normas Complementarias correspondientes al área técnica
Responsable técnico2 *	**Claudia Fernanda Landa Vargas**
Nombre*:	**Claudia Fernanda Landa Vargas**
Cargo*:	Secretaria de Asuntos Escolares
Funciones*:	Administrador de BD Alimentación de Información Ajuste de datos del BD Procesamiento de Datos

Obligaciones*:	Cumplir con lo establecido en los lineamientos y en las Normas Complementarias correspondientes al área técnica
	Encargados:
Nombre del Encargado 1*	**Claudia Fernanda Landa Vargas**
Cargo*:	Secretaria de Asuntos Escolares
Funciones*:	Procesos de inscripción, reinscripción, altas, bajas y cambios. Administrador de BD Alimentación de Información Ajuste de datos del BD Procesamiento de Datos
Obligaciones*:	Cumplir con lo establecido en los lineamientos y en las Normas Complementarias correspondientes al área Administrativa
Nombre del Encargado 2*	**Martha Noemí Campos Plazola**
Cargo*:	Jefa de la Oficina de Servicios Escolares
Funciones*:	Consultas de información-**Cuenta no permite cambios de datos**
Obligaciones*:	Cumplir con lo establecido en los lineamientos y en las Normas Complementarias correspondientes al área Administrativa
Nombre del Encargado 3*	**Nancy Daniela Olvera Ramírez**
Cargo*:	Jefa del Departamento de Orientación Educativa y Tutoría
Funciones*:	Consulta y manejo de Datos para fines de asignación de tutores Reportes de datos para profesores
Obligaciones*:	Cumplir con lo establecido en los lineamientos y en las Normas Complementarias correspondientes al área Administrativa –**Cuenta no modifica datos personales**
Nombre del Encargado 4*	**Juan Miguel Pérez Enríquez**
Cargo*:	Jefe del Departamento de Titulación
Funciones*:	Cargar datos académicos Consulta de Datos Alumnos Consultad de Datos Profesores
Obligaciones*:	Cumplir con lo establecido en los lineamientos y en las Normas Complementarias correspondientes al área Administrativa – **Cuenta no modifica datos personales**
Nombre del Encargado 5*	**Jesús Peña Delgadillo**
Cargo*:	Técnico académico
Funciones*:	Cargar datos académicos Consulta de Datos Alumnos Consultad de Datos Profesores
Obligaciones*:	Cumplir con lo establecido en los lineamientos y en las Normas Complementarias correspondientes al área Administrativa
Nombre del Encargado 6*	**Karla Lucía Hernández Sánchez**
Cargo*:	Coordinadora de Servicio Social
Funciones*:	Cargar datos de Alumnos que cumplen con el Servicio Social Consulta de datos académicos
Obligaciones*:	Cumplir con lo establecido en los lineamientos y en las Normas Complementarias correspondientes al área Administrativa –**Cuenta no modifica datos personales**
	Usuarios:
(Nombre del Usuario 1*)	**Victoria Chávez**
Cargo*:	Secretaria del departamento de titulación

Funciones*:	Responsable Sala de Exámenes Profesionales Capturar información de exámenes Manejo de Expedientes Enviar Expedientes a DGAE
Obligaciones*:	Cumplir con lo establecido en los lineamientos y en las Normas Complementarias correspondientes al área Administrativa –**Cuenta no modifica datos personales**
(Nombre del Usuario 2*)	**Javier Flores Covarrubias**
Cargo*:	Coordinador de Enseñanza Práctica
Funciones*:	Administrar el registro de asignatura prácticas y asignación de alumnos Registro de CTA y Nombre de alumnos a grupos prácticos
Obligaciones*:	Cumplir con lo establecido en los lineamientos y en las Normas Complementarias correspondientes al área Administrativa –**Cuenta no modifica datos personales**
(Nombre del Usuario 3*)	**Karla Lucía Hernández Sánchez**
Cargo*:	Coordinadora de Servicio Social
Funciones*:	Consulta número de cuenta, nombre y datos académicos
Obligaciones*:	Cumplir con lo establecido en los lineamientos y en las Normas Complementarias correspondientes al área Administrativa –**Cuenta no modifica datos personales**
(Nombre del Usuario 4*)	**Juan Miguel Pérez Enriquez**
Cargo*:	Jefe del Departamento de Titulación
Funciones*:	Consulta de Datos Alumnos Consulta de Datos Profesores.
Obligaciones*:	Cumplir con lo establecido en los lineamientos y en las Normas Complementarias correspondientes al área Administrativa –**Cuenta no modifica datos personales**
(Nombre del Usuario 5*)	**Nancy Daniela Olvera Ramírez**
Cargo*:	Jefa del Departamento de Orientación Educativa y Tutoría
Funciones*:	Consulta y manejo de Datos para fines de asignación de tutores Reportes de datos para profesores
Obligaciones*:	Cumplir con lo establecido en los lineamientos y en las Normas Complementarias correspondientes al área Administrativa –**Cuenta no modifica datos personales**
(Nombre del Usuario 6*)	**Martha Noemí Campos Plazola**
Cargo*:	Jefa de la Oficina de Servicios Escolares
Funciones*:	Emisión de constancias Tramites de alumnos Expedientes de Titulación
Obligaciones*:	Cumplir con los reglamentos y Legislación Universitaria
(Nombre del Usuario 7*)	**Claudia Fernanda Landa Vargas**
Cargo*:	Secretaria de Asuntos Escolares
Funciones*:	Administrador de BD Alimentación de Información Ajuste de datos del BD Procesamiento de Datos

Obligaciones*:	Cumplir con lo establecido en los lineamientos y en las Normas Complementarias correspondientes al área Administrativa
(Nombre del Usuario 8*)	**Jesús Peña Delgado**
Cargo*:	Técnico académico
Funciones*:	Cargar datos académicos Consulta de Datos Alumnos Consultad de Datos Profesores
Obligaciones*:	Cumplir con lo establecido en los lineamientos y en las Normas Complementarias correspondientes al área Administrativa
(Nombre del Usuario 9*)	**Académicos de la FMVZ**
Cargo*:	Profesor y Administrativos
Funciones*:	Consultar información Información de Correos Alumnos
Obligaciones*:	Cumplir con lo establecido en los lineamientos y en las Normas Complementarias correspondientes al área Administrativa –**Cuenta no modifica datos personales**
(Nombre del Usuario 10*)	**Laura Patricia Romero Romero**
Cargo*:	Jefa de la División de Estudios Profesionales
Funciones*:	Consulta de Información Alumnos Consulta Historia Académica
Obligaciones*:	Cumplir con lo establecido en los lineamientos y en las Normas Complementarias correspondientes al área Administrativa **-Cuenta no modifica datos personales**

Identificador único*	**FMVZ-SIS-065**
Nombre del sistema*	**INSCRIPCIONES FMVZ**
Datos personales con justificación (sensibles o no) contenidos en el sistema*:	Alumnos Número de cuenta Nombre alumno Año de ingreso Lugar Nacimiento Fecha nacimiento Nacionalidad Domicilio Calle y No Col. o población C.P. Delelg. o munic Estado Lada Teléfono casa Celular Lada trabajo Teléfono trabajo Lada familiar Teléfono familiar Correo electrónico 1

	Correo electrónico 2 Teléfono para informar en caso de emergencia Grupo sanguíneo Nombre de profesores Generación Créditos cursados
Responsable administrativo*	**Laura P. Romero Romero**
Nombre*:	Laura Patricia Romero Romero
Cargo*:	Jefa de la División de Estudios Profesionales
Funciones*:	Supervisar y controlar los procesos administrativos escolares, para el buen uso de los datos
Obligaciones*:	• Vigilar el cumplimiento de las disposiciones contenidas en la Legislación Universitaria, así como de los reglamentos internos de la Facultad. • Designación de encargados del sistema • Verificar que cumplan con los lineamientos y Normas Complementarias sobre medidas de seguridad técnica, administrativas y físicas para la protección de datos personales en posesión de la Universidad
Responsable técnico1 *	**Jesús Peña Delgadillo**
Nombre*:	Jesús Peña Delgadillo
Cargo*:	Técnico académico
Funciones*:	Resguardo de datos captados Ajuste de datos Uso de los datos captados con fines estadísticos Desarrollo y Mantenimiento del Sistema
Obligaciones*:	Cumplir con lo establecido en los lineamientos y en las Normas Complementarias correspondientes al área Administrativa
Responsable técnico2 *	**Claudia Fernanda Landa Vargas**
Nombre*:	**Claudia Fernanda Landa Vargas**
Cargo*:	Secretaria de Asuntos Escolares
Funciones*:	Administrador de BD Alimentación de Información proporcionada por DGAE Ajuste de datos de Base de Datos
Obligaciones*:	Cumplir con lo establecido en los lineamientos y en las Normas Complementarias correspondientes al área Administrativa

	Encargados:
Nombre del Encargado 1*	**Claudia Fernanda Landa Vargas**
Cargo*:	Secretaria de Asuntos Escolares
Funciones*:	Administrador de BD Alimentación de Información Ajuste de datos del BD Procesamiento de Datos
Obligaciones*:	Cumplir con lo establecido en los lineamientos y en las Normas Complementarias correspondientes al área Administrativa
Nombre del Encargado 2*	Jesús Peña Delgadillo
Cargo*:	Técnico académico
Funciones*:	Desarrollo y mantenimiento del Sistema de Inscripciones Respaldo de la información Inscripciones Ajuste de datos Uso de los datos captados con fines estadísticos Resguardo de datos
Obligaciones*:	Cumplir con lo establecido en los lineamientos y en las Normas Complementarias correspondientes al área Administrativa
	Usuarios:
(Nombre del Usuario 1*)	**Alumnos de la FMVZ**
Cargo*:	Estudiantes
Funciones*:	Actualizar y Modificar sus datos personales
Obligaciones*:	Conocer los lineamientos de protección de datos personales

ANEXO 2

Funciones y Obligaciones de quienes traten datos personales

Diciembre 2023

Tabla 1 Actividades del personal dentro de Sistema de Gestión de Seguridad de la Información en la FMVZ

Tratamiento de datos personales	TD	CSI	ESI	PUA	RSI
Recepción de solicitudes para cargar bases de datos en sistemas de la FMVZ		X			
Subir bases de datos					X
Captura de datos en Sistemas			X		
Revisar los documentos entregados por las áreas universitarias para detectar datos personales.			X		
Solicitar Respaldos de Datos en Sistemas			X		X
Genera Respaldos de sistemas					X
Proteger los datos personales contenidos en el sistema de accesos no autorizados					X
Mantener actualizado los servidores donde se alojan los sistemas de tratamiento.					X
Mantener actualizado los servidores donde se alojan los sistemas de tratamiento					X
Dictar políticas para el aseguramiento de los datos personales en la Facultad de Medicina Veterinaria y Zootecnia		X			X
Proporcionar la información para la capacitación en materia de protección de datos personales		X	X	X	X
Proteger el archivo físico de la Unidad de accesos no autorizados.				X	X

TD= Titular de la Dependencia
CSI= Coordinador de Seguridad de la Información
ESI= Encargado de Seguridad de la Información
PUA= Personal de la Unidad Administrativa
RSI= Responsable de Sistemas

Tabla 2 Relación de actividades dentro del Sistema de Gestión de Seguridad de la Información de la FMVZ

Actividades	TD	CSI	ESI	PUA	RSI
Política y Objetivos del SGSI	X	X			X
Funciones y obligaciones	X	X	X	X	X
Inventario de Datos Personales.	X		X	X	X
Análisis de Riesgo de los Datos Personales			X	X	X
Análisis de Brecha de las Medidas de Seguridad			X	X	X
Implementación de las Medidas de Seguridad		X	X	X	X
Capacitación		X	X	X	X
Apoyo para la creación de documentos internos			X	X	X
Revisiones y Auditoría	X	X		X	X

Tabla 3 Matriz de Rendición de Cuentas

Tratamiento de datos personales	TD	CSI	ESI	PUA	RSI
CSI= Coordinador de Seguridad de la Información	X				
ESI= Encargado de Seguridad de Información		X	X	X	X
PUA= Personal de la Unidad Administrativa	X	X			
RSI= Responsable de Sistemas		X			

ANEXO 3

Análisis de Riesgos

Diciembre 2023

ANEXO 4

Análisis de Brecha

Diciembre 2023

ANEXO 5

Plan de trabajo

Diciembre 2023

PLAN DE TRABAJO

La FMVZ, cuenta con un plan de trabajo general para establecer organizar las actividades que serán prioridad para el año en curso. A continuación se presenta el Plan para el 2024.

ANEXO 6

Formatos para cumplimiento de las Medidas de Seguridad Técnicas (MST)

Diciembre 2023

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

			Identificador único:		
Formato:	**2**	**Verificación anual**	**Acción concluida**	(**SI**)	
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					

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

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

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

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

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

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

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

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

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

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

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

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

			Identificador único:	
Formato:	**15**	**Verificación anual**	**Acción concluida**	(**SI**)
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. *Por ejemplo*: 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. *Por ejemplo*: *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 Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

			Identificador único:	
Formato:	**16**	**Verificación anual**	**Acción concluida**	(**SI**)
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 (*log*) 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			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

			Identificador único:	
Formato:	**17**	**Verificación anual**	**Acción concluida**	(**SI**)
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 Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

			Identificador único:		
Formato:	**18**	**Verificación anual**	**Acción concluida**	(**SI**)	
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 Administrador del sistema de información o servidor			**Fecha término**		
Observaciones / anotaciones					

			Identificador único:	
Formato:	**19**	**Verificación anual**	**Acción concluida**	(**SI**)
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. *Por ejemplo*: En caso de consultar vía un *Webservice* 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. *Por ejemplo*: Si la cuenta de acceso a un *Webservice* – 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. *Por ejemplo*: si la identificación para acceder a un respaldo remoto es del tipo correopersonal@google.com, deberá cambiarse por una cuenta del tipo cuentadegestion@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			**Fecha término**	
Observaciones / anotaciones				

			Identificador único:		
Formato:	**20**	**Verificación anual**	**Acción concluida**	(**SI**)	
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. *Por ejemplo*: En el equipo de cómputo las bitácoras de acceso de usuarios al sistema operativo y al sistema de información (*logs*), 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. *Por ejemplo*: diario, semanal, mensual. **C)** Establecer en el documento el procedimiento de resguardo de las bitácoras. *Por ejemplo*: respaldo y protección de *logs* 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 Administrador del sistema de información o servidor			**Fecha término**		
Observaciones / anotaciones					

			Identificador único:		
Formato:	**21**	**Verificación anual**	**Acción concluida**	(**SI**)	
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 Administrador de redes de datos			**Fecha término**		
Observaciones / anotaciones					

			Identificador único:		
Formato:	**22**	**Verificación anual**	**Acción concluida**	(**SI**)	
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 (*TCP y UDP*) que requiera el sistema de información para su operación. *Por ejemplo*: para servicios *Web* los puertos 80 y 8080 son los convencionales. **B)** Activar en el sistema operativo la herramienta correspondiente para el control de puertos de comunicación. *Por ejemplo*, en Linux puede tratarse de un *firewall* 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. *Por ejemplo*: Permitir el acceso al puerto de *SSH* 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 Administrador del sistema de información o servidor			**Fecha término**		
Observaciones / anotaciones					

			Identificador único:	
Formato:	**23**	**Verificación anual**	**Acción concluida**	(**SI**)
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:		**F)** 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. **G)** 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. **H)** 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. **I)** 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 Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

			Identificador único:		
Formato:	**24**	**Verificación anual**	**Acción concluida**	(**SI**)	
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 Administrador del sistema de información o servidor			**Fecha término**		
Observaciones / anotaciones					

			Identificador único:	
Formato:	**25**	**Verificación anual**	**Acción concluida**	(**SI**)
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 Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

			Identificador único:	
Formato:	**26**	**Verificación anual**	**Acción concluida**	(**SI**)
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			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

			Identificador único:	
Formato:	**27**	**Verificación anual**	**Acción concluida**	(**SI**)
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 Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

			Identificador único:	
Formato:	**28**	**Verificación anual**	**Acción concluida**	(**SI**)
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 Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

Políticas

Diciembre 2023

Políticas de Servicios del Centro de Datos y el Acuerdo de Nivel Operacional

1. Definiciones y acrónimos

ADMINISTRADOR. El DTE de la FMVZ.

ALOJAMIENTO. Asignación de servidor virtual en el CD, siendo operativo en infraestructura de cómputo y telecomunicaciones a cargo de la FMVZ.

CD. Centro de Datos. Infraestructura de cómputo y telecomunicaciones en condiciones de alta disponibilidad dentro del DTE.

CONFIRMACIÓN. Documento oficial emitido por el ADMINISTRADOR donde se informa al RESPONSABLE la asignación del SERVICIO y el ID SERVICIO y cualquier información adicional para el acceso, control y GESTIÓN del SERVICIO.

DGTIC. Dirección General de Cómputo y de Tecnologías de la Información y Comunicación de la UNAM.

DT. Dirección de Telecomunicaciones de la DGTIC.

DTE. Departamento de Tecnología Educativa de la FMVZ.

FMVZ. Facultad de Medicina Veterinaria y Zootecnia de la UNAM.

GESTIÓN. Conjunto de acciones realizadas por el RT en nombre del RESPONSABLE de manera exclusivamente remota.

ID SERVICIO. Identificador único del SERVICIO asignado por el DTE y asociado a la SOLICITUD del RESPONSABLE aprobada en la CONFIRMACIÓN, con un NIVEL determinado, una fecha de inicio y fecha de término, requerido para cualquier asunto relacionado con el mantenimiento y operación del SERVICIO.

NIVEL. Clasificación de la atención, respuesta a incidentes, capacidades de respaldo y recuperación ante desastres del SERVICIO.

OLA. Operational Level Agreement (Acuerdo de Nivel Operacional). Condiciones y límites con las que se proporciona el SERVICIO.

POLÍTICAS. Lineamientos y procedimientos establecidos en este documento.

PUBLICACIÓN. Acción de hacer accesible a otros usuarios, dentro o fuera de la UNAM, el ID SERVICIO y la información que contenga, por medio de la asignación de direccionamiento IPv4 e IPv6, y alta en el Servicio de Nombres de Dominio.

RESPONSABLE. Responsable administrativo del SERVICIO en el Departamento de la FMVZ que solicita el SERVICIO en el CD.

RT. El responsable técnico del SERVICIO y que está plenamente identificado ante el DTE por el RESPONSABLE, con quien tiene relación laboral.

SERVICIO. Asignación de infraestructura como servicio (IaaS) también conocida como infraestructura virtual en el CD, ya sea de manera inicial, reactivación o modificación de un SERVICIO existente.

SOLICITUD. Formato estándar donde el RESPONSABLE requiere el SERVICIO y acepta las POLÍTICAS y el OLA.

UNAM-CERT. Coordinación de Seguridad de la Información de la DGTIC.

2. Introducción

La FMVZ, a través del DTE, dispone de infraestructura de cómputo y telecomunicaciones con las tecnologías más necesarias en materia de suministro eléctrico, conectividad a la Red UNAM e Internet, almacenamiento masivo, virtualización y seguridad de la información, que constituyen el CD, localizado en el DTE, para proporcionar el SERVICIO al RESPONSABLE con alta disponibilidad.

3. Objetivo

Estas Políticas de Servicio del Centro de Datos y el Acuerdo de Nivel Operacional tienen por objetivo establecer las condiciones del SERVICIO, sus características, límites de responsabilidad y procedimientos para los departamentos de la FMVZ.

4. Del SERVICIO

4.1. El SERVICIO está orientado a apoyar a la comunidad de la FMVZ.

4.2. Para la SOLICITUD se deberán aceptar las POLÍTICAS y el OLA que corresponden al ID SERVICIO otorgado al RESPONSABLE a raíz de su SOLICITUD.

4.3. Cualquier fin, propósito y objetivo para el uso del SERVICIO que sean compatibles con los de la Universidad Nacional Autónoma de México, se consideran un uso autorizado y aceptable del SERVICIO.

4.4. El SERVICIO consiste en la asignación de infraestructura virtual apoyada por la infraestructura física del CD.

4.5. Los tipos de NIVEL de SERVICIO son:

4.5.1. Básico. Respuesta a reporte en menos de 8 horas hábiles. Resolución en menos de 3 días hábiles. Respaldo automático en bloque cada 7 días naturales. Restablecimiento de 0% a 100% en menos de 3 días hábiles.

4.5.2. Intermedio. Respuesta a reporte en menos de 8 horas hábiles. Resolución en menos de 3 días hábiles. Respaldo automático en bloque cada 7 días naturales. Restablecimiento de 0% a 100% en menos de 2 días hábiles.

4.5.3. Alto. Respuesta a reporte en menos de 4 horas hábiles. Resolución en menos de 1 día hábil. Respaldo automático en bloque cada 5 días naturales. Restablecimiento de 0% a 100% en menos de 4 horas hábiles.

4.6. El SERVICIO es considerado vigente si posee un ID SERVICIO válido con un NIVEL asignado.

4.7. Todo SERVICIO asignado puede renovarse en su vigencia mediante una nueva SOLICITUD de SERVICIO.

4.8. Ningún NIVEL puede cambiarse durante la vigencia del SERVICIO.

4.9. Ningún SERVICIO puede asignarse con propósitos de pruebas, desarrollo o evaluación. La infraestructura, almacenamiento y demás componentes que se asignen de forma temporal a pruebas no pueden ser asociados a estas POLÍTICAS y el respectivo OLA. Los recursos temporales de pruebas o desarrollos se facilitan por tiempo limitado sin garantía alguna de soporte, funcionamiento, respaldo o continuidad.

5. De la asignación del ID SERVICIO

5.1. Para la autorización y asignación del ID SERVICIO el RESPONSABLE deberá proporcionar al DTE, en todos los casos:

5.1.1. SOLICITUD completa indicando SERVICIO y NIVEL requeridos.

5.1.2. Aceptación de conformidad de las POLÍTICAS y OLA.

5.2. Toda SOLICITUD está sujeta a aprobación.

5.3. La FMVZ, a través del ADMINISTRADOR y previa consulta con las áreas afines (DT) podrá rechazar una SOLICITUD, cancelar o suspender un SERVICIO en caso de:

5.3.1. Declaraciones imprecisas del RESPONSABLE al momento de emitir la SOLICITUD.

5.3.2. Uso del SERVICIO que sea distinto al aceptable en estas POLÍTICAS.

5.3.3. Fallas de seguridad que pongan en riesgo el resto de la infraestructura del CD.

5.3.4. Cualquier omisión en sus acciones, descritas en el OLA, por parte del RESPONSABLE o el RT.

5.3.5. Fin de la vigencia del ID SERVICIO sin solicitud de renovación emitida por el RESPONSABLE.

5.3.6. A solicitud expresa por escrito del RESPONSABLE.

5.3.7. Actos u órdenes de las autoridades universitarias que requieran la suspensión o cancelación del SERVICIO.

5.4. El DTE notificará al RESPONSABLE, la aprobación o el rechazo. En este último caso se indicarán las razones de la no asignación.

6. De la PUBLICACIÓN

6.1. La asignación de un ID SERVICIO no implica la PUBLICACIÓN.

6.2. En caso de requerir la PUBLICACIÓN, previamente el RESPONSABLE debe:

6.2.1. Acceder con las credenciales del ID SERVICIO y verificar la GESTIÓN de acuerdo con su solicitud.

6.2.2. Cargar los contenidos, información, aplicaciones y/o códigos en lo general para los cuales solicitó el SERVICIO.

6.2.3. Verificar a través de la GESTIÓN la adecuada visualización y operatividad de sus sistemas alojados en el SERVICIO.

6.2.4. En caso de resultado positivo al inciso 6.2.3, solicitar por separado a UNAM-CERT la realización de pruebas de penetración (*Pentest*) y análisis de vulnerabilidades.

6.2.5. En caso de resultado aprobatorio del inciso 6.2.4, solicitar a la DT el alta, cambio o reasignación en el Servicio de Nombres de Dominio dentro del esquema unam.mx, de conformidad con los procedimientos y políticas establecidos al respecto por la DT.

6.3. Para dominios distintos a unam.mx, el RESPONSABLE realizará el trámite de registro ante la entidad de nombres de dominio que considere adecuada previa autorización por escrito de la DT.

6.4. En ningún caso puede realizarse la PUBLICACIÓN bajo el esquema unam.mx que no haya cumplido con todo lo indicado en el inciso 6.2.

7. De la solicitud de SERVICIO

7.1. La aceptación de estas POLÍTICAS y OLA implica la aprobación por parte del RESPONSABLE de todos los términos, condiciones, descripciones y responsabilidades descritos en este documento.

8. De las comunicaciones y el soporte técnico

8.1. Para todo asunto técnico, operativo y administrativo, tanto el RESPONSABLE como el RT pueden utilizar los siguientes medios de comunicación con el ADMINISTRADOR:

8.1.1. Correo electrónico a la cuenta ilopez@fmvz.unam.mx, las 24 horas, los 365 días del año.

8.1.2. Departamento de Tecnología Educativa, lunes a viernes en días activos del calendario oficial UNAM, de las 9:00 a 19:00 horas, Tiempo del Centro en el teléfono 5556225848 o vía correo electrónico en computofmvz@unam.mx

8.2. Para todos los casos, es indispensable proporcionar el ID SERVICIO para identificar de manera inequívoca el SERVICIO asignado.

9. Seguridad de la información

9.1. Son tareas a cargo del RESPONSABLE y el RT las siguientes en materia de seguridad de la Información para el SERVICIO:

9.1.1. Actualizar y mantener al día el sistema operativo y las aplicaciones, incluyendo servicios Web y especialmente aquellas que mejoran la seguridad e integridad del sistema y las aplicaciones cuyo funcionamiento está asociado al SERVICIO.

9.1.2. Instalar y mantener activa tecnología de protección del tipo cortafuegos *(firewall)*.

9.1.3. Instalar y mantener actualizado un software antivirus si el sistema operativo para el SERVICIO es de plataforma Windows.

9.1.4. Establecer los mecanismos adecuados para el control de acceso a aplicaciones y GESTIÓN del SERVICIO.

9.1.5. Obtener por escrito de UNAM-CERT el cumplimiento de normas mínimas de seguridad por medio de los resultados de pruebas de penetración (*Pentest*) y análisis de vulnerabilidades, enfocadas al sistema operativo y aplicaciones en ejecución, independientemente de requerir la PUBLICACIÓN del SERVICIO.

9.1.6. Aplicar las recomendaciones derivadas de las pruebas de penetración y análisis de vulnerabilidades previo permitir el acceso al SERVICIO de forma regular para otros usuarios.

9.2. Son tareas a cargo de la FMVZ a través del ADMINISTRADOR las siguientes en materia de seguridad de la Información para cualquier tipo de SERVICIO:

9.2.1. Proteger el acceso al CD evitando el ingreso de cualquier persona no autorizada y debidamente registrada.

9.2.2. Aplicar las políticas de seguridad de la información establecidas por UNAM-CERT.

9.2.3. Conservar a través de UNAM-CERT en adecuado estado de operación los equipos de seguridad perimetral de la red de datos de la UNAM y del CD.

9.2.4. Impedir la instalación, configuración, puesta en marcha o continuidad de operaciones de cualquier SERVICIO en el CD que no cumpla las políticas de seguridad de la información de UNAM-CERT a fin de evitar riesgos a los equipos y otros servicios alojados en el CD.

9.2.5. Notificar al RESPONSABLE y al RT, de forma inmediata, cualquier riesgo, vulnerabilidad o situación en lo general que ponga en riesgo la continuidad de la operación del SERVICIO, sus aplicaciones y datos asociados.

10. Confidencialidad y protección de datos

10.1. Las presentes **Políticas de Servicios del Centro de Datos y el Acuerdo de Nivel Operacional** no constituyen, en todo o en parte, compromiso alguno de la Universidad Nacional Autónoma de México o de cualquiera de sus entidades o dependencias, de su personal académico, académico – administrativo, empleados o cualquier otro miembro de su comunidad, para la prestación del SERVICIO a cualquier entidad externa a la institución.

10.2. Tampoco implica la prestación del SERVICIO compromiso de la institución con empresa, integrador o distribuidor alguno para la participación de estos últimos en cualquier proceso relacionado con el SERVICIO.

10.3. La UNAM se reserva el derecho a utilizar la información proporcionada por el RESPONSABLE y el RT para los fines del SERVICIO, sin compartir la información recibida con relación a este documento con otras personas, físicas o morales.

10.4. Las instancias que proporcionen cualquier tipo de información requerida por este documento o sus anexos asumen lo anterior en el entendido de que los datos relacionados con el SERVICIO que emitan a la FMVZ serán de tipo confidencial para cualquier persona ajena a la comunidad universitaria, no significan un compromiso definitivo para el acceso al SERVICIO y tampoco sustituyen los procesos definidos dentro de la normatividad de la UNAM para otros servicios, recursos y tecnologías asociados con el SERVICIO.

10.5. Cualquier área(antes era instancia) involucrada con los datos relacionados con estas POLÍTICAS asume que no puede liberar hacia terceros, en todo o en parte, información proporcionada a la FMVZ al respecto del SERVICIO, para ningún fin o propósito.

10.6. La FMVZ no puede proporcionar información alguna relacionada con los datos, aplicaciones, usuarios, cuentas, accesos, consultas, programas, códigos, almacenamientos, recursos, licencias, objetivos y funciones de los sistemas de información asociados al SERVICIO e instalados, mantenidos y configurados por el RESPONSABLE y el RT, a instancia interna o externa a la UNAM, sin la autorización por escrito del RESPONSABLE.

10.7. En el caso de finalización del SERVICIO sin renovación, la FMVZ eliminará de su infraestructura en un plazo no inferior a treinta días naturales y no superior a sesenta días naturales todo dato, sistema, código, aplicación, recurso y demás elementos a cargo del RESPONSABLE y el RT que no hayan sido retirados por estos últimos previo al fin de vigencia del ID SERVICIO.

11. Vigencia

11.1. Las presentes **Políticas de Servicios del Centro de Datos y el Acuerdo de Nivel Operacional** estarán vigentes a partir del 9 de agosto de 2021 y podrán ser modificadas con fines de mejora en la calidad y estabilidad de los servicios que amparan.

11.2. Estas POLÍTICAS reemplazan a cualquier versión previa publicada a la fecha de inicio de vigencia que se señala en el inciso inmediato anterior.

12. Acuerdo de Nivel Operacional (OLA)

12.1. Los compromisos de la FMVZ a través del ADMINISTRADOR con relación al RESPONSABLE y el SERVICIO otorgado son:

12.1.1. Mantener en las mejores condiciones operativas el SERVICIO, en alta disponibilidad al menos igual a la proporcionada por la DT en términos de conectividad de red, suministro eléctrico y sistemas de aire acondicionado, las 24 horas del día, los 365 días del año, así como la correcta operación, seguridad y protección la infraestructura del CD.

12.1.2. Asignar al ID SERVICIO los elementos requeridos por el RESPONSABLE en la SOLICITUD que sean factibles a partir de la infraestructura disponible.

12.1.3. Responder cualquier reporte, incidencia o tema relacionado con el SERVICIO en los términos descritos por el NIVEL asignado.

12.1.4. Notificar al RT y al RESPONSABLE, por los medios señalados en la sección 8 de las POLÍTICAS, cualquier variación, contingencia, riesgo, amenaza, mantenimiento preventivo, mantenimiento correctivo o actualización relacionados con el SERVICIO. Para el caso de medidas preventivas con al menos 48 horas previas a la realización de la actividad. Para el caso de contingencias, tan pronto como sea del conocimiento del ADMINISTRADOR.

12.1.5. Realizar, en conjunto con el RT, la instalación lógica de los servidores virtuales asignados asociados al SERVICIO.

12.1.6. Configurar los servicios de red, sistemas de nombre de dominio y servicios asociados para la adecuada operación de servidores virtuales en el CD, en conjunto con la DT.

12.1.7. Asignar una dirección IPv4 y una IPv6 pública por cada infraestructura virtual como parte del proceso de PUBLICACIÓN. La ampliación de direcciones IP asignadas dependerá de la disponibilidad en el CD.

12.1.8. Asignar el nombre de dominio solicitado a la DT por el RESPONSABLE una vez cumplidos los requerimientos para la PUBLICACIÓN y los procedimientos de registro de nombres de dominio establecidos por la DT.

12.1.9. Asignar la protección general de seguridad al SERVICIO a través de cortafuegos o tecnologías similares.

12.1.10. Actualizar hipervisores, servidores virtuales, subsistemas de almacenamiento y demás equipos y programas asociados al SERVICIO, a excepción de las aplicaciones específicas a cargo del RT.

12.1.11. Monitorear todos los servidores y nodos físicos de cómputo a través de métodos automatizados y no automatizados para asegurar la estabilidad del SERVICIO.

12.1.12. Ejecutar el mantenimiento preventivo y correctivo que requieren apertura de equipos de cómputo a su cargo fuera del DTE.

12.1.13. Realizar copias de seguridad automática de toda la información contenida en el SERVICIO con la periodicidad del NIVEL asignado.

12.1.14. Sujetarse a y asegurar la observancia de las políticas de seguridad y acceso al CD.

12.2. Los compromisos del RESPONSABLE con relación a la FMVZ y el SERVICIO asignado son:

12.2.1. Solicitar y usar el SERVICIO única y exclusivamente para los fines, propósitos y objetivos de la Universidad Nacional Autónoma de México como se describen en su Ley Orgánica, sin fines de lucro y sin perjuicio de propios y terceros.

12.2.2. Asumir que el SERVICIO otorgado reside en infraestructura compartida del CD y que la prioridad a la atención de fallas en el SERVICIO depende del NIVEL solicitado, justificado y autorizado.
12.2.3. Asumir toda la responsabilidad legal sobre la información transmitida, resguardada, publicada, protegida y/o respaldada por medio del SERVICIO, sobre cualquier vínculo hacia sitios, sistemas y repositorios dentro o fuera de la UNAM, accesibles desde los sistemas y acervos asociados al SERVICIO y en cualquier proceso y flujo de información hacia sistemas de correo electrónico, sitios Web, comercio electrónico, propios o de terceros, asociados al SERVICIO.
12.2.4. Librar a la FMVZ en lo particular, y a la UNAM en lo general, ante cualquier reclamación o demanda de propios o terceros respecto al uso, publicación, disponibilidad y accesibilidad de la información asociada al SERVICIO.
12.2.5. Notificar al RT del SERVICIO sobre el cumplimiento en lo relativo a leyes y reglamentos en vigor sobre derechos de autor, transparencia, acceso a la información y protección de datos personales.
12.2.6. Publicar de manera visible las condiciones de uso del sistema de información asociado al SERVICIO, así como políticas de confidencialidad, protección de datos personales y protección de los derechos de autor.
12.2.7. Notificar por escrito al ADMINISTRADOR cualquier cambio del RT mientras esté vigente el ID SERVICIO.
12.2.8. Respaldar en medio fuera de línea toda la información digital contenida en el SERVICIO de forma periódica e independiente a los respaldos generales que de manera automática realice el ADMINISTRADOR.
12.3. Los compromisos del RT con relación a la FMVZ y el SERVICIO asignado son:
12.3.1. Respaldar en medio fuera de línea toda la información digital contenida en el SERVICIO de forma periódica e independiente a los respaldos generales que de manera automática realice el ADMINISTRADOR.
12.3.2. Poseer un respaldo general fuera de línea, es decir, en infraestructura distinta a la del SERVICIO, de su acervo de información digital con una antigüedad no superior a 30 días naturales desde la ejecución del último respaldo general inmediato anterior.
12.3.3. Actualizar el sistema operativo, librerías y demás elementos de software necesarios para la ejecución de las aplicaciones residentes en el SERVICIO.
12.3.4. Monitorear y supervisar la adecuada operación de las aplicaciones asociadas al SERVICIO.
12.3.5. Reportar cada 30 días naturales al ADMINISTRADOR el tráfico total del SERVICIO medido en múltiplos de bytes.
12.3.6. Notificar cualquier falla que detecte en su ámbito de responsabilidades al ADMINISTRADOR, de forma inmediata, y confirmar los reportes a través de los mecanismos de comunicación indicados en la sección 8 de las POLITICAS
12.3.7. Tener los conocimientos técnicos suficientes y necesarios para la administración de los recursos asociados al SERVICIO.
12.3.8. Instalar y actualizar cualquier licencia de software comercial, de fuente libre o desarrollada ad hoc para el correcto funcionamiento del SERVICIO asignado

12.3.9. Sujetarse a las políticas de seguridad, así como atender las recomendaciones y evaluaciones descritas en la sección 6 de estas POLÍTICAS para la PUBLICACIÓN.
12.3.10. Facilitar el monitoreo central que realice el ADMINISTRADOR.
12.3.11. Conservar al menos un esquema de seguridad activo, como el asignado por el ADMINISTRADOR. El RT puede instalar y configurar alguna tecnología alternativa de seguridad, pero debe bloquear todo el tráfico por defecto y permitir solo el tráfico que vaya a utilizar.
12.3.12. Evaluar regularmente las aplicaciones Web y scripts para verificar que son seguros y que están actualizados. En caso de asociar al SERVICIO aplicaciones o foros que dependan de sistemas de comentarios, el RT debe instalar alguna protección contra spam. La alternativa CAPTCHA está permitida.
12.3.13. No mantener el SERVICIO fuera de línea una vez que ha aprobado la PUBLICACIÓN por más de 24 horas.
12.3.14. No utilizar el SERVICIO como unidad de almacenamiento en red.
12.3.15. Instalar, en acuerdo y colaboración con el ADMINISTRADOR, los equipos virtuales asignados en el SERVICIO.
12.3.16. Incluir en la fase de instalación de software de sistema operativo y/o aplicaciones, controladores, y cualquier otro componente lógico necesario para la adecuada instalación del servidor virtual asociado al SERVICIO
12.3.17. Configurar, administrar y respaldar los servidores virtuales asignados en el SERVICIO.
12.3.18. Monitorear y supervisar la adecuada operación de las aplicaciones residentes en los servidores virtuales asociados al SERVICIO.
12.4. La FMVZ no asume responsabilidad alguna en los siguientes casos con relación al SERVICIO y el NIVEL asignados:
12.4.1. No asignación del SERVICIO solicitado por insuficiencia, falsedad o nulidad de datos en la SOLICITUD.
12.4.2. No asignación o interrupción del SERVICIO por no disponibilidad de recursos suficientes en el CD a partir de lo requerido por el RESPONSABLE y que no hayan sido autorizados.
12.4.3. Pérdida de información o fallas en la prestación del SERVICIO por pérdida del control de contraseñas de acceso, cambios en sistemas de información, omisiones en respaldos fuera de línea y en lo general, por cualquier omisión o cumplimiento parcial en sus compromisos por parte del RESPONSABLE en lo relativo al SERVICIO.
12.4.4. Pérdida o borrado accidental de datos por parte del RT, el RESPONSABLE y/o los usuarios del SERVICIO.
12.4.5. Falla en la reposición total de datos debido a que, en el tiempo transcurrido entre el último respaldo y la aparición de una falla, haya existido un borrado intencional o accidental de los datos contenidos en el SERVICIO.
12.4.6. Funcionalidad, accesibilidad, compatibilidad, visualización, consulta, recuperación, operabilidad y disponibilidad de aplicaciones, bases de datos y acervos asociados al SERVICIO, funciones todas ellas en el ámbito de competencia del RT y el RESPONSABLE.
12.4.7. Usos distintos del SERVICIO a los declarados y autorizados en la SOLICITUD.

12.4.8. Expectativas de NIVEL de SERVICIO distintas a las características del NIVEL asignado.

12.4.9. Alteraciones en la operación de sistemas, aplicaciones, códigos y demás componentes asociados al SERVICIO bajo el ámbito de competencia del RT que no hayan sido aprobados en lo técnico por el ADMINISTRADOR.

Última Actualización: 30/07/2021

Políticas de uso de contraseñas

La Facultad de Medicina Veterinaria y Zootecnia (FMVZ) a través del Departamento de Tecnología Educativa (DTE) establece los siguientes lineamientos para la creación de contraseñas para cuentas y su uso en sistemas, aplicaciones, programas, cuentas de correo, redes sociales y todo lo relacionado con cuentas institucionales, así como en la creación de sistemas y aplicaciones que utilizarán autenticación y quedarán albergadas en la FMVZ.

1. Definiciones y acrónimos

FMVZ: Facultad de Medicina Veterinaria y Zootecnia

DTE: Departamento de Tecnología Educativa

Usuario: Todo empleado o prestatario de servicios autorizado por FMVZ alumnos y terceros que haga uso de los activos o servicios informáticos de la institución, para el desempeño de sus funciones, consulta o atención al servicio.

Dispositivo: Todo aquel equipo de cómputo como lo son Computadoras, Laptops, Celulares, Tablets, Servidores, Proyectores, Lectores Biométricos, Impresoras, Puntos de Acceso, Equipos de telecomunicaciones, etc.

Sistema: Todo aquel programa o aplicación de cómputo para Dispositivos de cómputo que haga uso de cuentas para ingresar al mismo.

Cuenta Institucional: Cuenta oficial asociada a la prestación de servicios de tecnología de información y comunicación, asignada por DTE.

2. Creación de contraseñas

Se deberá complir con los siguientes puntos para la creación de contraseñas.

2.1. La longitud mínima para una contraseña deberá ser al menos 10 caracteres. Esta longitud es para contraseñas que sirvan de acceso a un dispositivo de hardware o para cuenta de cualquier tipo de software, si los dispositivos y sistemas lo permiten. En su defecto, deberán cubrir el mayor número de campos de longitud de la contraseña que el sistema o dispositivo permite.

2.2. La contraseña deberá usar un conjunto de caracteres variados, alfanuméricos y de gran extensión en lo posible (Mayúsculas, minúsculas, símbolos y números. Ej. “M1Pas$w0Rd.”), las cuales deberán ser conformadas por al menos:

- Letras mayúsculas y minúsculas (a-z A-Z)

- Incluir Números (0-9)
- Incluir caracteres especiales como: °!”#$%&/()=?¡|0¿

2.3. Evitar usar como referencias fechas de nacimiento o datos relevantes relacionados con su persona. (CURP, RFC, número celular, etc.)

3. Recomendaciones:

3.1. Se recomienda el uso de una contraseña única para cada cuenta.

3.2. Cambiar periódicamente las contraseñas y evitar usar las mismas. De ser posible, cambiarla al menos cada 6 meses.

3.3. El usuario es responsable de sus contraseñas, por lo que es su responsabilidad si éstas son compartidas con personas ajenas y la FMVZ se deslinda del mal uso de las cuentas y la información que pudiere derivar de dicha contraseña compartida.

3.4. Si existe alguna razón para creer que una contraseña se encuentra comprometida, debe cambiarla inmediatamente siguiendo las reglas de la sección 2.

4. Gestión

De ser posible, utilice alguna herramienta de almacenamiento y gestión de contraseñas:

- KeePass (Gratuito - https://keepass.info)
- LastPass (Gratuito / Paga https://www.lastpass.com/es)
- Enpass (Gratuito / Paga https://www.enpass.io/)
- Keeper (Paga https://www.keepersecurity.com/es_ES/)
- 1Password (Paga https://1password.com/es/)
- RoboForm (Gratuito / Paga https://www.roboform.com/es)

Las herramientas antes mencionadas cuentan con diferentes funcionalidades extras, la elección de dicha herramienta dependerá de las necesidades de cada uno.

5. Buenas prácticas

Evite usar alguna de las siguientes malas prácticas en el manejo de contraseñas:

- Apuntar las contraseñas en lugares no apropiados, tales como: libretas, post-its, pizarrones, papelitos o lugares poco seguros.
- Enviar contraseñas a través de un medio inseguro
- Usar una contraseña para todos los sistemas (correo, finanzas computadora, teléfono, etc)
- Utilizar datos personales en la creación de contraseñas (nombre, fecha de nacimiento, nombre de mascotas, etc)
- Utilizar contraseñas por defecto.
- Difundir la contraseña con personal no autorizado.
- Usar patrones predecibles o usar contraseñas poco seguras, tales como:
    a. Qwerty
    b. 1234567890
    c. 123456
    d. Password
    e. password1
    f. iloveyou

Última Actualización: 5/08/2021

Políticas de borrado seguro

La Facultad de Medicina Veterinaria y Zootecnia (FMVZ) a través del Departamento de Tecnología Educativa (DTE) establece las siguientes políticas para el borrado de archivos conforme a los niveles de criticidad de la información que se deseen eliminar.

1. Responsabilidades.

Es responsabilidad de cada uno de los jefes de las áreas de la Facultad de Medicina Veterinaria y Zootecnia (FMVZ) dar aviso al Departamento de Tecnología Educativa (DTE) sobre la transferencia de equipo entre personal y es responsabilidad del Departamento de Adquisidores Almacén e Inventarios, de la Secretaría Administrativa, avisar al DTE sobre las Tecnologías de la Información (TI) que se darán de baja.

Es responsabilidad del DTE dar aviso al Departamento de Apoyo Técnico en Cómputo (DATC) de los equipos que se transferirán entre personal y/o del equipo que se dará de baja a fin de que se realice el proceso de borrado seguro.

El Departamento de Apoyo Técnico en Cómputo (DATC) tienen como responsabilidad borrar la información de forma segura de los equipos que se van a dar de baja y de los equipos que serán traspasados; dicha información puede ser: fotos, documentos, música, videos o cualquier otro tipo de archivo de los equipos de cómputo de la FMVZ, así como realizar el borrado seguro conforme a las presentes políticas de archivos con información sensible, reservada y/o que contenga datos personales.

2. Borrado Seguro

El borrado seguro consiste en eliminar la información de cierta forma para que esta no pueda ser recuperada. Existen tres tipos de borrado seguro:

- Física: Consiste en la destrucción toral del dispositivo para que no sea recuperado por ningún medio la información que contuviee este. Éste Métido es válido para cualquier tipo de dispositivos como: USB, SSD, HDD, CD, DVD, Blue-ray Disc, etc.
- Desmagnetización: Consiste en exponer el dispositivo a un campo magnético. Éste método de borrado seguro solo se puede utilizar en HDD, disquetes, cintas magnéticas, etc.
- Sobreescritura: Consiste en la utilización de un software, el cual va a realizar una escritura de datos con ciertos patrones sobre el documneto que se desea borrar. Este

procedimiento no es aplicable para dispositivos qe no son regrabables como CD, DVD, Blue-Ray Disc, etc.

3. Aplicabilidad

Los tres métodos de borrado seguro no son aplicables a los diferentes dispositivos con los que se cuentan hoy en día. A continuación, se presenta la siguiente tabla de métodos de borrad seguro que se pueden aplicar a los diferentes dispositivos.

Dispositivo dispositivo	Tipo de física	Destrucción	Desmagnetización	Sobreescritura
Discos duros o HDD	Magnético	Aplica	Aplica	Aplica
Discos flexibles (floppies o disquetes)	Magnético	Aplica	Aplica	Aplica
Cintas	Magnético	Aplica	Aplica	Aplica
CD, DVD, Blue-ray disc	Óptico	Aplica	No aplica	No aplica
Pen driver o USB	Electrónico	Aplica	No aplica	Aplica**
Discos de estado sólido o SSD	Electrónico	Aplica	No aplica	Aplica**

**Para los dispositivos electrónicos se deben utilizar herramientas que cuenten con estándares que aseguren el borrado seguro de la información.

4. Motivos

El borrado seguro se aplicará en los siguientes casos:

- Baja del equipo
- Archivos que sean trasladados al Sistema de Archivos
- Equipo transferido a personal interno de la FMVZ
- Equipo transferido a un área Universitaria diferente a la FMVZ
- Solicitante exigiendo la cancelación de sus datos personales

5. Herramientas

Las herramientas para el borrado seguro de archivos deben de contar como mínimo el método DoD5220.22-M para dispositivos magnéticos y el método NIST 80-88 para dispositivos como USB, SSD, etc.

Algunas de las herramientas que se pueden utilizar para realizar el borrado seguro son:

- Windows:
  - SDelete
  - Wipe My Disks de HDDGURU
  - Eraser
- MacOS
  - Permanent eraser
  - Disk Utility
- Linux
  - srm
  - wipe
- Multiplataforma
  - Dban
  - Blancco Driver Eraser

6. Bases de datos

El borrado seguro de la información contenida en cualquier tipo de motor de base de datos (MySQL, SQL, Oracle, etc) se deberá realizar mediante un método de sobre-escritura de la información contenida en el registro o registros, posteriormente se procederá a realizar el borrado del registro: en caso de que el registro afecte la integridad de la información contenida en la base de datos solamente se realizará la anonimización o seudonimización de los datos.

Última Actualización: 5/08/2021

Solicitud y políticas de uso de cuenta de correo electrónico en dominio @fmvz.unam.mx

1. **Definiciones y acrónimos.**

ALMACENAMIENTO: Capacidad de resguardo de mensajes y archivos asociados en las carpetas de la CUENTA, y notificada al USUARIO junto con las credenciales de acceso a la CUENTA.

CUENTA: Cuenta de correo electrónico en dominio @fmvz.unam.mx, propiedad de la UNAM.

CUENTA INSTITUCIONAL: CUENTA para uso por áreas, proyectos o funciones específicas de la UNAM.

CUENTA PERSONAL: CUENTA de uso exclusivo e individual por un miembro de la comunidad universitaria para el desempeño de las funciones motivo de su empleo, cargo o comisión.

FMVZ: Facultad de Medicina Veterinaria y Zootecnia.

IDENTIFICADOR: Denominación de la CUENTA compuesta por el nombre de USUARIO y el dominio @fmvz.unam.mx

IMAP: Protocolo de acceso a mensajes de Internet. Estándar tecnológico que permite el acceso a mensajes almacenados en un servidor de correo electrónico.

INSTANCIA: Entidad académica o dependencia universitaria de la UNAM a la que está adscrito el USUARIO.

POP3: Protocolo de Oficina de Correo. Estándar tecnológico para clientes de correo para obtener los mensajes almacenados en un servidor remoto.

RFC: Registro Federal de Contribuyentes

SERVICIO: Plataforma para el envío, recepción, reenvío y almacenamiento de mensajes de correo electrónico y archivos asociados, administrado por la FMVZ.

SOLICITUD: Requerimiento de acción relacionado con la CUENTA.

FORMATO DE SOLICITUD: Formulario con datos necesarios del USUARIO para la asignación de la CUENTA por la FMVZ, la modificación de características de la CUENTA o la revocación de ésta.

TIC: Tecnologías de Información y Comunicación

UBICACIÓN: Localización del SERVICIO, ya sea en el Centro de Datos de la FMVZ (SERVICIO LOCAL) o en infraestructura de nube propiedad de un tercero (SERVICIO EN NUBE), cualquiera de ellos con medidas para el encriptado de información y protección de datos personales.

UNAM: Universidad Nacional Autónoma de México.

USUARIO: El titular de la CUENTA, persona adscrita a alguna INSTANCIA cuya identidad está validada por medio de documento probatorio emitido por la UNAM.

2. **Objetivos de la CUENTA.**

2.1. Facilitar la comunicación del USUARIO dentro y fuera de la UNAM por medio del SERVICIO, para el cumplimiento de sus funciones.

2.2. Identificar al USUARIO para el otorgamiento de servicios asociados de TIC, proporcionados por la UNAM.

3. **Características de la CUENTA**

3.1. La CUENTA permite el acceso al SERVICIO para el USUARIO

3.2. LA CUENTA PERSONAL es de uso individual e intransferible. La CUENTA INSTITUCIONAL podrá ser utilizada por varias personas asociadas a un área, proyecto o servicio.

3.3. La información contenida en la CUENTA es propiedad y acceso exclusivos del USUARIO y la FMVZ no asume responsabilidad alguna por la información en ella contenida.

3.4. Una vez que haya sido autorizada y notificada la contraseña inicial al USUARIO, la FMVZ no tendrá acceso a la información contenida en la CUENTA.

3.5. En ningún caso una persona distinta al USUARIO podrá acceder a su contraseña o hacer uso de la CUENTA. Únicamente cuando la autoridad ministerial o judicial competente lo solicite por escrito, la FMVZ permitirá el acceso a personas distintas al USUARIO a la información contenida en la CUENTA PERSONAL.

3.6. El IDENTIFICADOR será, preferiblemente, el número de cuenta (en el caso de estudiantes), número de empleado del USUARIO o el que el usuario indique expresamente en su solicitud.

3.7. La FMVZ no garantiza la continuidad del SERVICIO EN NUBE debido a que la infraestructura en la cual se proporciona no es propiedad de la UNAM.

3.8 La CUENTA es accesible mediante los protocolos estándares POP3 e IMAP para clientes de correo electrónico.

3.9. La CUENTA es accesible mediante el servicio de Webmail (Interfaz en navegador Web) desde el sitio **www.mail.google.com**

4. **Asignación de la CUENTA**

4.1. Para la asignación de la cuenta, se acreditará la relación laboral y/o académica vigente con la UNAM mediante su RFC o número de cuenta, a través de la Secretraría General o la División de Estudios Profesionales de la FMVZ según sea el caso.

4.2. El interesado debe proporcionar una cuenta de correo en servicio alterno con el propósito de recuperar su información y acceso a la CUENTA en caso de pérdida de la contraseña.

4.3. La contraseña de la CUENTA se integra por al menos 8 caracteres alfanuméricos y símbolos. En el caso de estudiantes será su número de cuenta, el cual solo tendrá un primero uso y deberá escribir una nueva contraseña integrada preferentemente por al menos 8 caracteres alfanuméricos y símbolos.

4.4. La FMVZ no garantiza la asignación del IDENTIFICADOR conforme al punto 3.6, debido a la asignación previa a otra persona, por lo que propondrá al USUARIO un IDENTIFICADOR similar al solicitado, para su consideración.

4.5. La FMVZ hará el tratamiento de la información que proporcione el USUARIO en su SOLICITUD de acuerdo con lo establecido en el Aviso de Privacidad Integral de la FMVZ, publicado en https://www.fmvz.unam.mx/fmvz/avisos/Aviso_Privacidad.pdf

5. **Revocación de la CUENTA**

5.1. La UNAM se reserva el derecho de revocar al USUARIO el acceso a la CUENTA cuando se presente alguno de los siguientes supuestos:

5.1.1. Conclusión de relación laboral entre el USUARIO y la UNAM

5.1.2. SOLICITUD explícita del USUARIO.

5.1.3. Cualquier acción comprobada que haya realizado el USUARIO que contravenga estas Políticas de Uso.

5.1.4. Falsificación de identidad del USUARIO

5.1.5. Por indicaciones de las autoridades universitarias mediante causa debidamente motivada y justificada por el área jurídica.

5.1.6. Ausencia o fallecimiento del USUARIO.

5.1.7. Inactividad de la CUENTA por más de 2 años.

5.1.8. Por disposición de la autoridad ministerial o judicial competente.

6. **Usos permitidos de la CUENTA**

6.1. Redacción, envío, reenvío y recepción de mensajes de correo electrónico y archivos adjuntos, correspondientes con la actividad del USUARIO por su relación laboral con la UNAM.

6.2.Resguardo de mensajes enviados, recibidos, reenviados y borradores, así como archivos asociados, hasta el máximo del ALMACENAMIENTO otorgado menos un 10% (diez por ciento)

6.3. Como identificador en otros servicios digitales proporcionados exclusivamente por la UNAM.

7**. Restricciones en el uso de la CUENTA**

7.1. Cualquier uso distinto a los permitidos por cualquier medio, dispositivo, sistema o servicio, conocido o por conocer, en línea o fuera de línea, proporcionado por terceros.

7.2. Está prohibido transferir el uso y la responsabilidad de la CUENTA a un tercero, bajo cualquier circunstancia. Todo mensaje enviado, reenviado o almacenado por un tercero en la CUENTA es responsabilidad absoluta del USUARIO.

7.3. Está prohibido el uso de la CUENTA con fines de lucro, así como para el ofrecimiento o solicitud de bienes y servicios personales.

7.4. Está prohibido el uso de la CUENTA en acciones que transgredan el marco normativo de la UNAM y sus objetivos institucionales.

7.5. Está prohibido el uso de la CUENTA en acciones que alteren la convivencia pacífica y el respeto a la diversidad cultural, ética y personal, en actos que vayan en contra de la igualdad, la libertad de pensamiento y del respeto y la tolerancia o que atenten contra la privacidad y la protección de información personal.

7.6. Está prohibido el uso de la CUENTA para difundir mensajes o actos deshonestos, falsos, violentos, que pongan en riesgo la integridad y seguridad física de personas o su patrimonio, que alteren el respeto al medio ambiente, o que no vigilen la propiedad intelectual o la protección a la autoría intelectual.

8. **Mantenimiento de la CUENTA**

8.1. El USUARIO debe mantener el consumo del espacio de ALMACENAMIENTO asignado por debajo de un 90% (noventa por ciento) con el propósito de garantizar que la mayoría de los mensajes que reciba puedan ser entregados con sus respectivos archivos adjuntos.

8.2. Es responsabilidad del USUARIO realizar respaldos de la información contenida en la CUENTA de manera periódica.

8.3. Los respaldos que el USUARIO realice de la información contenida en su CUENTA deberán ubicarse en un medio o dispositivo de almacenamiento distinto al SERVICIO.

8.4. El USUARIO puede utilizar diversos dispositivos para acceder al contenido de la CUENTA, siendo su entera responsabilidad la configuración de esos dispositivos, clientes y programas de correo electrónico.

9. **Declaraciones del USUARIO.**

9.1. El USUARIO declara que conoce las presentes Políticas de Uso de la CUENTA y se obliga a emplearla únicamente para los usos permitidos, por lo que asume la responsabilidad por cualquier uso distinto a ellos, liberando a la UNAM de todo tipo de responsabilidad ante terceros por el uso de la CUENTA y la información contenida en ella.

9.2. El USUARIO declara que no posee otra CUENTA PERSONAL dentro del dominio @fmvz.unam.mx.

9.3. El USUARIO acepta que la FMVZ puede negarle la asignación de la CUENTA en caso de no cumplir con uno o más de los requisitos de asignación descritos en el punto 4 de estas Políticas de Uso.

9.4. El USUARIO reconoce que el contenido de la CUENTA PERSONAL será siempre confidencial y de su exclusivo uso individual, el IDENTIFICADOR de la cuenta es de conocimiento público y no será considerado nunca como dato personal, dato personal sensible o dato privado, a la vez que libera a la UNAM de cualquier responsabilidad en el uso que terceros den al IDENTIFICADOR asignado.

9.5. El USUARIO reconoce que el contenido de la CUENTA INSTITUCIONAL podrá ser liberado a terceros y asume la responsabilidad absoluta de la información contenida en la CUENTA INSTITUCIONAL.

9.6. El USUARIO declara que la CUENTA INSTITUCIONAL es transferible a otra persona al término del encargo, responsabilidad o relación laboral del primero con la UNAM.

9.7. El USUARIO acepta que su IDENTIFICADOR puede ser utilizado por la UNAM, sus entidades y dependencias, para enviarle información, avisos o notificaciones exclusivamente de carácter institucional a través de listas de distribución, estando en su pleno derecho el USUARIO de solicitar la remoción de su identificador de dichas listas de distribución a los administradores respectivos, quienes a su vez están obligados a comunicar el mecanismo para solicitar la remoción de sus listas de distribución.

9.8. El USUARIO acepta que la única razón para que persona distinta al USUARIO acceda a la información contenida en la CUENTA PERSONAL es la expuesta en el punto 3.5.

9.9. El USUARIO se obliga a cambiar la contraseña asignada por la FMVZ al momento de aprobar su solicitud cuando ingrese por primera vez a la interfaz Web del SERVICIO.

9.10. El USUARIO declara que conoce la Ley Orgánica, el Código de Ética y los objetivos institucionales de la UNAM, y que en el cumplimiento y observancia de ese marco normativo hará uso de la CUENTA asignada.

9.11. El USUARIO reconoce que el dominio @fmvz.unam.mx es propiedad de la UNAM, y que por tanto no puede hacer uso de ese dominio de forma personal, privativa, discrecional o en forma alguna que atente contra la institución, sus principios, código de ética y objetivos.

9.12. El USUARIO manifiesta que no usará la CUENTA en nombre de un tercero y no permitirá el acceso de un tercero a la información de su CUENTA.

9.13. El USUARIO se compromete a mantener la confidencialidad de su contraseña para el uso de la CUENTA y a no proporcionarla, bajo ninguna circunstancia.

9.14. El USUARIO se obliga a cumplir la totalidad de los aspectos de mantenimiento de la CUENTA descritos en las presentes Políticas de Uso.

9.15. El USUARIO reconoce que deberá requisitar y remitir a la FMVZ cualquier SOLICITUD de acción sobre la CUENTA

9.16. El USUARIO se compromete a notificar a la FMVZ por medio de mensaje a la cuenta computofmvz@unam.mx cualquier sospecha, comprobación o validación de riesgo de seguridad en la CUENTA tan pronto como sea de su conocimiento.

9.17. El USUARIO se obliga a notificar a la FMVZ, a la cuenta computofmvz@unam.mx, el final de su relación laboral o académica con la UNAM una vez que haya concluido el respaldo de la información contenida en la CUENTA o dentro de los 5 (cinco) días hábiles posteriores a la terminación de la relación laboral, lo que ocurra primero.

10. **Transitorios**

10.1. El uso oficial de la CUENTA iniciará a partir de la notificación de la misma, por escrito, al USUARIO.

10.2. La FMVZ podrá modificar las presentes Políticas en cualquier momento. Por lo tanto, al menos 15 días hábiles previos a la entrada en vigor de las nuevas Políticas de Uso, deberá hacerlas del conocimiento de los USUARIOS a través de avisos en las CUENTAS.

Recomendaciones generales y mejores prácticas para el uso de la cuenta de correo electrónico en dominio @fmvz.unam.mx

1. Conocer los lineamientos de Google, para el uso del buzón de correo.
2. Organizar en carpetas la información contenida en la CUENTA para optimizar su uso.
3. Eliminar los mensajes no deseados, mensajes no requeridos o no solicitados.
4. Realizar de manera periódica respaldos de la información contenida en la CUENTA, aún para el SERVICIO LOCAL.
5. Cambiar la contraseña de la CUENTA al menos cada 3 (tres) meses para asegurar la confidencialidad de su información.
6. Colocar una firma de texto en cada mensaje con el nombre completo del USUARIO y el aviso de confidencialidad emitido por la FMVZ.
7. No utilizar la contraseña para acceso a la CUENTA en algún otro servicio digital, de la UNAM o de terceros, conocido o por conocer.
8. No utilizar la CUENTA como identificador en otros servicios ajenos a la UNAM, tales como redes sociales, otras cuentas de correo electrónico, sistemas bancarios, plataformas de streaming y comercio electrónico, entre otros.

Última Actualización: 13/08/2021

Bitácora

Diciembre 2023

Formato de Bitácora de vulneraciones a los Sistemas de Información		
Nombre Sistema de Tratamiento		
Fecha del incidente		
Nombre de quien reporta el incidente		
Cargo		
Área universitaria		
Responsable del área		
Causa de la vulneración		
Componente(s) del sistema vulnerado(s)		
Cantidad de titulares de datos personales afectados		
Soporte de la información vulnerada	☐ Físico ☐Electrónico ☐Mixto	
Seleccione el tipo de vulneración	☐ Pérdida o extravío ☐Destrucción no autorizada	
	☐ Robo ☐Copia no autorizada	
	☐ Uso, acceso o tratamiento no autorizado	
	☐ Daño, alteración o modificación no autorizada	
Tipo de titular afectado	☐ Extranjeros ☐ Trabajadores ☐Menores de edad ☐ Alumnos ☐Estudiantes de movilidad nacional ☐ Profesores de asignatura ☐ Profesores de tiempo completo ☐Investigadores ☐ Técnicos Académicos ☐Proveedores o contratistas ☐ Terceros (visitantes, etc.)	
Tipo de datos personales Comprometidos	☐ Identificativos Laborales	
	☐ Datos Académicos	
	☐ Procedimientos administrativos / Judiciales / Procedimientos seguidos en forma de juicio	
	☐ Patrimonial ☐Salud ☐ Afiliaciones políticas o ideológicas	
	☐ Origen étnico ☐ Características Personales	
	☐ Vida Sexual ☐ Discapacidades	
Las acciones correctivas implementadas de forma inmediata y definitiva.	_____ _____	
Nombre y firma de quién reporta	Nombre y firma del administrador del sistema	Nombre y firma del titular del área