Universidad Nacional Autónoma de México

Instituto de Investigaciones Estéticas

DOCUMENTO DE SEGURIDAD
DE DATOS PERSONALES

Agosto 2022

V 1.1

Índice

Presentación

A nuestro Instituto lo distingue el peso de una tradición disciplinaria ocupada en forjar la historia del arte en este país a la luz de hallazgos artísticos significativos, investigaciones rigurosas, metodologías transversales y divulgación del conocimiento artístico, estético y patrimonial en expresiones que corren desde el arte antiguo hasta el arte contemporáneo. Hace más de ochenta años, un 20 de febrero de 1935, el historiador del arte y académico Manuel Toussaint y Ritter presentó las actas constitutivas del Laboratorio de Arte. Un año más tarde, el Laboratorio de Arte se convirtió en Instituto de Investigaciones Estéticas (IIE), y desde entonces a la fecha, el trabajo de las distintas generaciones de investigadores y técnicos académicos que han conformado nuestra comunidad ha abonado el camino, marcado por sus fundadores, en el primer tercio del siglo pasado: "hacer la historia de nuestras artes plásticas".

Hoy, a sus 85 años de existencia, el IIE se ha posicionado como un referente innegable en el estudio del arte mexicano, latinoamericano y de las prácticas artísticas y culturales en el contexto global.

Bajo el mismo deber universitario de pertenecer a la máxima casa de estudios, el IIE presente documento compila la forma en que el IIE implementa un Sistema de Gestión de la Seguridad de Datos Personales. Su alcance se concentra en la protección de los datos personales que recabe y el tratamiento que dará a ellos.

Introducción

El presente documento de seguridad constituye el instrumento que describe las medidas de seguridad administrativas, físicas y técnicas aplicables a los sistemas de tratamiento de datos personales del Instituto de Investigaciones Estéticas (IIE), con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información personal que éstos contienen.

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

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

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

El cimiento del formato del documento de seguridad es la aplicación de un enfoque basado en los riesgos de los activos universitarios, específicamente los datos personales y los soportes que los resguardan. Además, el formato considera el tamaño y estructura de la institución, objetivos, clasificación de la información, requerimientos de seguridad y procesos que se precisan en razón de los activos que posee esta Máxima Casa de Estudios, los cuales están contemplados en el estándar internacional en materia de seguridad de la información ISO/IEC 27002:2013 "Tecnología de la información - Técnicas de seguridad - Código de práctica para los controles de seguridad de la información".

Aplica a todas las áreas administrativas y técnico-académicas que tienen en su poder datos personales y datos personales sensibles.

Términos, definiciones y abreviaturas

Activo: Todo elemento de valor para la Universidad, involucrado en el tratamiento de datos personales, entre ellos, las bases de datos, el conocimiento de los procesos, el personal, el hardware, el software, los archivos o documentos en papel.

Aviso de privacidad: Documento a disposición del titular en forma física, electrónica o en cualquier formato generado por el *responsable*, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de éstos.

Bases de datos: Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

Borrado seguro: Procedimiento para la eliminación en un dispositivo o medio de almacenamiento, conocido o por conocer, que impide la recuperación de los datos personales.

Ciclo vital del documento: las tres fases por las que atraviesan los documentos de archivo, sea cual sea su soporte, desde su recepción o generación hasta su conservación permanente o baja documental, a saber: archivo de trámite, archivo de concentración y archivo histórico.

Confidencialidad: Es el principio de seguridad de la información que consiste en que la información no pueda estar disponible o divulgarse a personas o procesos no autorizados por el Área Universitaria respectiva.

Control de seguridad en la red: Configuración de equipo activo de telecomunicaciones y software para proteger la transmisión de datos personales.

Disponibilidad: Es el principio de seguridad de la información que consiste en ser accesible y utilizable a solicitud de personas o procesos autorizados por el Área Universitaria respectiva.

Documento de seguridad: Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el *responsable* para garantizar la Confidencialidad, Integridad y Disponibilidad de los datos personales que posee.

Encargado: La persona física o jurídica distinta a las áreas, entidades o dependencias universitarias, que realizan el tratamiento de los datos personales a nombre de la Universidad, suscribiendo para tal efecto los instrumentos consensuales correspondientes acordes con la Legislación Universitaria aplicable.

Integridad: Es el principio de seguridad de la información consistente en garantizar la exactitud y la completitud de la información y los sistemas, de manera que éstos no puedan ser modificados sin autorización, ya sea accidental o intencionalmente.

Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos técnicos administrativos y físicos que permitan proteger los datos personales.

Medidas de seguridad administrativas: Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional; la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales.

Medidas de seguridad físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento, los cuales pueden ser desde medidas preventivas, cotidianas y correctivas para tener un control de acceso, preservación, conservación de las instalaciones, recursos o bienes en los cuales se resguarda información e incluso a la información misma, asegurando así su disponibilidad e integridad. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

A. Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;
B. Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;
C. Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y
D. Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

Medidas de seguridad técnicas: Conjunto de acciones y mecanismos para proteger los datos personales que se encuentren en formato digital, así como los sistemas informáticos que les den tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

A. Asegurar que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados.
B. Generar un esquema de privilegios para que el usuario realice las actividades que requiere con motivo de sus funciones.
C. Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware.
D. Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

Red de datos: Conjunto de componentes electrónicos activos y medios de comunicación conocidos o por conocer tales como fibra óptica, enlaces inalámbricos, cable, entre otros, que permiten el intercambio de paquetes de datos entre dispositivos electrónicos para el procesamiento de información.

Responsable: Las áreas universitarias que manejan, resguardan y/o deciden sobre el tratamiento de datos personales.

Seguridad de la información: La preservación de la confidencialidad, integridad y disponibilidad de la información que puede abarcar, además de otras propiedades como la autenticidad, la responsabilidad, la fiabilidad y el no repudio.

Servicios de nube privada: Modelos de servicio de tecnología de información proporcionados bajo demanda a las áreas universitarias, en infraestructura propiedad de la Universidad y que incluye cómputo, almacenamiento, plataforma, seguridad y respaldos.

Servicios de nube pública: Modelo de servicio de tecnología de información adquirida bajo demanda a terceros, operada en infraestructura ajena a la Universidad.

Sistema de Gestión de Seguridad de Datos Personales: Conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y la seguridad de los datos personales.

Sistemas para el tratamiento: Conjunto de elementos mutuamente relacionados o que interactúan para realizar la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales, en medios físicos o electrónicos.

Software libre: Es un software cuyo código fuente puede ser estudiado, modificado, y utilizado libremente con cualquier finalidad y redistribuido con cambios o mejoras sobre él.

Soporte: Medio, ya sea electrónico o físico, en el que se registra y guarda información, como sería: el papel, así como los audiovisuales, fotográficos, digitales, electrónicos, sonoros y visuales, entre otros, y los que produzca el avance de la tecnología.

Soportes electrónicos: Son los medios de almacenamiento accesible sólo a través del uso de algún dispositivo electrónico conocido o por conocer, que procese su contenido para examinar, modificar o almacenar los datos; tales como cintas magnéticas de audio, video y datos, fichas de microfilm, discos ópticos (CD, DVD y Blu-ray), discos magneto-ópticos, discos magnéticos (flexibles y duros) y demás medios para almacenamiento masivo no volátil.

Soportes físicos: Son los medios de almacenamiento accesibles de forma directa y sin intervención de algún dispositivo para examinar, modificar o almacenar los datos; tales como documentos, oficios, formularios impresos, escritos autógrafos, documentos de máquina de escribir, fotografías, placas radiológicas, carpetas, expedientes, entre otros.

Supresión: La erradicación del registro de los datos personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el *responsable*.

Transferencia: Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del Titular, Responsable o Encargado.

Tratamiento: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

Vulneración de seguridad: En cualquier fase del tratamiento de datos, se considera la pérdida o destrucción no autorizada; el robo, extravío o copia no autorizada; el uso, acceso o tratamiento no autorizado, o el daño, la alteración o modificación no autorizada

Abreviaturas

IIE: Instituto de Investigaciones Estéticas de la UNAM

Inventario de sistemas de tratamiento de datos personales

1. Sistema de consulta de acervos fotográficos - Collective Access del IIE
2. Sistema de gestión de cuerpos colegiados - Palimpsesto
3. Sistema de almacenamiento en nube privada - Protego (Owncloud)
4. Sistema de gestión de la publicación electrónica de la Revista Anales - Open Journal System (OJS)
5. Archivos académicos de la Secretaría Académica del IIE
6. Archivos administrativos de la Secretaría Administrativa del IIE
7. Sistema de préstamos "Circula" del programa ALEPH 500 v.21.
8. Sistema de Registro de asistentes a eventos
9. Sistema de Uso de Imagen
10. Sistema Integral de Personal
11. Sistema de Datos sobre contingencia COVID-19

Sistema de consulta de acervos fotográficos - Collective Access del IIE	
Finalidad del tratamiento	Consulta de acervos fotográficos
Datos personales recabados	Nombre del usuario Correo electrónico
Uso de los datos	Creación de Identificador de usuario y Contraseña
Formato de almacenamiento	Base de datos del sistema.
Descripción general de la ubicación física y/o electrónica de los datos personales	Servidores del Instituto.

Sistema de gestión de cuerpos colegiados - Palimpsesto	
Finalidad del tratamiento	Disposición de documentos para atención de los Cuerpos Colegiados
Datos personales recabados	Nombre del usuario Correo electrónico
Uso de los datos	Creación de Identificador de usuario y Contraseña
Formato de almacenamiento	Base de datos del sistema.
Descripción general de la ubicación física y/o electrónica de los datos personales	Servidores del Instituto.

Sistema de almacenamiento en nube privada - Protego (Owncloud)	
Finalidad del tratamiento	Respaldo de archivos institucionales.
Datos personales recabados	Nombre del usuario Correo electrónico
Uso de los datos	Creación de Identificador de usuario y Contraseña
Formato de almacenamiento	Base de datos del sistema.
Descripción general de la ubicación física y/o electrónica de los datos personales	Servidores del Instituto.

Sistema de gestión de la publicación electrónica de la Revista Anales - Open Journal System (OJS)	
Finalidad del tratamiento	Disposición de documentos para la publicación periódica de artículos.
Datos personales recabados	Nombre del usuario Correo electrónico
Uso de los datos	Creación de Identificador de usuario y Contraseña
Formato de almacenamiento	Base de datos del sistema.
Descripción general de la ubicación física y/o electrónica de los datos personales	Servidores del Instituto.

Sistema de Archivos académicos de la Secretaría Académica del IIE	
Finalidad del tratamiento	Trámites académicos.
Datos personales recabados	Nombre Fecha de nacimiento Domicilio Calidad migratoria Situación académica Número de trabajador UNAM Correo electrónico CURP Títulos de grado académico Credenciales oficiales
Uso de los datos	Trámites académicos
Formato de almacenamiento	Físico, bases de datos y documentos digitales.
Descripción general de la ubicación física y/o electrónica de los datos personales	Físico: archivo de la Secretaría Académica. Digitales en el servidor del Instituto.

Cargo del servidor público responsable	Dirección. Secretaría Académica. Cuerpos colegiados Comisiones auxiliares
En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que justifican éstas	Contratos, promociones, definitividad, entre otros.
Ciclo de vida y riesgo inherente de los datos personales	Físicos: se mantiene una copia simple de la documentación entregada. Digitales: de manera permanente.

Sistema de Archivos administrativos de la Secretaría Administrativa del IIE	
Finalidad del tratamiento	Trámites administrativos del personal contratado por el IIE o de personal colaborador
Datos personales recabados	Nombre Fecha de nacimiento Domicilio Calidad migratoria Situación académica Número de trabajador UNAM Correo electrónico Clave Única de Registro de Población (CURP) Registro Federal de Contribuyentes (RFC) Títulos de grado académico
Uso de los datos	Trámites administrativos.
Formato de almacenamiento	Físico, bases de datos y documentos digitales.
Descripción general de la ubicación física y/o electrónica de los datos personales	Físico: archivo de la Secretaría Administrativa. Digitales en los discos duros y en el servidor del Instituto.
Cargo del servidor público responsable	Secretaría Administrativa Departamento de Personal Departamento de Bienes y Suministros Departamento de Presupuesto

En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que justifican éstas	Adquisiciones, contrataciones de personal, ejercicio del presupuesto y gasto del IIE

Sistema de préstamos "Circula" del programa ALEPH 500 v.21.	
Finalidad del tratamiento	Registro de usuarios de la Biblioteca.
Datos personales recabados	Nombre Tipo de usuario Número de trabajador Número de cuenta de alumno UNAM o externo Correo electrónico Domicilio
Uso de los datos	Para el control de préstamos.
Formato de almacenamiento	En base de datos y papeletas para usuarios externos.
Descripción general de la ubicación física y/o electrónica de los datos personales	En un servidor del Instituto.
Cargo del servidor público responsable	Coordinador de la Biblioteca
Servidores públicos que tienen acceso a los sistemas de tratamiento	El coordinador y los bibliotecarios.
Ciclo de vida y riesgo inherente de los datos personales	Las papeletas un año. La información digital es permanente.

Sistema de Registro de asistentes a eventos	
Finalidad del tratamiento	Registrar la información de los asistentes a los eventos del Instituto de Investigaciones Estéticas.
Datos personales recabados	Nombre Correo electrónico de los asistentes a los eventos del IIE.
Uso de los datos	Elaboración de constancias y envío de invitaciones a las actividades del IIE.
Formato de almacenamiento	Electrónico.
Descripción general de la ubicación física y/o electrónica de los datos personales	La información se encuentra en un servidor en el Departamento de Cómputo del IIE.
Fundamento legal	Principios fundamentales, visión y objetivo del IIE.
Cargo del servidor público responsable	Secretaria Técnica.
Servidores públicos que tienen acceso a los sistemas de tratamiento	Secretaria Técnica.
Ciclo de vida y riesgo inherente de los datos personales	Permanente, o cuando solicitan hacer cambio de correo para enviar información. Al tratarse de datos personales contenidos en un Sistema electrónico, los riesgos que por la propia naturaleza tendría dicho sistema son: el uso indebido de la información, la falla en los equipos electrónicos o en los sistemas; por ello, el Instituto cuenta con un área soporte encargada de ejecutar acciones para garantizar la seguridad de la información.

Sistema de Uso de imagen	
Finalidad del tratamiento	Autorización para el uso de su imagen en la difusión de las actividades académicas del IIE.
Datos personales recabados	Nombre Correo electrónico Número de trabajador
Uso de los datos	Difundir por los diferentes canales de comunicación del Instituto las grabaciones de las actividades académicas.
Formato de almacenamiento	En archivo electrónico y físicos.
Descripción general de la ubicación física y/o electrónica de los datos personales	En archivos de la Secretaría Técnica
Cargo del servidor público responsable	Secretaría Técnica Departamento de Informática
Servidores públicos que tienen acceso a los sistemas de tratamiento	Secretaría Técnica Departamento de Informática
Ciclo de vida y riesgo inherente de los datos personales	Permanente.
En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que justifican éstas	De acuerdo con las Disposiciones Generales para la Actividad Editorial y de Distribución de la UNAM, se debe informar al Consejo Editorial de la UNAM, en el momento en que éste lo solicite, acerca de los dictámenes que se emiten (art. 37). Los dictámenes se presentarán con nombre y adscripción del dictaminador.
Ciclo de vida y riesgo inherente de los datos personales	Permanente. Al tratarse de datos personales contenidos en un sistema electrónico, los riesgos que por la propia naturaleza tendría dicho sistema son: el uso indebido de la información, la falla en los equipos electrónicos o en los sistemas.

Sistema Integral de Personal	
Finalidad del tratamiento	Trámites del Personal Académico. Confianza y Funcionarios y personal de Base, trámite de Prestadores de Servicios.
Datos personales recabados	Datos personales tales como: acta de nacimiento, comprobante de domicilio, INE, CURP, RFC, CV, entre otros.
Uso de los datos	Dar de alta, prorroga, nuevo nombramiento, licencias, permisos, actualizaciones.
Formato de almacenamiento	Digital en el sistema y físico en expedientes.
Descripción general de la ubicación física y/o electrónica de los datos personales	En la Dirección General de Personal, Secretaría Administrativa y Departamento de Personal.
Cargo del servidor público responsable	Jefe de Personal.
Servidores públicos que tienen acceso a los sistemas de tratamiento	La Secretaría Administrativa y Departamento de Personal.
En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que justifican éstas	La Dirección General de Personal.
Ciclo de vida y riesgo inherente de los datos personales	Permanente. Al tratarse de datos personales contenidos en un Sistema electrónico, los riesgos que por la propia naturaleza tendría dicho sistema son: el uso indebido de la información, la falla en los equipos electrónicos o en los sistemas; por ello, el Instituto cuenta con un área soporte encargada de ejecutar acciones para garantizar la seguridad de la información.

Sistema de Datos sobre contingencia COVID-19	
Finalidad del tratamiento	Se recaba la información para integrar la base de datos del personal del IIE para fines de la Contingencia Sanitaria.
Datos personales recabados	RFC
Uso de los datos	Se requiere un conteo de las personas que se ratifica como sospechosa o caso confirmado, así como saber quién ya cuenta con esquema de vacunación y que tipo de vacuna se aplicó y únicamente se recaba la información del personal adscrito a esta Dependencia.
Formato de almacenamiento	Electrónico.
Descripción general de la ubicación física y/o electrónica de los datos personales	Esta información solo la recaba el Responsable Sanitario y se hace desde su equipo.
Cargo del servidor público responsable	Secretaria Técnica.
Servidores públicos que tienen acceso a los sistemas de tratamiento	Secretaria Técnica.
En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que justifican éstas	Secretaría Administrativa.
Ciclo de vida y riesgo inherente de los datos personales	Hasta que la autoridad competente o responsable lo determine.

Análisis de riesgos

La información de este apartado se clasifica como reservada por un periodo de 5 años, a partir del 24 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.

Análisis de brecha

La información de este apartado se clasifica como reservada por un periodo de 5 años, a partir del 24 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.

Plan de trabajo

La información de este apartado se clasifica como reservada por un periodo de 5 años, a partir del 24 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.

Medidas de seguridad para la protección de datos personales

Con la finalidad de mantener un monitoreo y revisión de las medidas de seguridad, se llevarán a cabo de manera permanente las acciones siguientes:

1. Se mantendrá actualizado el inventario de datos personales y de los sistemas de tratamiento de los mismos.
2. El Departamento de Informática mantendrá monitoreados los esquemas de seguridad implementados para la infraestructura de tecnología de la información, comunicaciones y sistemas que permitan garantizar conexiones seguras, tanto fuera como dentro del Instituto.
3. Para garantizar el cumplimiento de las políticas en materia de protección de datos personales establecidas en el presente documento, el mismo se publicará en el sitio web del IIE y se enviará por medios electrónicos al personal del Instituto.
4. Se llevarán a cabo diversas medidas de seguridad físicas para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento mediante las siguientes actividades:
    a. Prevenir el acceso no autorizado al perímetro del lugar en que se resguarden los datos personales en sus instalaciones físicas.
    b. Prevenir el daño o interferencia a las instalaciones físicas, recursos e información.
    c. Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico, que pueda salir de las instalaciones del Instituto.
    d. Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz que asegure su disponibilidad, funcionalidad e integridad.
5. Las acciones a monitorear son las siguientes:
    a. Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras.
    b. Las nuevas amenazas que podrían estar activadas dentro y fuera de la organización y que no han sido valoradas.
    c. La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes.
    d. Las vulnerabilidades identificadas para determinar aquellas expuestas a amenazas nuevas pasadas que vuelvan a surgir.
    e. El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto que resulten en un nivel inaceptable de riesgo.

Programa de Capacitación

Se mantendrá la constante capacitación de personal responsable o corresponsable del manejo y uso de datos personales, mediante los cursos ofrecidos por la Dirección General de Cómputo y de Tecnologías de información y Comunicación, y la Unidad de Transparencia de la UNAM.

Asimismo, se busca continuar con la concientización y sensibilización de las prácticas relativas a Transparencia y manejo de datos personales, en las tareas sustantivas del IIE.

Aprobación del Documento de Seguridad

		Nombre y firma de quienes revisaron el presente documento
Responsable del desarrollo	**Lic. Raquel López Zúñiga** Jefa de Vinculación Institucional Enlace de Transparencia Responsable de Seguridad de Datos Personales **Ing. Víctor Hugo Zamora Guerrero** Jefe del Departamento de Informática Responsable de Seguridad de Datos Personales	 
Revisó	**Lic. Raquel López Zúñiga** Jefa de Vinculación Institucional Enlace de Transparencia Responsable de Seguridad de Datos Personales	
Autorizó	**Dra. Angélica Velázquez Guadarrama** Directora del IIE	
Fecha de aprobación	15 de agosto de 2022	
Fecha de actualización	15 de agosto de 2022	