UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

DGECI
Dirección General de Cooperación e Internacionalización
UNAM

DIRECCIÓN GENERAL DE COOPERACIÓN E INTERNACIONALIZACIÓN
COORDINACIÓN DE SISTEMAS Y TECNOLOGÍAS DE LA INFORMACIÓN

ANEXOS DE LAS NORMAS COMPLEMENTARIAS SOBRE MEDIDAS DE SEGURIDAD TÉCNICAS, ADMINISTRATIVAS Y FÍSICAS PARA LA PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LA UNIVERSIDAD

SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES (SGSDP)

INTRODUCCIÓN

Dirección General de Cooperación e Internacionalización

Con la finalidad de organizar e integrar las acciones institucionales que fortalecen la proyección internacional de la UNAM, se han creado diversas oficinas de internacionalización en distintos momentos:

- 1955, Oficina de Intercambio Cultural y Becas
- 1961, Departamento de Intercambio Cultural, Relaciones Públicas y Becas
- 1970, Comisiones de Becas e Intercambio Académico
- 1977, Dirección General de Intercambio Académico
- 2000, Oficina de Colaboración Interinstitucional
- **2009, Dirección General de Cooperación e Internacionalización (DGECI)**

La creciente presencia de la UNAM así como sus consecuentes relaciones con Instituciones de Educación Superior (IES) de otros países, llevó a la creación en el año 2015 de la Coordinación de Relaciones y Asuntos Internacionales (CRAI), dependencia a la que se le ha encomendado consolidar la internacionalización, fortalecer las alianzas, y coordinar las políticas y acciones en beneficio de la comunidad universitaria; desde esa fecha, la DGECI fue adscrita a dicha Coordinación.

Esta Dirección General forma parte de la administración central y como tal, presta servicios y apoyo a las entidades académicas (facultades, escuelas, centros e institutos), a las coordinaciones (de la investigación científica, de humanidades, de difusión cultural, y de estudios de posgrado) y a las secretarías que encabezan dichas entidades, todo ello coordinado por la CRAI.

La DGECI se encarga fundamentalmente de fomentar y operar programas de cooperación, gestionando la suscripción de convenios de colaboración académica con IES internacionales y nacionales, así como de la operación de programas de intercambio estudiantil de licenciatura y de personal académico. Por otro lado, coadyuva en la planeación y desarrollo de estrategias para fortalecer la cooperación académica y la internacionalización de la UNAM con IES, delegaciones diplomáticas, redes de cooperación académica, asociaciones y organismos públicos y privados, tanto nacionales como extranjeros.

El presente documento contiene las medidas de seguridad administrativa, física y técnica aplicables a los sistemas de tratamiento de datos personales de la Dirección General de Cooperación e Internacionalización (DGECI), con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información personal que éstos contienen.

Su propósito es identificar y documentar los sistemas de gestión de tratamiento de datos personales que posee la DGECI, permitiendo identificar a los responsables, encargados y usuarios de cada sistema, así como las medidas de seguridad implementadas en cada uno de ellos.

El documento tiene como objetivo validar la seguridad implementada dentro de los sistemas gestionados por la DGECI. Es la versión 1.0 e incluye las medidas de seguridad técnicas y administrativas establecidas por la UNAM. El documento estará en constante evolución conforme se vayan cumpliendo las medidas implementadas o modificadas dentro de algún sistema de gestión.

El alcance del Sistema de Gestión de Seguridad de Datos Personales (SGSDP) de la DGECI se centra en proteger los datos personales tratados, incluidos los sensibles, que se recaben en los sistemas de gestión de la DGECI, respecto de accesos no autorizados ni de tratamientos distintos a los fines para los que fueron recabados.

SISTEMA DE GESTIÓN DE MOVILIDAD ESTUDIANTIL SALIENTE

La DGECI tiene como una de sus principales funciones la de gestionar y dar seguimiento a la movilidad saliente de licenciatura en sus diversas modalidades (semestral, estancias de investigación, cursos cortos o estancias de experiencia profesional).

Por tal motivo se creó el Sistema de Gestión de Movilidad Estudiantil Saliente (SGMES) con el fin de conocer el estatus y tener el control de todas las solicitudes permitiendo administrar la movilidad saliente internacional y nacional.

Este sistema recaba información personal con el objetivo de conocer a los aspirantes que participan en cualquiera de las convocatorias emitidas por la DGECI y puedan ser objeto de una asignación (lugar, apoyo económico o beca).

El detalle de los datos personales que se manejan en este sistema se describe en el Anexo 1 Inventario de sistemas de tratamiento de datos personales en el apartadoo **DGECI/SGMES.**

SISTEMA DE GESTIÓN DE MOVILIDAD ESTUDIANTIL ENTRANTE

La DGECI también es la encargada de gestionar y dar seguimiento a la movilidad estudiantil entrante en sus diversas modalidades (semestral, estancias de investigación, cursos cortos o estancias de experiencia profesional).

Por tal motivo se cuenta con el Sistema de Gestión de Movilidad Estudiantil Entrante (SGMEE)con el fin de tener una mejor gestión y control del ciclo de vida de las solicitudes, esto paraconocer el estatus y su comportamiento en todo el proceso de la movilidad, teniendo el controlde todas las gestiones realizadas en cada una de ellas.

Este sistema recaba información personal con el objetivo de conocer el perfil de los aspirantesque participan en cualquiera de las convocatorias emitidas por la DGECI y que desean realizarmovilidad estudiantil en las Entidades Académicas (EA) de la UNAM..

El detalle de los datos personales que se manejan en este sistema se describe en el Anexo 1 Inventario de sistemas de tratamiento de datos personales en el apartado **DGECI/SGMEE.**

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

El detalle de los roles y responsabilidades del personal que se encarga de gestionar y establecer las medidas de seguridad de datos personales en los sistemas SGMES y SGMEE, se describen en el Anexo 2 funciones y responsabilidades de los involucrados en el tratamiento de datos personales en el apartado **DGECI/SGMES y DGECI/SGMEE.**

DGECI/SGMES
Sistema de Gestión de Movilidad Estudiantil Saliente
Responsabilidades en el tratamiento de datos personales
Crear las convocatorias de movilidad dentro del sistema.
Configurar y definir los datos personales solicitados en las convocatorias de movilidad.
Autorizar la liberación de las convocatorias previamente configuradas.
Notificar a los Responsables de Movilidad Estudiantil (RME) y Responsables de Internacionalización (RURI) la apertura del registro de aspirantes de las convocatorias.
Revisar los documentos y datos personales de las solicitudes registradas por los titulares.
Validar la información de los documentos que contengan datos personales de las solicitudes registradas en el sistema.
Gestionar la información de los datos personales de las solicitudes registradas en el sistema.
Salvaguardar la información física y electrónica de los titulares de los datos personales.
Establecer el canal de comunicación con las IES de destino.
Proteger los datos personales contenidos en el sistema de accesos no autorizados.
Comunicar y transferir información de los titulares de los datos personales.
Proteger los equipos de trabajo utilizados para la gestión de documentos con datos personales.
Generar los respaldos del sistema.
Asegurar el mecanismo para evitar accesos no autorizados al sistema.
Actualizar y verificar la seguridad del servidor donde se alojan los sistemas de tratamiento de datos personales.
Actualizar y verificar la seguridad y comportamiento del sistema de gestión.
Establecer las políticas para el uso y aseguramiento de los datos personales en las convocatorias.
Implementar mejora continua al sistema.

DGECI/SGMEE
Sistema de Gestión de Movilidad Estudiantil Entrante
Responsabilidades en el tratamiento de datos personales
Crear las convocatorias de movilidad dentro del sistema.
Configurar y definir los datos personales solicitados en las convocatorias de movilidad.
Autorizar la liberación de las convocatorias previamente configuradas.
Notificar a los responsables de movilidad estudiantil de las IES contraparte la apertura del registro de aspirantes de las convocatorias.
Revisar los documentos y datos personales de las solicitudes registradas por los titulares.
Validar la información de los documentos que contengan datos personales de las solicitudes registradas en el sistema.

Gestionar la información de los datos personales de las solicitudes registradas en el sistema.
Salvaguardar la información física y electrónica de los titulares de los datos personales.
Establecer el canal de comunicación con las EA de la UNAM.
Proteger los datos personales contenidos en el sistema de accesos no autorizados.
Comunicar y transferir información de los titulares de los datos personales.
Proteger los equipos de trabajo utilizados para la gestión de documentos con datos personales.
Generar respaldos del sistema.
Asegurar el mecanismo para evitar accesos no autorizados al sistema.
Actualizar y verificar la seguridad del servidor donde se alojan los sistemas de tratamiento de datos personales.
Actualizar y verificar la seguridad y comportamiento del sistema de gestión.
Establecer las políticas para el uso y aseguramiento de los datos personales en las convocatorias.
Implementar mejora continua al sistema.

Análisis de riesgos

La DGECI cuenta con un análisis de riesgo que considera puntos críticos importantes para mantener la seguridad en el tratamiento de datos personales en los sistemas gestionados por los responsables y encargados:

1. Identificación de los principales riesgos.
2. Priorización del impacto de cada riesgo.
3. Definición de acciones para mitigar el riesgo.
4. Asignación de tiempos para erradicar el riesgo.

El detalle del análisis de riesgo se encuentra incluido en el Anexo 4 Análisis de Riesgo.

Análisis de Brecha

La DGECI cuenta con un análisis de brecha que describe las mejoras necesarias para mitigar los riesgos previamente identificados. Contiene las medidas de seguridad necesarias a realizar, describiendo las acciones para solventar el riesgo.

El detalle del análisis de riesgo se encuentra incluido en el Anexo 5 Análisis de Brecha

Plan de Trabajo

La DGECI cuenta con un plan de trabajo donde se identifican los controles de seguridad faltantes, la descripción de la actividad a desarrollar, el tiempo que tardará la implementación de dicho control que reforzará la seguridad del tratamiento de datos personales.

El detalle del plan de trabajo se encuentra incluido en el Anexo 6 Plan de trabajo

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

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

- 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 esta versión 1.0 del documento se registran las actividades realizadas para cumplir con lo dispuesto para la etapa 1 en el Anexo 7. Cumplimiento de las MST.

DENOMINACIÓN DE LAS ÁREAS INVOLUCRADAS

ÁREA	IDENTIFICADOR	DESCRIPCIÓN
Dirección General de Cooperación e Internacionalización	**DGECI**	La DGECI se encarga fundamentalmente de fomentar y operar programas de cooperación, gestionando la suscripción de convenios de colaboración académica con Instituciones de Educación Superior (IES) internacionales y nacionales, así como de la operación de programas de intercambio estudiantil de licenciatura como de académicos. Por otro lado, coadyuva en la planeación y desarrollo de estrategias para fortalecer la cooperación académica y la internacionalización de la UNAM con IES, delegaciones diplomáticas, redes de cooperación académica, asociaciones y organismos públicos y privados, tanto nacionales como extranjeros.
Dirección General	**DG**	Instancia que dirige la dependencia, responsable de establecer y liderar las estrategias para el cumplimiento de los objetivos institucionales. Supervisa las funciones administrativas de las áreas que la conforman.
Dirección de Intercambio y Movilidad Estudiantil	**DIME**	Dirección encargada de planear, gestionar y evaluar los programas de movilidad y de becas para los alumnos de licenciatura de la UNAM que realizan actividades académicas en instituciones extranjeras y/o nacionales, así como la movilidad de estudiantes extranjeros y nacionales que realizan actividades académicas en la UNAM.
Dirección de Cooperación Académica	**DCA**	Dirección encargada de identificar y apoyar las alianzas de colaboración con IES internacionales y nacionales, a través de la suscripción de acuerdos que deriven en la implementación de programas de intercambio estudiantil y colaboración académica.
Subdirección de Enlace Institucional	**SEI**	Subdirección encargada de planear, gestionar y dirigir las estrategias y acciones destinadas a fortalecer la vinculación entre entidades académicas y dependencias de la UNAM, con IES y organismos públicos y privados, internacionales y nacionales para el desarrollo y coordinación de proyectos de internacionalización.
Unidad Administrativa	**UA**	Unidad encargada de administrar los recursos humanos, financieros y materiales, así como, coordinar los servicios de apoyo para el cumplimiento de sus objetivos y metas institucionales conforme a la normatividad aplicable y al Sistema de Gestión de la Calidad.
Coordinación Jurídica	**CJ**	Coordinación encargada de proporcionar apoyo jurídico a las diferentes áreas de la dependencia. También es esencial en el desarrollo de los convenios de la dependencia.
Coordinación de Tecnologías de la Información	**CTI**	Coordinación encargada del desarrollo, administración y mantenimiento de los sistemas de internacionalización y movilidad.

ANEXO 1

INVENTARIO DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

ENERO 2024

V1.2

Área**s: DGECI (DIME, DCA, SEI y CTI)**	
Identificador único	**DGECI/SGMES**
Nombre del sistema	**Sistema de Gestión de Movilidad Estudiantil Saliente**
Datos personales (sensibles o no sensibles) contenidos en el sistema:	• **Datos de identificación**: Nombre completo, sexo, fotografía, domicilio en México, teléfono particular, teléfono celular, teléfono oficina, correo electrónico1, correo electrónico2, estado civil, firma, firma digital, RFC, CURP, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, domicilio georreferenciado, país destino, datos de una persona de contacto para casos de emergencia (nombre, teléfono fijo, teléfono móvil, correo electrónico, parentesco con el alumno) y de un beneficiario designado por el alumno (nombre, fecha de nacimiento, parentesco con el alumno). • **Datos académicos**: Número de cuenta UNAM, licenciatura, plantel, área de conocimiento, idiomas, tipo de certificado de idioma y puntaje, semestre en curso, avance de créditos, promedio, último periodo de registro, generación, vigencia, último semestre inscrito, clave de plan de estudios, nombre del plan de estudios, modalidad. • **Datos patrimoniales**: Ingreso mensual familiar, número de familiares dependientes, cuenta clabe personal. • **Datos apoyos económicos previos o vigentes**: Becas DGECI, manutención, transporte, alimentación. • **Datos de tránsito y movimientos migratorios:** Itinerario de viaje, domicilio en el extranjero o nacional. • **Datos personales sensibles**: Origen racial o étnico, discapacidad. • **Documentos que se agregan al sistema y contienen datos personales:** Identificación oficial, carta de motivos, carta de aceptación IES, oficio de postulación de la Entidad Académica (EA), comprobante de domicilio, pasaporte, CURP, certificado de idioma, documento de visado, currículum vitae, historia académica, oficio de postulación DGECI, dictamen de revalidación, comprobante de inscripción, carta compromiso, comprobantes de ingresos, declaratoria o documento referente al origen étnico o racial, aprobación del consejo, carta de invitación, respuesta del comité de evaluación, programa de trabajo, comprobante o certificado de discapacidad, proyecto de investigación, carta de aceptación de la Sede de la UNAM en el Extranjero, expediente IES, expediente DGECI, carta beca, cronograma de actividades, póliza de seguro de gastos médicos mayores, itinerario de viaje, comprobante de inscripción IES, dictamen de revalidación de la EA, dictamen de revalidación final de la EA, certificado de calificaciones IES, historia académica con revalidación, reporte de impactos, título académico o acta de examen de titulación, comprobante de servicio social, certificado de bachillerato, formato course selection, programa académico, carta de recomendación académica, comprobante de registro de Santander, contrato de estudios,
Responsable:	**Dirección de Intercambio y Movilidad Estudiantil**
Nombre:	**Mtra. Brenda Gasca Zambrano**
Cargo:	**Directora de Intercambio y Movilidad Estudiantil**
Funciones:	• Validar la configuración de las convocatorias de becas y movilidad estudiantil internacional y nacional emitidas por la DIME. • Autorizar la liberación de las convocatorias de becas y movilidad estudiantil internacional y nacional emitidas por la DIME. • Consultar información de los datos personales de las solicitudes registradas en el sistema. • Establecer el canal de comunicación con las instituciones destino para la movilidad internacional y nacional.

Obligaciones:	• Salvaguardar la información de los titulares de los datos personales. • Comunicar y transferir la información mínima necesaria para el cumplimiento de los objetivos de las convocatorias de becas y movilidad estudiantil. • No compartir los datos personales de los titulares con terceros no involucrados con el proceso la movilidad y gestión de becas. • No vender o comercializar los datos personales de los titulares por ningún motivo.
Responsable:	**Dirección de Cooperación Académica**
Nombre:	**Mtra. Jessica Carpinteiro Martínez**
Cargo:	**Directora de Cooperación Académica**
Funciones:	• Validar la configuración de las convocatorias de apoyos económicos de movilidad estudiantil emitidas por la DCA. • Autorizar la liberación de las convocatorias de apoyos económicos de movilidad estudiantil emitidas por la DCA. • Consultar información de los datos personales de las solicitudes registradas en el sistema. • Validar la configuración del Comité de Selección que evalúa la asignación de apoyos económicos. • Establecer el canal de comunicación con las instancias destino para la movilidad internacional.
Obligaciones:	• Salvaguardar la información de los titulares de los datos personales. • Comunicar y transferir la información mínima necesaria para el cumplimiento de los objetivos de las convocatorias de apoyos económicos. • No compartir los datos personales de los titulares con terceros no involucrados con el proceso la movilidad y gestión de los apoyos económicos. • No vender o comercializar los datos personales de los titulares por ningún motivo.
Responsable:	**Subdirección de Enlace Institucional**
Nombre:	**Mtra. María Dolores Gabriela González Casanova Fernández**
Cargo:	**Subdirectora de Enlace Institucional**
Funciones:	• Validar la configuración de las convocatorias de apoyos económicos de movilidad académica emitidas por la SEI. • Autorizar la liberación de las convocatorias de apoyos económicos de movilidad académica emitidas por la SEI. • Consultar información de los datos personales de las solicitudes registradas en el sistema. • Validar la configuración del Comité de Selección que evalúa la asignación de apoyos económicos.

Obligaciones:	• Comunicar los resultados de las convocatorias emitidas por la DGECI a las entidades académicas de la UNAM correspondientes. • Salvaguardar la información de los titulares de datos personales. • Comunicar y transferir la información mínima necesaria para el cumplimiento de los objetivos de las convocatorias de apoyos económicos. • No compartir los datos personales de los titulares con terceros no involucrados con el proceso la movilidad y gestión de los apoyos económicos. • No vender o comercializar los datos personales de los titulares por ningún motivo.
Encargados:	**Dirección General de Cooperación e Internacionalización**
Nombre del encargado 1:	**L.I. Luis Alfonso Baeza Villalobos**
Cargo:	**Coordinador de Tecnologías de la Información**
Funciones:	• Crear nuevos usuarios y asignar privilegios de acceso. • Apoyar en la configuración de convocatorias de movilidad gestionadas por la DGECI. • Actualizar y modificar usuarios.
Obligaciones:	• Salvaguardar la información de los titulares de los datos personales. • Implementar las herramientas necesarias para la seguridad de las plataformas institucionales. • Generar los respaldos de los datos contenidos en las plataformas, siguiendo la política de respaldos de la DGECI. • Validar el buen funcionamiento de las plataformas institucionales. • Validar la seguridad de los servidores donde se alojan las plataformas de la DGECI. • Coordinar los proyectos de TI de la dependencia • No compartir los datos personales de los titulares con terceros no involucrados con la movilidad. • No vender o comercializar los datos personales de los titulares por ningún motivo.
Nombre del encargado 2:	**Mtro. Idelfonso De la Cruz Hernández**
Cargo:	**Jefe de Área de Tecnologías de la Información**
Funciones:	• Dar mantenimiento a la plataforma. • Actualizar y modificar el flujo de negocio de la plataforma.
Obligaciones:	• Salvaguardar la información de los titulares de los datos personales. • Implementar las herramientas necesarias para la seguridad de las plataformas institucionales. • Generar los respaldos de los datos contenidos en las plataformas, siguiendo la política de respaldos de la DGECI. • Validar el buen funcionamiento de las plataformas institucionales. • No compartir los datos personales de los titulares con terceros no involucrados con la movilidad. • No vender o comercializar los datos personales de los titulares por ningún motivo.

Nombre encargado 3:	**Lic. Edith Andrea Martínez Lazcano**
Cargo:	**Coordinadora de Movilidad Estudiantil Saliente**
Funciones:	• Gestionar la información de los titulares de los datos personales que registran una solicitud de participación en las convocatorias de movilidad estudiantil internacional y nacional que gestiona la DIME. • Analizar la información en búsqueda de posibles omisiones en las solicitudes registradas en el sistema. • Configurar las convocatorias de movilidad estudiantil internacional y nacional gestionadas por la DIME. • Validar la liberación de las convocatorias de movilidad estudiantil internacional y nacional gestionadas por la DIME. • Validar la información de los alumnos (titulares de los datos personales) de forma integral y completa. • Consultar información de las solicitudes registradas en el sistema. • Realizar trámites internos de validación o cancelación de solicitudes. • Establecer el canal de comunicación con las instituciones origen para la integración de movilidad internacional y nacional.
Obligaciones:	• Salvaguardar la información de los titulares de los datos personales. • Notificar a los titulares de datos personales, cambios y agregados de cualquier dato personal. • Comunicar y transferir la información mínima necesaria para el cumplimiento de los requisitos de la aplicación a una beca económica. • No compartir los datos personales de los titulares con terceros no involucrados con la movilidad internacional y nacional. • No vender o comercializar los datos personales de los titulares por ningún motivo.
Nombre del encargado 4:	**Mtra. Jeanneth Miramontes Mejía**
Cargo:	**Delegada Administrativa**
Funciones:	• Gestionar la información de los titulares de los datos personales que registran una solicitud de participación en las convocatorias de movilidad estudiantil internacional y nacional que gestiona la DIME. • Analizar la información en búsqueda de posibles omisiones en las solicitudes registradas en el sistema. • Validar solicitudes de movilidad estudiantil internacional y nacional para postular con las IES contrapartes. • Consultar información de las solicitudes registradas en el sistema. • Realizar trámites internos de validación o cancelación de solicitudes.
Obligaciones:	• Salvaguardar la información de los titulares de los datos personales. • Notificar a los titulares de datos personales, cambios y agregados de cualquier dato personal. • No compartir los datos personales de los titulares con terceros no involucrados con la movilidad internacional y nacional. • No vender o comercializar los datos personales de los titulares por ningún motivo.

Nombre del encargado 5:	**Socorro Camacho Olalde**
Cargo:	**Asistente Ejecutiva**
Funciones:	• Gestionar la información de los titulares de los datos personales que registran una solicitud de participación en las convocatorias de movilidad estudiantil internacional y nacional que gestiona la DIME. • Analizar la información en búsqueda de posibles omisiones en las solicitudes registradas en el sistema. • Validar solicitudes de movilidad estudiantil internacional y nacional para postular con las IES contrapartes. • Consultar información de las solicitudes registradas en el sistema. • Realizar trámites internos de validación o cancelación de solicitudes.
Obligaciones:	• Salvaguardar la información de los titulares de los datos personales. • Notificar a los titulares de datos personales, cambios y agregados de cualquier dato personal. • No compartir los datos personales de los titulares con terceros no involucrados con la movilidad internacional y nacional. • No vender o comercializar los datos personales de los titulares por ningún motivo.
Nombre del encargado 6:	**Mtra. Mariana Ramírez Hernández**
Cargo:	**Jefa del Departamento de Cooperación Académica**
Funciones:	• Gestionar la información de los titulares de los datos personales que registran una solicitud de participación en las convocatorias de movilidad estudiantil internacional que gestiona la DCA. • Analizar la información en búsqueda de posibles omisiones en las solicitudes registradas en el sistema. • Configurar las convocatorias de movilidad estudiantil internacional gestionadas por la DCA. • Validar la información de los alumnos (titulares de los datos personales) de forma integral y completa. • Validar las solicitudes con base en los resultados emitidos por el Comité de Selección de las convocatorias de movilidad estudiantil que gestiona la DCA. • Consultar información de las solicitudes registradas en el sistema. • Realizar trámites internos de validación o cancelación de solicitudes.
Obligaciones:	• Salvaguardar la información de los titulares de los datos personales. • Notificar a los titulares de datos personales, cambios y agregados de cualquier dato personal. • No compartir los datos personales de los titulares con terceros no involucrados con la movilidad internacional y nacional. • No vender o comercializar los datos personales de los titulares por ningún motivo.

Nombre del encargado 7:	**Lic. Ana María Matute Trejo**
Cargo:	**Asistente de procesos**
Funciones:	• Gestionar la información de los titulares de los datos personales que registran una solicitud de participación en las convocatorias de movilidad académica que gestiona la SEI. • Analizar la información en búsqueda de posibles omisiones en las solicitudes registradas en el sistema. • Configurar las convocatorias de movilidad académica gestionadas por la SEI. • Validar la información de los académicos (titulares de los datos personales) de forma integral y completa. • Validar las solicitudes con base en los resultados emitidos por el Comité de Selección de las convocatorias de movilidad académica que gestiona la SEI. • Consultar información de las solicitudes registradas en el sistema. • Realizar trámites internos de validación o cancelación de solicitudes.
Obligaciones:	• Salvaguardar la información de los titulares de los datos personales. • Notificar a los titulares de datos personales, cambios y agregados de cualquier dato personal. • No compartir los datos personales de los titulares con terceros no involucrados con la movilidad internacional y nacional. • No vender o comercializar los datos personales de los titulares por ningún motivo.
Usuarios:	**Dirección General de Cooperación e Internacionalización**
Nombre del usuario:	**Anexo Lista Usuarios_RME_RURI_SGMES.docx**
Cargo:	**Responsable de Movilidad Estudiantil (RME)** **Representante de la Red Universitaria de Responsables de Internacionalización (RURI)**
Funciones:	• Generar las solicitudes de movilidad estudiantil y académica de su entidad académica en las convocatorias activas. • Gestionar y revisar los datos personales de los titulares de su entidad, que presentan solicitudes de movilidad estudiantil y académica. • Notificar a los titulares respecto a la detección de errores u omisiones en la información de las solicitudes registradas para que realicen las correcciones que, en su caso, correspondan. • Validar las solicitudes de movilidad estudiantil y académica de su entidad. • Priorizar las solicitudes de movilidad estudiantil y académica de su entidad. • Consultar información de las solicitudes registradas en el sistema de su entidad. • Realizar trámites internos de validación de solicitudes.
Obligaciones:	• Salvaguardar la información de los titulares de los datos personales de su entidad académica. • Notificar a los titulares de datos personales, cambios y agregados de cualquier dato personal de su entidad académica. • No compartir los datos personales de los titulares con terceros no involucrados con la movilidad estudiantil y académica de su entidad. • No vender o comercializar los datos personales de los titulares por ningún motivo.

Áreas: DGECI (DIME y CTI)	
Identificador único	**DGECI/SGMEE**
Nombre del Sistema	**Sistema de Gestión de Movilidad Estudiantil Entrante**
Datos personales (sensibles o no sensibles) contenidos en el sistema:	• **Datos de identificación**: Nombre completo, sexo, fotografía,domicilio país de origen, domicilio y contacto en México,teléfono particular, teléfono celular, teléfono oficina, correoelectrónico1, correo electrónico2, estado civil, CURP, NSS,INE, número de pasaporte, fecha vencimiento pasaporte,país que emite el pasaporte, lugar de nacimiento, fecha denacimiento, nacionalidad, nombres de contacto deemergencia y de beneficiario, relación o parentesco, fecha denacimiento del contacto, teléfono de casa, teléfono celular. • **Datos académicos**: Número de cuenta, universidad de origen, escuela o facultad, campus, licenciatura o grado, idiomas, certificado de idioma y puntaje, semestre cursando, total de semestres de la licenciatura, avance en créditos, promedio general, número total de créditos, entidad académica UNAM destino, carrera destino UNAM. • **Datos patrimoniales**: Seguro(s). • **Datos apoyos económicos**: Fuentes de financiamiento durante la movilidad, becas, manutención. • **Datos de tránsito y movimientos migratorios**: Formato migratorio FMM2, FMM3, visa, itinerario de vuelo ida y vuelta. • **Datos personales sensibles**: Discapacidades. • **Documentos que se agregan al sistema y contienen datos personales:** Historia académica oficial, comprobantede inscripción semestre actual, carta de motivos, carta derecomendación, pasaporte vigente, carta VISA para embajada, forma migratoria múltiple, certificado de español,Protocolo o proyecto, seguro facultativo IMSS, formato deseguro de prácticas de campo, carta de invitación del tutor,Pago de equivalencia del promedio, identificación oficial,CURP, carta compromiso, póliza de seguro de gastosmédicos, itinerario de viaje, comprobante de inscripciónUNAM, certificado UNAM, carta de postulación de la IESorigen, carta de aceptación de la EA destino, carta aceptaciónUNAM-DGECI, carta derechos imagen, cambio domicilioadscripción IMSS.
Responsable:	**Dirección de Intercambio y Movilidad Estudiantil**
Nombre:	**Mtra. Brenda Gasca Zambrano**
Cargo:	**Directora de Intercambio y Movilidad Estudiantil**
Funciones:	• Validar la configuración de las convocatorias de becas y movilidad estudiantil internacional y nacional emitidas por la DIME. • Autorizar la liberación de las convocatorias de becas y movilidad estudiantil internacional y nacional emitidas por la DIME. • Consultar información de los datos personales de las solicitudes registradas en el sistema. • Establecer el canal de comunicación con las instituciones destino para la movilidad internacional y nacional.
Obligaciones:	• Salvaguardar la información de los titulares de los datos personales. • Comunicar y transferir la información mínima necesaria para el cumplimiento de los objetivos de las convocatorias de becas y movilidad estudiantil. • No compartir los datos personales de los titulares con terceros no involucrados con el proceso la movilidad y gestión de becas. • No vender o comercializar los datos personales de los titulares por ningún motivo.

Encargados:	**Dirección General de Cooperación e Internacionalización**
Nombre del encargado 1:	**L.I. Luis Alfonso Baeza Villalobos**
Cargo:	**Coordinador de Tecnologías de la Información**
Funciones:	• Crear nuevos usuarios y asignar privilegios de acceso. • Apoyar en la configuración de convocatorias de movilidad gestionadas por la DGECI. • Actualizar y modificar usuarios.
Obligaciones:	• Salvaguardar la información de los titulares de los datos personales. • Implementar las herramientas necesarias para la seguridad de las plataformas institucionales. • Generar los respaldos de los datos contenidos en las plataformas, siguiendo la política de respaldos de la DGECI. • Validar el buen funcionamiento de las plataformas institucionales. • Validar la seguridad de los servidores donde se alojan las plataformas de la DGECI. • Coordinar los proyectos de TI de la dependencia • No compartir los datos personales de los titulares con terceros no involucrados con la movilidad. • No vender o comercializar los datos personales de los titulares por ningún motivo.
Nombre del encargado 2:	**Act. José Ernesto Fernández Muñoz**
Cargo:	**Jefe de Departamento de Cómputo y Sistemas**
Funciones:	• Dar mantenimiento a la plataforma. • Actualizar y modificar usuarios. • Actualizar y modificar nombre de las IES. • Apoyar en el seguimiento de la operación de la movilidad en cualquier etapa.
Obligaciones:	• Salvaguardar la información de los titulares de los datos personales. • Implementar las herramientas necesarias para la seguridad de las plataformas institucionales. • Generar los respaldos de los datos contenidos en las plataformas, siguiendo la política de respaldos de la DGECI. • Validar el buen funcionamiento de las plataformas institucionales. • No compartir los datos personales de los titulares con terceros no involucrados con la movilidad. • No vender o comercializar los datos personales de los titulares por ningún motivo.
Nombre del encargado 3:	**Mtro. Idelfonso de la Cruz Hernández**
Cargo:	**Jefe de Área de Tecnologías de la Información**
Funciones:	• Dar mantenimiento a la plataforma. • Actualizar y modificar funciones.
Obligaciones:	• Salvaguardar la información de los titulares de los datos personales. • Implementar las herramientas necesarias para la seguridad de las plataformas institucionales. • Generar los respaldos de los datos contenidos en las plataformas, siguiendo la política de respaldos de la DGECI. • Validar el buen funcionamiento de las plataformas institucionales. • No compartir los datos personales de los titulares con terceros no involucrados con la movilidad. • No vender o comercializar los datos personales de los titulares por ningún motivo.

Nombre del encargado 4:	**Esp. Carlos Eduardo Navarro Rojas**
Cargo:	**Jefe de Departamento de Movilidad Entrante**
Funciones:	• Gestionar la información de los titulares de los datos personales que registran una solicitud de participación en las convocatorias de movilidad estudiantil internacional y nacional que gestiona la DIME. • Analizar la información en búsqueda de posibles omisiones en las solicitudes registradas en el sistema. • Configurar las convocatorias de movilidad estudiantil internacional y nacional gestionadas por la DIME. • Validar la liberación de las convocatorias de movilidad estudiantil internacional y nacional gestionadas por la DIME. • Validar la información de los estudiantes (titulares de los datos personales) de forma integral y completa. • Consultar información de las solicitudes registradas en el sistema. • Realizar trámites internos de validación o cancelación de solicitudes. • Postular a los estudiantes (titulares de los datos personales) en las entidades académicas de la UNAM. • Establecer el canal de comunicación con las instituciones origen para la integración de movilidad internacional y nacional.
Obligaciones:	• Salvaguardar la información de los titulares de los datos personales. • Notificar a los titulares de datos personales, cambios y agregados de cualquier dato personal. • Comunicar y transferir la información mínima necesaria para el cumplimiento de los requisitos de la aplicación a una beca económica. • No compartir los datos personales de los titulares con terceros no involucrados con la movilidad internacional y nacional. • No vender o comercializar los datos personales de los titulares por ningún motivo.
Nombre del encargado 5:	**Lic. Fabiola Sebastiana Silva Reyes**
Cargo:	**Jefe de Área de Movilidad Estudiantil Entrante**
Funciones:	• Gestionar la información de los titulares de los datos personales que registran una solicitud de participación en las convocatorias de movilidad estudiantil internacional y nacional que gestiona la DIME. • Analizar la información en búsqueda de posibles omisiones en las solicitudes registradas en el sistema. • Validar la información de los estudiantes (titulares de los datos personales) de forma integral y completa. • Consultar información de las solicitudes registradas en el sistema. • Realizar trámites internos de validación o cancelación de solicitudes. • Postular a los estudiantes (titulares de los datos personales) en las entidades académicas de la UNAM. • Establecer el canal de comunicación con las instituciones origen para la integración de movilidad internacional y nacional.

Obligaciones:	• Salvaguardar la información de los titulares de los datos personales. • Notificar a los titulares de datos personales, cambios y agregados de cualquier dato personal. • Comunicar y transferir la información mínima necesaria para el cumplimiento de los requisitos de la aplicación a una beca económica. • No compartir los datos personales de los titulares con terceros no involucrados con la movilidad internacional y nacional. • No vender o comercializar los datos personales de los titulares por ningún motivo.
Nombre del encargado 6:	**Javier Enciso** Pérez
Cargo:	**Jefe de Área de Movilidad Estudiantil Entrante**
Funciones:	• Gestionar la información de los titulares de los datos personales que registran una solicitud de participación en las convocatorias de movilidad estudiantil internacional y nacional que gestiona la DIME. • Analizar la información en búsqueda de posibles omisiones en las solicitudes registradas en el sistema. • Validar la información de los estudiantes (titulares de los datos personales) de forma integral y completa. • Consultar información de las solicitudes registradas en el sistema. • Realizar trámites internos de validación o cancelación de solicitudes. • Postular a los estudiantes (titulares de los datos personales) en las entidades académicas de la UNAM. • Establecer el canal de comunicación con las instituciones origen para la integración de movilidad internacional y nacional.
Obligaciones:	• Salvaguardar la información de los titulares de los datos personales. • Notificar a los titulares de datos personales, cambios y agregados de cualquier dato personal. • Comunicar y transferir la información mínima necesaria para el cumplimiento de los requisitos de la aplicación a una beca económica. • No compartir los datos personales de los titulares con terceros no involucrados con la movilidad internacional y nacional. • No vender o comercializar los datos personales de los titulares por ningún motivo.
Usuarios:	**Dirección General de Cooperación e Internacionalización**
Nombre del usuario:	**Anexo Lista Usuarios_RME_EA _IES_SGMEE.docx**
Cargo:	**Responsable de Movilidad Estudiantil (RME) de entidades académicas (EA)** **Responsable de Movilidad Estudiantil en Instituciones de Educación Superior (IES)**

Funciones:	• Generar las solicitudes de movilidad estudiantil de su institución en las convocatorias activas. • Gestionar y revisar los datos personales de los titulares de su institución, que presentan solicitudes de movilidad estudiantil. • Notificar a los titulares respecto a la detección de errores u omisiones en la información de las solicitudes registradas para que realicen las correcciones que, en su caso, correspondan. • Validar las solicitudes de movilidad estudiantil de su institución. • Priorizar las solicitudes de movilidad estudiantil de su institución. • Consultar información de las solicitudes registradas en el sistema de su institución. • Realizar trámites internos de validación de solicitudes.
Obligaciones:	• Salvaguardar la información de los titulares de los datos personales de su institución. • Notificar a los titulares de datos personales, cambios y agregados de cualquier dato personal de su institución. • No compartir los datos personales de los titulares con terceros no involucrados con la movilidad estudiantil de su institución. • No vender o comercializar los datos personales de los titulares por ningún motivo.

ANEXO 2

FUNCIONES Y OBLIGACIONES DE QUIENES TRATAN DATOS PERSONALES

ENERO 2024

V1.2

		Áreas DGECI: DIME, DCA, SEI, CJ y CTI
Identificador único	**ESTRUCTURA/DGECI**	
Director General -DG-	**Mtro. Gerardo Reza Calderón**	**Titular de la Dependencia**
Directora de Intercambio y Movilidad Estudiantil -DIME-	**Mtra. Brenda Gasca Zambrano**	**Responsable de Datos Personales**
Directora de Cooperación Académica -DCA-	**Mtra. Jessica Carpinteiro Martínez**	**Responsable de Datos Personales**
Subdirección de Enlace Institucional -SEI-	**Mtra. María Dolores Gabriela González Casanova Fernández**	**Responsable de Datos Personales**
Coordinador de Tecnologías de la Información -CTI-	**L.I. Luis Alfonso Baeza Villalobos**	**Encargado de la Seguridad de Datos Personales**
Jefe de Departamento de Cómputo y Sistemas-CT -CTI-	**Act. José Ernesto Fernández Muñoz**	**Enlace de Transparencia**
Coordinadora Jurídica -CJ-	**Mtra. Verónica Rivas San Vicente**	**Asesora en Datos Personales**
Gestores de Movilidad -GM-	**Lic. Edith Andrea Martínez Lazcano Mtra. Jeanneth Miramontes Mejía Socorro Camacho Olalde Esp. Carlos Eduardo Navarro Rojas Lic. Fabiola Sebastiana Silva Reyes Javier Enciso Pérez Mtra. Mariana Ramírez Hernández Lic. Ana María Matute Trejo**	**Encargados de la Gestión Datos Personales**

Áreas DGECI: DIME, DCA, SEI, CJ y CTI	
Identificador único	**DSDP/DGECI**
Nombre del sistema	**Elaboración del Documento de Seguridad de Datos Personales (DSDP)**

Tratamiento de datos personales	DG	DIME	DCA	SEI	CTI	CJ
Elaboración de políticas y objetivos del DSDP.	X	X	X	X	X	X
Definir las funciones y obligaciones.	X	X	X	X	X	
Elaborar el inventario de datos personales de los sistemas.	X	X	X	X	X	
Elaborar el análisis de riesgo del tratamiento de datos personales.	X				X	
Elaborar el análisis de brecha de las medidas de seguridad del tratamiento de datos personales.	X				X	
Implementación de las Medidas de Seguridad en los sistemas de gestión.					X	
Elaboración de talles de capacitación para el personal de DGECI con respecto al manejo de datos personales.					X	X
Revisión y validación de DSDP.	X				X	X

Áreas DGECI: DIME, DCA, SEI y CTI	
Identificador único	**DGECI/SGMES**
Nombre del sistema	**Sistema de Gestión de Movilidad Estudiantil Saliente**
Soporte electrónico correspondiente a las convocatorias emitidas por la DGECI	

Tratamiento de datos personales	DG	DIME	DCA	SEI	CTI	CJ	GM
Crear las convocatorias de movilidad dentro del sistema.		X	X	X	X		
Configurar y definir los datos personales solicitados en las convocatorias de movilidad.		X	X	X	X	X	
Autorizar la liberación de las convocatorias previamente configuradas.	X	X	X	X			
Notificar a los Responsables de Movilidad Estudiantil (RME) y Responsables de Internacionalización (RURI) la apertura del registro de aspirantes de las convocatorias.		X	X	X			X
Revisar los documentos y datos personales de las solicitudes registradas por los titulares.					X		X

Validar la información de los documentos que contengan datos personales de las solicitudes registradas en el sistema.							X
Gestionar la información de los datos personales de las solicitudes registradas en el sistema.							X
Salvaguardar la información física y electrónica de los titulares de los datos personales.		X	X	X	X		X
Establecer el canal de comunicación con las IES de destino.		X	X	X			
Proteger los datos personales contenidos en el sistema de accesos no autorizados.					X		X
Comunicar y transferir información de los titulares de los datos personales.	X	X					
Proteger los equipos de trabajo utilizados para la gestión de documentos con datos personales.	X	X	X	X	X	X	X
Generar los respaldos del sistema.					X		
Asegurar el mecanismo para evitar accesos no autorizados al sistema.					X		
Actualizar y verificar la seguridad del servidor donde se alojan los sistemas de tratamiento de datos personales.					X		
Actualizar y verificar la seguridad y comportamiento del sistema de gestión.					X		
Establecer las políticas para el uso y aseguramiento de los datos personales en las convocatorias.	X				X	X	
Implementar mejora continua al sistema.					X		

Identificador único	DGECI/SGMEE				
Nombre del sistema	**Sistema de Gestión de Movilidad Estudiantil Entrante**				
Soporte electrónico correspondiente a las convocatorias emitidas por la DIME					
Tratamiento de datos personales	**DG**	**DIME**	**CTI**	**CJ**	**GM**
Crear las convocatorias de movilidad dentro del sistema.		X	X		
Configurar y definir los datos personales solicitados en las convocatorias de movilidad.		X	X	X	
Autorizar la liberación de las convocatorias previamente configuradas.	X	X			
Notificar a los responsables de movilidad Estudiantil de las IES contraparte la apertura del registro de aspirantes de las convocatorias.		X			X
Revisar los documentos y datos personales de las solicitudes registradas por los titulares.					X
Validar la información de los documentos que contengan datos personales de las solicitudes registradas en el sistema.					X
Gestionar la información de los datos personales de las solicitudes registradas en el sistema.					X
Salvaguardar la información física y electrónica de los titulares de los datos personales.		X	X		X
Establecer el canal de comunicación con las EA de la UNAM.		X			X
Proteger los datos personales contenidos en el sistema de accesos no autorizados.		X			X
Comunicar y transferir información de los titulares de los datos personales.		X			X
Proteger los equipos de trabajo utilizados para la gestión de documentos con datos personales.	X	X	X	X	X
Generar los respaldos del sistema.			X		
Asegurar el mecanismo para evitar accesos no autorizados al sistema.			X		
Actualizar y verificar la seguridad del servidor donde se alojan los sistemas de tratamiento de datos personales.			X		
Actualizar y verificar la seguridad y comportamiento del sistema de gestión.			X		
Establecer las políticas para el uso y aseguramiento de los datos personales en las convocatorias.	X	X	X		
Implementar mejora continua al sistema.			X		

ANEXO 3

ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

La información de este Anexo se clasifica como reservada por un periodo de 5 años, a partir del 19 de agosto de 2022, de conformidad con lo dispuesto en los artículos 104, fracciones I, II y III, 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

AGOSTO 2022

V1.1

ANEXO 4

ANÁLISIS DE RIESGOS

La información de este Anexo se clasifica como reservada por un periodo de 5 años, a partir del 19 de agosto de 2022, de conformidad con lo dispuesto en los artículos 104, fracciones I, II y III, 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

AGOSTO 2022

V1.1

ANEXO 5

ANÁLISIS DE BRECHA

La información de este Anexo se clasifica como reservada por un periodo de 5 años, a partir del 19 de agosto de 2022, de conformidad con lo dispuesto en los artículos 104, fracciones I, II y III, 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

AGOSTO 2022

V1.1

ANEXO 6

PLAN DE TRABAJO

La información de este Anexo se clasifica como reservada por un periodo de 5 años, a partir del 19 de agosto de 2022, de conformidad con lo dispuesto en los artículos 104, fracciones I, II y III, 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

AGOSTO 2022

V1.1

ANEXO 7

CUMPLIMIENTO DE LAS MST

AGOSTO 2022

V1.1

SISTEMA DE GESTIÓN DE MOVILIDAD			(SGM)	
Formato	**1**	**Verificación anual**	**Acción concluida**	(X)
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**	
L.I. Luis Alfonso Baeza Villalobos			15 de marzo de 2020	
Nombre y firma Programador, desarrollador o diseñador del sistema de información			**Fecha término** 15 de marzo de 2020	
Observaciones / anotaciones		Se revisaron las tablas que contienen datos personales en los ambientes de desarrollo y se cambiaron por datos ficticios. Los ambientes están controlados en 3 capas. Ambiente de desarrollo donde las tablas alumno, alumno_conctacto, domicilio alumno, intento_acceso_alumno_log, seguimiento_solicitud, solicitud_paeci, sol_alumno_historico, users; se encuentran con datos personales ficticios y configuraciones de convocatorias ficticias. Ambiente QA donde las tablas alumno, alumno_conctacto se encuentran con datos personales ficticios y con configuraciones de convocatorias reales. Ambiente de producción.		

SISTEMA DE GESTIÓN DE MOVILIDAD			(SGM)	
Formato:	**2**	**Verificación anual**	**Acción concluida**	(X)
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**	
L.I. Luis Alfonso Baeza Villalobos			15 de marzo de 2020	
Nombre y firma			**Fecha término**	
Administrador del sistema de información			15 de marzo de 2020	
Observaciones / anotaciones		Se creo un usuario con privilegios SELECT, UPDATE, INSERT, CALL para la base de datos productiva y se eliminaron todos los privilegios de todos los usuarios estándar a producción.		

SISTEMA DE GESTIÓN DE MOVILIDAD			(SGM)	
Formato:	**3**	**Verificación anual**	**Acción concluida**	(X)
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**	
L.I. Luis Alfonso Baeza Villalobos			16 de marzo de 2020	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor			18 de marzo de 2020	
Observaciones / anotaciones	Se realizó la renovación del SSL 26 de marzo de 2021. Se configuraron SSL tipo wildcard para tener control de los dominios *.unaminternacional.unam.mx, certificado generado por la DGTIC.			

VEEAM DGECI				
Formato:	**4**	**Verificación anual**	**Acción concluida**	(X)
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**	
L.I. Luis Alfonso Baeza Villalobos			18 de marzo de 2020	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor			20 de marzo de 2020	
Observaciones / anotaciones	DGTIC entregó el acceso al BaaS el 20 de enero de 2021. Los respaldos del SGM se realizan de forma automática con doble periodicidad (diario y semanal).			

Equipo de cómputo y sistemas				
Formato:	**5**	**Verificación anual**	**Acción concluida**	(X)
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**	
L.I. Luis Alfonso Baeza Villalobos			23 de marzo de 2020	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor			23 de marzo de 2020	
Observaciones / anotaciones	La CTI realiza un formato por cada equipo para la baja, así mismo el equipo permanece en la bodega para bajas y se da aviso a la UA para la entrega del equipo para su baja.			

SERVIDORES FÍSICOS Y VIRTUALES				
Formato:	**6**	**Verificación anual**	**Acción concluida**	(X)
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**	
L.I. Luis Alfonso Baeza Villalobos			21 de marzo de 2020	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor			21 de marzo de 2020	
Observaciones / anotaciones	Se configuraron los servidores físicos y virtuales con el servidor NTP de la UNAM.			

SERVIDORES FÍSICOS Y VIRTUALES, EQUIPOS DE OFICINA				
Formato:	**7**	**Verificación anual**	**Acción concluida**	(X)
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 *antimalware* 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**	
L.I. Luis Alfonso Baeza Villalobos			25 de marzo de 2020	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor			27 de marzo de 2020	
Observaciones / anotaciones		Se tiene activo el antivirus clamAV, HIDS y SELINUX para monitorear el estatus del servidor físico y virtual. Se tiene activo el antivirus Karspersky en los equipos de cómputo de la oficina. Se verifica el comportamiento de estas herramientas diario. Esta revisión verifica el hostname, la bitácora de evento y la detección de actividad maliciosa.		

SERVIDORES FÍSICOS Y VIRTUALES, EQUIPOS DE OFICINA				
Formato:	**8**	**Verificación anual**	**Acción concluida**	(X)
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**	
L.I. Luis Alfonso Baeza Villalobos			30 de marzo de 2020	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor			02 de abril de 2020	
Observaciones / anotaciones		Se planifica la actualización de seguridad de servidor cada 6 meses. Se verifican los componentes de seguridad del servidor web, del HIDS, de la base de datos, del repositorio de documentos.		

SISTEMA DE GESTIÓN DE MOVILIDAD			**SGM**	
Formato:	**9**	**Verificación anual**	**Acción concluida**	(X)
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**	
L.I. Luis Alfonso Baeza Villalobos			06 de abril de 2020	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor			10 de abril de 2020	
Observaciones / anotaciones		La plataforma está definida por perfiles de acceso jerárquico, que permite a la CTI administrar la plataforma y a la DIME, DCA y SEI gestionar la información completa de cada convocatoria y registro.		

SISTEMA DE GESTIÓN DE MOVILIDAD			SGM	
Formato:	**10**	**Verificación anual**	**Acción concluida**	(X)
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**
L.I. Luis Alfonso Baeza Villalobos	13 de abril de 2020
Nombre y firma	**Fecha término**
Administrador del sistema de información o servidor	15 de abril de 2020

Observaciones / anotaciones	Se implementó un mecanismo de no instalación de SW ajeno al necesario para el funcionamiento de la plataforma.

SISTEMA DE GESTIÓN DE MOVILIDAD			**SGM**	
Formato:	**11**	**Verificación anual**	**Acción concluida**	(X)
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**	
L.I. Luis Alfonso Baeza Villalobos			16 de abril de 2020	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor			17 de abril de 2020	
Observaciones / anotaciones		Los servidores se encuentran en el centro de datos de la DGTIC, cumpliendo con las medidas de seguridad físicas. La DGTIC cuenta con el plano de seguridad perimetral del centro de datos y la DGECI se rige bajo sus estatutos.		

SISTEMA DE GESTIÓN DE MOVILIDAD			SGM	
Formato:	**12**	**Verificación anual**	**Acción concluida**	(X)
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**	
L.I. Luis Alfonso Baeza Villalobos			20 de abril de 2020	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor			21 de abril de 2020	
Observaciones / anotaciones		La Unidad Administrativa realiza el control de la salida de equipo de cómputo, describiendo el recurso solicitado con el VoBo del Departamento de Servicios y Suministros. La CTI tendrá el control del equipo que se solicita para salida o entrada dentro de la dependencia.		

SISTEMA DE GESTIÓN DE MOVILIDAD			SGM	
Formato:	**13**	**Verificación anual**	**Acción concluida**	(X)
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**	
L.I. Luis Alfonso Baeza Villalobos			21 de abril de 2020	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor			21 de abril de 2020	
Observaciones / anotaciones				

SISTEMA DE GESTIÓN DE MOVILIDAD			SGM	
Formato:	**14**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:		**Artículo 20. Aplicar el procedimiento de borrado seguro que impida la recuperación en las bases de datos y todos sus respaldos.**		
Aplicable en:		Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Tres días hábiles.		
Importancia de la acción:		Se debe verificar que el procedimiento de borrado seguro es funcional y que el dato no persiste en función del tipo de borrado (registro, tabla, base, sistema).		
Proceso recomendado:		**A)** Realizar una copia integral del sistema de información y colocarla en un servicio temporal. *Por ejemplo:* máquina virtual directorio temporal en el servidor. **B)** Ingresar a la copia del sistema de información y realizar el borrado de un registro. Verificar que el dato no persiste en la base de datos por medio de forma de consulta o comando. **C)** Realizar el mismo proceso del punto B para una tabla y finalmente para la base de datos completa. D) En caso de persistencia del dato, instalar y ejecutar herramientas para borrado seguro. *Por ejemplo*: en Linux se dispone *de shred, wipe, secure-delete, srm, sfill, sswap, sdmem,* que se pueden instalar desde el administrador de aplicaciones. **D)** Llenar y firmar este formato.		
Mejores prácticas, referencias:		**1.-** Se recomienda usar al menos un comando a nivel de sistema operativo para el borrado seguro de conformidad con el procedimiento establecido.		
Conocimientos requeridos:		Administración de sistema operativo. Instalación de aplicaciones. Gestión de archivos.		
Ejecución			**Fecha inicio**	
L.I. Luis Alfonso Baeza Villalobos			22 de abril de 2020	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor			24 de abril de 2020	
Observaciones / anotaciones				

SISTEMA DE GESTIÓN DE MOVILIDAD			SGM	
Formato:	**15**	**Verificación anual**	**Acción concluida**	(X)
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**	
L.I. Luis Alfonso Baeza Villalobos			27 de abril de 2020	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor			27 de abril de 2020	
Observaciones / anotaciones				

SISTEMA DE GESTIÓN DE MOVILIDAD			SGM	
Formato:	**16**	**Verificación anual**	**Acción concluida**	(X)
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**	
L.I. Luis Alfonso Baeza Villalobos			11 de mayo de 2020	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor			20 de mayo de 2020	
Observaciones / anotaciones				

SISTEMA DE GESTIÓN DE MOVILIDAD			SGM	
Formato:	**17**	**Verificación anual**	**Acción concluida**	(X)
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**	
L.I. Luis Alfonso Baeza Villalobos			21 de mayo de 2020	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor			26 de mayo de 2020	
Observaciones / anotaciones				

SISTEMA DE GESTIÓN DE MOVILIDAD			**SGM**	
Formato:	**18**	**Verificación anual**	**Acción concluida**	(X)
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**	
L.I. Luis Alfonso Baeza Villalobos			27 de mayo de 2020	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor			8 de junio de 2020	
Observaciones / anotaciones				

SISTEMA DE GESTIÓN DE MOVILIDAD			SGM	
Formato:	**19**	**Verificación anual**	**Acción concluida**	(X)
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 xxx@google.com, deberá cambiarse por una cuenta del tipo xxxx@unam.mx **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Nunca deben usarse cuentas, servicios, suscripciones, licencias o cualquier otro elemento informático cuyo control dependa de una sola persona.		
Conocimientos requeridos:		Administración de sistema de información. Gestión de bases de datos.		
Ejecución			**Fecha inicio**	
L.I. Luis Alfonso Baeza Villalobos			9 de junio de 2020	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor			4 de agosto de 2020	
Observaciones / anotaciones				

SISTEMA DE GESTIÓN DE MOVILIDAD			SGM	
Formato:	**20**	**Verificación anual**	**Acción concluida**	(X)
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**	
L.I. Luis Alfonso Baeza Villalobos			5 de agosto de 2020	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor			10 de agosto de 2020	
Observaciones / anotaciones				

SISTEMA DE GESTIÓN DE MOVILIDAD			SGM	
Formato:	**21**	**Verificación anual**	**Acción concluida**	(X)
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**	
L.I. Luis Alfonso Baeza Villalobos			11 de agosto de 2020	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor			14 de agosto de 2020	
Observaciones / anotaciones				

SISTEMA DE GESTIÓN DE MOVILIDAD			**SGM**	
Formato:	**22**	**Verificación anual**	**Acción concluida**	(X)
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**	
L.I. Luis Alfonso Baeza Villalobos			17 de agosto de 2020	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor			21 de agosto de 2020	
Observaciones / anotaciones				

SISTEMA DE GESTIÓN DE MOVILIDAD			SGM	
Formato:	**23**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:		**Artículo 18. I. b) Contar con entornos para desarrollo, pruebas y operación.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Veinte días hábiles.		
Importancia de la acción:		Para evitar riesgos innecesarios a la información, el desarrollo y actualización de los mismos deberá ser realizado siempre en una plataforma y ambientes por separado.		
Proceso recomendado:		**A)** Instalar y configurar equipos similares en características, preferentemente virtuales, a los equipos donde se instalará el sistema de información en su nueva o actualizada versión. **B)** Crear un repositorio en un equipo central de desarrollo para el resguardo de códigos, documentación, inventarios de datos y manuales de usuario, administrador y programador. **C)** Ejecutar las pruebas de nuevas versiones o actualizaciones del sistema de información en el equipo dispuesto para tal efecto. Nunca usar -equipos físicos o virtuales con el sistema actualmente en producción como las plataformas para evaluación de versiones en desarrollo. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Se deben realizar respaldos de la información en los sistemas en desarrollo del mismo modo que como se realicen con el sistema en producción.		
Conocimientos requeridos:		Administración de sistema de información. Desarrollo de aplicaciones.		
Ejecución			**Fecha inicio**	
L.I. Luis Alfonso Baeza Villalobos			24 de agosto de 2020	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor			18 de septiembre de 2020	
Observaciones / anotaciones				

SISTEMA DE GESTIÓN DE MOVILIDAD			SGM	
Formato:	**24**	**Verificación anual**	**Acción concluida**	(X)
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**	
L.I. Luis Alfonso Baeza Villalobos			21 de septiembre de 2020	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor			9 de octubre de 2020	
Observaciones / anotaciones				

SISTEMA DE GESTIÓN DE MOVILIDAD			**SGM**	
Formato:	**25**	**Verificación anual**	**Acción concluida**	(X)
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**	
L.I. Luis Alfonso Baeza Villalobos			12 de octubre de 2020	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor			13 de octubre de 2020	
Observaciones / anotaciones				

SISTEMA DE GESTIÓN DE MOVILIDAD			SGM	
Formato:	**26**	**Verificación anual**	**Acción concluida**	(X)
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**	
L.I. Luis Alfonso Baeza Villalobos			14 de octubre de 2020	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor			16 de octubre de 2020	
Observaciones / anotaciones				

SISTEMA DE GESTIÓN DE MOVILIDAD			SGM	
Formato:	**27**	**Verificación anual**	**Acción concluida**	(X)
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**	
L.I. Luis Alfonso Baeza Villalobos			12 de octubre de 2020	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor			13 de octubre de 2020	
Observaciones / anotaciones				

SISTEMA DE GESTIÓN DE MOVILIDAD			**SGM**	
Formato:	**28**	**Verificación anual**	**Acción concluida**	(X)
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**	
L.I. Luis Alfonso Baeza Villalobos			26 de octubre de 2020	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor			6 de noviembre de 2020	
Observaciones / anotaciones				

ANEXO 8

POLÍTICAS DE RESPALDO

La información de este Anexo se clasifica como reservada por un periodo de 5 años, a partir del 19 de agosto de 2022, de conformidad con lo dispuesto en los artículos 104, fracciones I, II y III, 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

AGOSTO 2022

V1.1

ANEXO 9

POLÍTICAS DE ACTUALIZACIÓN

AGOSTO 2022

V1.1

OBJETIVO

Definir el procedimiento necesario para la actualización de sistemas operativos, paqueterías necesarias para el buen funcionamiento de estos, así como el software antimalware y antivirus utilizado para la protección de los sistemas de gestión y los servidores y equipos de cómputo de la DGECI.

ALCANCE

Las presentes políticas definen la periodicidad para la actualización de sistemas operativos, paqueterías y software antimalware y antivirus conforme a los niveles de criticidad de los equipos de cómputo de la DGECI.

RESPONSABILIDADES

Es responsabilidad de la CTI de la DGECI realizar la configuración inicial de los equipos de cómputo asignados al personal: funcionarios, administrativos, de confianza y de base para llevar a cabo sus labores correspondientes en la DGECI.

La CTI debe realizar las siguientes acciones en los equipos de oficina de la DGECI:

- Establecer los periodos en los equipos de cómputo para la implementación de actualizaciones o parches de seguridad necesarios para un rendimiento óptimo y seguro
- Actualizar en todo el equipo de cómputo de la DGECI el software antimalware o antivirus que cumpla con la protección necesaria para los usuarios de la DGECI
- Instalar o actualizar el software necesario para el desempeño de las funciones diarias de los usuarios que utilizan los equipos de cómputo

La CTI realiza las siguientes acciones en los servidores donde se alojan los sistemas de gestión de la DGECI:

- Instalar o actualizar las paqueterías, parches de seguridad o software agregado necesario para el buen funcionamiento de los servidores y equipos de red bajo su responsabilidad
- Instalar el software necesario que permita el monitoreo de la seguridad en tiempo real y de aviso de una posible intrusión externa que comprometa los datos personales de los titulares
- Llevar el control de las actualizaciones críticas implementadas en cada servidor para su buen funcionamiento

Sobre la forma de interacción y responsabilidad del personal de la DGECI que cuenta con un equipo asignado, se procede de la siguiente manera:

- Contactar a la CTI en caso de un incidente que comprometa al equipo de cómputo en el manejo de datos personales
- Contactar a la CTI cuando el equipo indique una necesidad de actualizar
- Analizar con el antivirus los dispositivos extraíbles que conecten a su equipo de cómputo
- Conectar dispositivos extraíbles de confianza adquiridos por la CTI o UA
- Informar a la CTI cuando se desea instalar algún software nuevo para realizar alguna actividad especifica

ACTUALIZACIONES

Las actualizaciones por parte de los equipos de desarrollo de los diferentes sistemas operativos o software instalado se validan cada cierto tiempo para mejorar, prevenir, parchar o rectificar fallas que imposibilitan el buen uso del sistema o software. Por ello, es indispensable que las actualizaciones o recomendaciones se instalen de forma periódica en dichos equipos de desarrollo.

Cumpliendo con los requerimientos solicitados por las MST se debe tener en cuenta que una acumulación de actualizaciones sin aplicar en cualquier equipo, ya sea servidor o equipo de oficina, compromete la seguridad de este y se expone más a un ataque, virus o malware y pueda explotar alguna vulnerabilidad afectando o exponiendo la seguridad de los sistemas de gestión que contiene datos persónales.

La CTI realiza actualizaciones de performance, seguridad y mejoras de los servidores productivos conforme a lo siguiente:

- No se permite la instalación de software incompleto en versión beta o similar
- Las actualizaciones deberán estar verificadas por la página oficial de la aplicación o sistema operativo
- Se deberán probar los cambios en el ambiente QA antes de liberar a producción
- Los servicios se reinician por aplicativo llevando un control de la hora de inicio y fin del proceso
- Los reinicios generales deberán ser reportados a la CTI, quien analizara el impacto de esta acción avisando a los posibles afectados para la toma de precauciones
- Los reinicios generales se realizarán en un horario que no afecte demasiado el fuljo de trabajo de la DGECI

La CTI realiza actualizaciones de performance, seguridad y mejoras de los equipos de cómputo utilizados por el personal de la DGECI conforme a lo siguiente:

- Verifica que las actualizaciones automáticas se encuentren activas dentro de los equipos de cómputo
- Verifica que los equipos de cómputo cuenten con el software antivirus actualizado con la versión oficial adquirida para la DGECI
- Asigna las VPN actualizadas a los equipos móbiles que requieran una conexión segura a la red UNAM
- Asegura que los usuarios no instalen paqueterías o software, dichas actualizaciones estarán a cargo de la CTI
- Realiza una vez concluida la fase de mantenimiento a nivel hardware, un proceso de análisis de actualizaciones mayores del sistema operativo, paqueterías o software a los equipos. Buscando complementar las medidas de seguridad con la actualización del momento

PERIODICIDAD

La periodicidad implementada para las actualizaciones en los equipos de cómputo, servidores, entre otros, del personal de la DGECI se realiza de la siguiente forma:

- Verificar que tenga instalado el sistema operativo Windows 10
- Verificar los parches de seguridad complementarios liberados en los boletines de Microsoft necesarios para el buen funcionamiento del equipo cada fin de mes
- Verificar los parches o actualizaciones críticas liberadas cada seis meses validando que se instale correctamente dicho parche

CONTROL DE CAMBIOS

Todas las actualizaciones a los equipos cuentan con una bitácora para conocer el estado de este, que describe cuando se realizó la acción, así como la eventualidad o problema que resolvió.

BITACORA DE ACTUALIZACIONES			
ELABORÓ	**FECHA**	**TIPO ACTUALIZACIÓN**	**MOTIVO**
		☐ **S.O WIN** ☐ **S.O LIN** ☐ **Base de Datos** ☐ **Servidor Web** ☐ **Antivirus** ☐ **Lenguaje** ☐ **Otro**	☐ **Critica** ☐ **Seguridad** ☐ **Opcional** ☐ **Mantenimiento**

ANEXO 10

POLÍTICAS DE BORRADO SEGURO

AGOSTO 2022

V1.1

OBJETIVO

Definir el procedimiento necesario para implementar el borrado seguro a los sistemas operativos, archivos, directorios, bases de datos, ubicados dentro de los equipos de cómputo y servidores de la DGECI.

ALCANCE

El borrado seguro es una medida a través de la que se establecen métodos y técnicas para la eliminación definitiva de los datos, de modo que la probabilidad de recuperarlos sea mínima. Por lo que en la DGECI resulta importante el establecimiento de un procedimiento de eliminación adecuada en los medios de almacenamiento en desuso, porque representa una medida de seguridad efectiva para minimizar las fugas o el mal uso de los datos personales por parte de una persona mal intencionada o no autorizada.

RESPONSABILIDADES

Es responsabilidad de cada uno de los directores, subdirectores y coordinadores de las áreas funcionales de la DGECI dar aviso a la CTI sobre la necesidad de los cambios del equipo entre el personal, describiendo el motivo y si el equipo contiene o gestionó datos personales. Es responsabilidad de la Unidad Administrativa de la DGECI, llevar el control del inventario completo de la asignación o bajas del equipo de cómputo de oficina o servidores de la DGECI.

La CTI tiene como responsabilidad borrar la información de forma segura de los equipos que se van a dar de baja y de los equipos que van a ser reasignados previa solicitud. La información para eliminar puede ser: información sensible, reservada o que contenga datos personales de la comunidad UNAM, fotos, documentos, música, videos o cualquier otro tipo de archivo de los equipos de cómputo de la DGECI.

Es responsabilidad de la CTI de la DGECI implementar un procedimiento para la eliminación adecuada de cualquier medio de almacenamiento ubicado dentro de los quipos de oficina o de los servidores de la DGECI.

La CTI debe realizar las siguientes acciones en los equipos de oficina de la DGECI:

PROCESOS DE BORRADO Y ELIMINACIÓN DE LA INFORMACIÓN EN EQUIPOS WINDOWS

En la DGECI utilizamos varios métodos de borrado en los medios extraíbles de almacenamiento de la información, dentro de los cuales destacan los siguientes:

Formato desde otro medio extraíble: En el caso de los discos duros, se formatean desde un DVD o USB externos para eliminar la información desde un disco de arranque del sistema operativo. Esta acción se realiza, principalmente, en discos duros de equipos que se reasignan dentro de la misma dependencia. El proceso puede variar de entre 30 a 45 minutos, dependiendo del equipo así como del procesador.

> 1) Crear disco de inicio o arranque del S.O. 2) Insertar un disco en la PC o laptop y reiniciar el sistema. 3) Entrar al BIOS y elegir el medio extraíble como inicio. 4) Seguir los pasos en pantalla eligiendo opciones de borrado personalizado y total. 5) Eliminar particiones. 6) Formatear la unidad. 7) Instalar el S.O. 8) Configurar el S.O.

Reinicio desde el sistema operativo. Este proceso se utiliza cuando no se cuenta con algún medio extraíble para reinstalar el sistema operativo, se realiza desde el mismo Windows a través de la configuración del sistema. El proceso tarda entre 40 a 60 minutos y se realiza cuando se reasigna un equipo dentro de la misma dependencia.

> 1) Menú inicio y seleccionar “configuración”. 2) Elegir la opción “actualización y seguridad”. 3) Seleccionar “recuperación”. 4) Elegir la opción de “reestablecer” y continuar con la configuración en la pantalla solicitada.

En la CTI se cuenta con un hardware de la marca StratTech, para dos unidades SATA de 2.5" a 3.5", que funciona sin necesidad de conectarse a un equipo de cómputo. Dicho hardware realiza un borrado por sector, eliminando todo tipo de particiones por lo que el disco queda sin ejecución a menos que se instale un nuevo sistema operativo. El proceso tarda entre 60 y 90 minutos y proporciona el borrado completo para la no recuperación de la información.

1) Se conecta a la corriente eléctrica el hardware. 2) Se inserta el disco duro en una de las entradas o slots. 3) Se enciende el hardware. 4) En la parte trasera hay un botón el cual se presiona por 15 segundos indicados por los leds de la parte frontal que se encenderán y apagarán. 4) Comenzará a parpadear el primer led y se deja trabajando el hardware. 5) Esperar a que los 4 leds estén encendidos sin parpadear.

	Áreas DGECI: CTI
Sistema operativo	**WINDOWS**
Proceso	**Descripción**
Formateo de los discos duros	• Herramienta eraser de archivos, en todo el disco • Herramienta lógica Wipe My Disks de HDDGURU • Herramienta física Start Tech para formateo bit a bit en disco SATA de 2.5" a 3.5"

PROCESOS DE BORRADO Y ELIMINACIÓN DE LA INFORMACIÓN EN EQUIPOS GNU/LINUX

Se utilizan las siguientes herramientas para el borrado seguro de archivos y/o discos duros, ya sea en equipos de oficina o servidores.

	Áreas DGECI: CTI
Sistema operativo	**GNU/LINUX**
Proceso	**Descripción**
Borrado seguro de archivos para equipos	• Herramienta shred para el borrado seguro de los archivos delicados en equipos GNU/Linux • Herramienta srm para el borrado seguro de los directorios delicados en equipos GNU/Linux
Formateo de los discos duros	• Herramienta lógica hdparm para equipos GNU/Linux • Herramienta física Start Tech para formateo bit a bit en disco SATA de 2.5" a 3.5"

MOTIVOS

Para la implementación de un borrado seguro en cualquier equipo de cómputo, dispositivo o medio de almacenamiento se debe cumplir uno de solo siguientes supuestos:

- Baja de equipo por obsolescencia
- Baja de equipo por descompostura
- Reasignación de equipo interna de la DGECI
- Reasignación a una dependencia diferente a la DGECI
- Solicitante exigiendo la cancelación de sus datos personales

BITACORA

El borrado seguro cuentan con una bitácora que permite conocer las acciones aplicadas, describiendo cuando se realizó la acción, así como la eventualidad o problema que resolvió.

BITACORA BOORADO SEGURO				
ACCIÓN	**ELABORÓ**	**FECHA**	**TIPO BORRADO**	**MOTIVO**
			☐ **S.O WIN** ☐ **S.O LIN** ☐ **Base de Datos** ☐ **Documentos**	☐ **Baja equipo** ☐ **Reasignación** ☐ **Solicitud**

VALIDACIONES		
Validó	**Elaboró**	**Autorizó**

ANEXO 11

BITÁCORA

AGOSTO 2022

V1.1

DGECI
Dirección General de Cooperación e Internacionalización
UNAM

BITACORA DE VULNERACIONES

FORMATO DE IDENTIFICACIÓN DE INCIDENTES

INFORMACIÓN DE LA PERSONA QUE DETECTA UN INCIDENTE

Nombre			
Cargo			
Área **universitaria**			
Responsable del área			
Correo		**Teléfono**	

INFORMACIÓN SOBRE EL INCIDENTE

Sistema vulnerado		
Causa de vulneración		
Pérdida o robo de Datos Personales	☐ **SI**	☐ **NO**
Tipo de titular afectado	☐ **Alumno UNAM** ☐ **Estudiante internacional** ☐ **Estudiante nacional**	☐ **Trabajador UNAM** ☐ **Académico UNAM** ☐ **Académico internacional** ☐ **Académico nacional**
Tipo de dato comprometido	☐ **Identificativos** ☐ **Laborales** ☐ **Académicos**	☐ **Sensibles** ☐ **Patrimoniales**
Datos personales involucrados		
Descripción del incidente		
FECHA		**HORA**

INFORMACIÓN TÉCNICA DEL INCIDENTE

☐ **Robo o pérdida**	☐ **Uso no autorizado**
☐ **Denegación del servicio**	☐ **Acceso no autorizado**
☐ **Código malicioso**	☐ **Ingeniería social personal**
☐ **Modificación no autorizada**	☐ **Daño físico al servidor**
☐ **Otro**	

ACCIONES CORRECTIVAS DE MANERA INMEDIATA

VALIDACIONES

Nombre y firma de quien reporta	**Nombre y firma CTI**	**Nombre y firma CJ**	**Nombre y firma DG**

APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

Responsable del desarrollo:	**L.I. Luis Alfonso Baeza Villalobos** Coordinador de Tecnologías de la Información abaeza@global.unam.mx	
Revisó:	**Mtra. Verónica Rivas San Vicente** Coordinadora Jurídica veronica.rivas@global.unam.mx	
Autorizó:	**Mtro. Gerardo Reza Calderón** Director General de Cooperación e Internacionalización reza@global.unam.mx	
Fecha de aprobación:	**24 de agosto de 2022**	
Fecha de actualización:	**09 de enero de 2024**	

Enero 2024

V1.2