ÍNDICE

Introducción ---------- 4

1. Objetivo ---------- 5

2. Términos, definiciones y abreviaturas---------- 5

2.1. Términos y condiciones ---------- 5

2.2. Abreviaturas ---------- 9

3. Alcance ---------- 9

3.1. Funciones y Responsabilidades ---------- 9

3.2. Sistema de Gestión de Seguridad de Datos Personales ---------- 10

3.2.1. Política del Sistema de Seguridad de Datos Personales -- 10

3.2.2. Objetivo del SGSDP ---------- 11

4. Anexos ---------- 12

Anexo I. *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* ---------- 12

Anexo II. Inventario de sistemas de tratamiento de datos personales – 12

II.I. Estructura y descripción de los sistemas de tratamiento de datos personales ---------- 17

Anexo III. Análisis de Riesgos ---------- 18

Anexo IV. Análisis de Brecha ---------- 23

Anexo V. Plan de Trabajo ---------- 26

Anexo VI. Capacitación ---------- 28

Anexo VI. Formato Universitario de “Solicitud de ejercicio de derechos ARCO” ---------- 29

Anexo VII. Carta de confidencialidad ---------- 31

Introducción

El presente documento de seguridad contiene las medidas de seguridad administrativas, físicas y técnicas aplicables a los sistemas de tratamiento de datos personales del Centro de Investigaciones Interdisciplinarias en Ciencias y Humanidades (CEIICH), con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información personal que éstos contienen.

Su propósito es identificar los sistemas de tratamiento de datos personales que posee esta área universitaria, 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, documento contenido en el Anexo 1.

El cimiento del formato de documento de seguridad es la aplicación de un enfoque basado en los riesgos de los activos universitarios, específicamente los datos personales y los soportes que los resguardan. Además, el formato considera el tamaño y estructura de la institución, objetivos, clasificación de la información, requerimientos de seguridad y procesos que se precisan en razón de los activos que posee esta Máxima Casa de Estudios, los cuales se encuentran 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”.

1. Objetivo.

Describir las medidas de seguridad del Sistema de Gestión de la Seguridad de Datos Personales del Centro de Investigaciones Interdisciplinarias en Ciencias y Humanidades (CEIICH) de la Universidad Nacional Autónoma de México, desde su obtención, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales, así como proteger todos los datos personales y datos personales sensibles que se recaben y de accesos no autorizados ni de tratamientos distintos a los fines para los que fueron recabados mediante cualquiera de los siguientes tipos de soportes:

a) En soportes físicos.
b) En soportes electrónicos.
c) En redes de datos.

2. Términos, condiciones y abreviaturas.

2.1 Términos y definiciones.

2.1.1. 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 los documentos en papel.

2.1.2. Aviso de privacidad: Documento a disposición del titular de 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.

2.1.3 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.

2.1.4. 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.

2.1.5. 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.

2.1.6. 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.

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

2.1.8. 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.

2.1.9. 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.

2.1.10. Encargado: La persona física o jurídica distinta a las áreas, entidades o dependencias universitarias, que realiza 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.

2.1.11. Evaluación de impacto en la protección de datos personales (EIDP): Documento mediante el cual las Áreas Universitarias que pretendan poner en operación o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales, valoran los impactos reales sobre determinado tratamiento de datos personales, a efecto de identificar y mitigar posibles riesgos relacionados con los principios, deberes y derechos de los titulares, así como los deberes de los Responsables y Encargados, previstos en la normativa aplicable.

2.1. 12. 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 intencionadamente.

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

2.1.14. 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.

2.1.15. 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.

2.1.16. 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, y
d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

2.1.17. 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.

2.1.18. Responsable: Las Áreas Universitarias que manejan, resguardan y/o deciden sobre el tratamiento de datos personales.

2.1.19. Seguridad de la información: La preservación de la

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

2.1.20. Servicios de nube privada: Modelo 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.

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

2.1.22. 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.

2.1.23. 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.

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

2.1.25. Soportes electrónicos: Son los medios de almacenamiento accesibles 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, vídeo y datos, fichas de microfilm, discos ópticos (CDs, DVDs y Blue-rays), discos magneto ópticos, discos magnéticos (flexibles y duros) y demás medios para almacenamiento masivo no volátil.

2.1.26. 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; XXXVII. 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.

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

2.1.28. 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.

2.1.29. 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.

2.2. Abreviaturas.

2.2.1. CEIICH: Centro de Investigaciones Interdisciplinarias en Ciencias y Humanidades de la UNAM.
2.2.2. SGSDP: Sistema de Gestión de Seguridad de Datos Personales.
2.2.3. TIC: Tecnologías de la Información y la Comunicación.

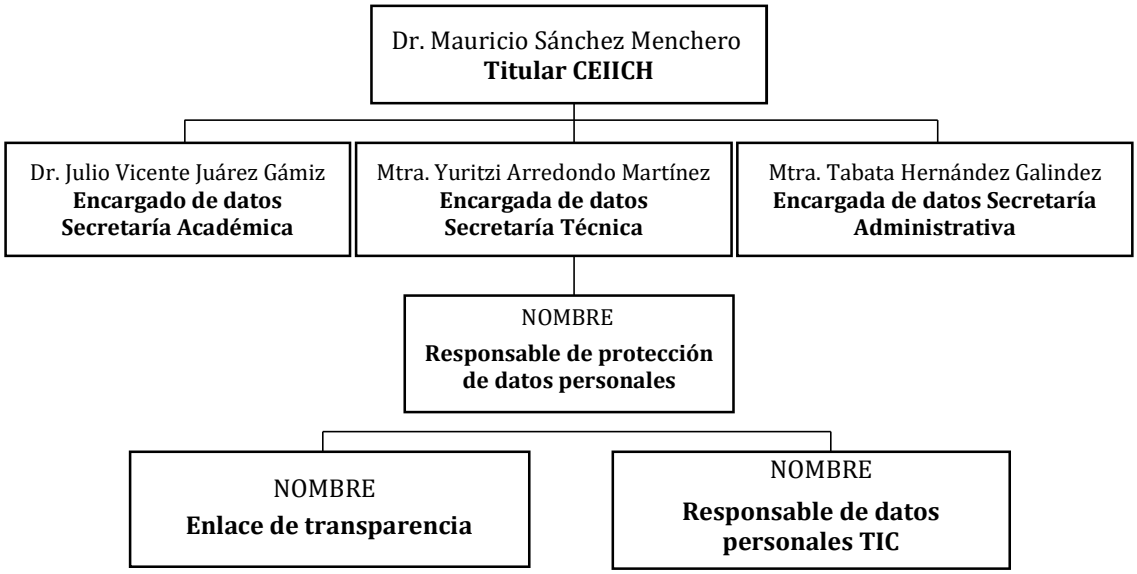
3. Alcance.

Aplica a todas las áreas administrativas, académicas y de servicio que tienen en su poder datos personales y datos personales sensibles.

3.1. Funciones y Responsabilidades.

En el SGSDP del CEIICH, la responsabilidad, autoridad e interrelaciones del personal que ata datos personales, se mantiene con la siguiente cadena de rendición de cuentas:

a) Organigrama del SGSDP del CEIICH:



Las funciones y responsabilidades generales de los integrantes del SGSDP son:

Titular: Supervisar que el Sistema de Gestión de Seguridad de Datos Personales se cumpla de acuerdo a este Documento de Seguridad.

Responsables: Verificar que el Sistema de Gestión de Seguridad de Datos Personales se cumpla en sus áreas específicas (administrativas, académicas y/o técnicas) de acuerdo a este Documento de Seguridad.

Encargadas/os: Mantener el Sistema de Gestión de Seguridad de Datos Personales en sus áreas específicas (administrativas, académicas y/o técnicas) de acuerdo a este Documento de Seguridad.

Usuarias/os: Utilizar el sistema de Gestión de Seguridad de Datos Personales en sus áreas específicas (administrativas, académicas y/o técnicas) de acuerdo a este Documento de Seguridad.

Rol	Figura
Titular	Titular del CEIICH.
Responsable	Responsable designado por el titular del CEIICH.
Encargada/o	De acuerdo al uso de los datos personales definidos en el Anexo 2: Titular de la Secretaría Académica. Titular de la Secretaría Técnica. Titular de la Secretaría Administrativa.
Usuarias/os	Definido en el Anexo 2 de acuerdo al uso de datos personales.

3.2. Sistema de Gestión de Seguridad de Datos Personales.

El CEIICH establece y mantiene un Sistema de Gestión de Seguridad de Datos Personales y documenta sus políticas, sistemas, programas, procedimientos e instrucciones necesarias para asegurar la integridad, confidencialidad y disponibilidad de los datos personales, según el *Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México*, publicado el 26 de agosto de 2016 y a las *Normas Complementarias sobre Medidas de Seguridad Técnicas, Administrativas y Físicas para la Protección de Datos Personales en Posesión de la Universidad*, publicadas el 10 de enero de 2020.

3.2.1. Política del Sistema de Seguridad de Datos Personales.

El CEIICH se compromete a cumplir con las medidas de seguridad para la protección de datos personales desde su obtención, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales, así como proteger todos los datos personales y datos personales sensibles que se recaben y de accesos no autorizados ni de tratamientos distintos a los fines para los que fueron recabados mediante soportes físicos, electrónicos o en redes de datos.

3.2.2. Objetivo del SGSDP.

Asegurar la integridad, confidencialidad y disponibilidad de la información que contengan datos personales.

4. Anexos.

ANEXO I. Lineamientos para la protección de datos personales en posesión de la Universidad Nacional Autónoma de México.

El documento puede consultarse en la Gaceta UNAM del 25 de febrero de 2019, No. 5031, pp. 24 a 32; y en la dirección URL: https://www.gaceta.unam.mx/index/wp-content/uploads/2019/02/190225-convocatorias.pdf

ANEXO II. Inventario de "Sistemas de Tratamiento de Datos Personales".

Centro de Investigaciones Interdisciplinarias en Ciencias y Humanidades- Departamento de Cómputo.	
Identificador único*	PlataformaSIICH
(Nombre del sistema A1)	PlataformaSIICH_01
Datos personales (sensibles o no) contenidos en el sistema*:	**Información del personal académico del CEIICH y becarios posdoctorales.** **Datos de identificación**: Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico personal e institucional, CURP, RFC, fecha de nacimiento, nacionalidad, edad, fotografía, grado de estudios, datos laborales. Convenios institucionales y jurídicos del CEIICH.
Responsable*:	
Nombre*:	**Ing. Fidel Adrián Pineda Bedolla**
Cargo*:	**Jefe del Departamento de Cómputo.**
Funciones*:	• Apoyar a las áreas académico-administrativas del CEIICH para el almacenamiento, procesamiento y consulta de información a través del desarrollo de este sistema de cómputo.
Obligaciones*:	• Garantizar el correcto almacenamiento de la información en la base de datos de los sistemas. • Garantizar el correcto procesamiento y consulta de la información. • Administrar las cuentas de acceso al sistema para el procesamiento y consulta de información. • Establecer niveles de permisos a usuarios, relacionados con el procesamiento y consulta de datos.

	• Supervisar la realización de respaldos periódicos de la información, para garantizar su disponibilidad ante posibles fallos o eventualidades que se lleguen a presentar.
	Encargados:
(Nombre del Encargado 1*)	**Mtro. Jorge Pantaleón Martínez.**
Cargo*:	**Técnico Académico del Departamento de Cómputo.**
Funciones*:	• Mantener actualizado el sistema operativo. • Mantener actualizada a su última versión la base de datos. • Respaldo de las bases de datos. • Actualización de servidores y bases de datos.
Obligaciones*:	• Dar de alta a los usuarios. • Subir información a la base de datos. • Verificar que la información que se ingresa al sistema no presente errores o discrepancias. • Realizar respaldos periódicos de la información, para garantizar su disponibilidad ante posibles fallos o eventualidades que se lleguen a presentar.
	Usuarios:
(Nombre del Usuario 1*)	**Ing. Andrea Torres Reyes**
Cargo*:	**Jefa del Departamento de Planeación y Seguimiento Académico.**
Funciones*:	• Consulta y revisión de datos contenidos en el sistema para llevar a cabo procesos de planeación académica. • Solicitar creación de nuevos perfiles cuando sea requerido.
Obligaciones*:	• Informar al encargado y/o responsable cuando un dato contenido en el sistema sea modificado. • Manejar responsablemente los datos, compartiéndolos únicamente con las personas que tienen acceso al sistema.
(Nombre del Usuario 2*)	**Juana Patricia Sámano Luna.**
Cargo*:	**Asistente ejecutiva de la Secretaría Académica.**
Funciones*:	• Consulta y revisión de datos contenidos en el sistema. • Solicitar la creación de nuevos perfiles cuando sea requerido.
Obligaciones*:	• Informar al encargado y/o responsable cuando un dato contenido en el sistema sea modificado. • Manejar responsablemente los datos, compartiéndolos únicamente con las personas que tienen acceso al sistema.

Centro de Investigaciones Interdisciplinarias en Ciencias y Humanidades- Departamento de Cómputo.	
Identificador único*	Sistema de Gestión de Espacios del CEIICH.
(Nombre del sistema A2) *	SGE
Datos personales (sensibles o no) contenidos en el sistema*:	Datos de identificación: Nombre, correo electrónico personal e institucional. Datos de eventos académicos: Nombre, horario de usos de los espacios del CEIICH.
Responsable*:	
Nombre*:	**Ing. Fidel Adrián Pineda Bedolla**
Cargo*:	**Jefe del Departamento de Cómputo.**
Funciones*:	• Apoyar a las áreas académico-administrativas del CEIICH para el almacenamiento, procesamiento y consulta de información a través del desarrollo de este sistema de cómputo.
Obligaciones*:	• Garantizar el correcto almacenamiento de la información en la base de datos de los sistemas. • Garantizar el correcto procesamiento y consulta de la información. • Administrar las cuentas de acceso al sistema para el procesamiento y consulta de información. • Establecer niveles de permisos a usuarios, relacionados con el procesamiento y consulta de datos. • Realizar respaldos periódicos de la información, para garantizar su disponibilidad ante posibles fallos o eventualidades que se lleguen a presentar.
	Encargados:
(Nombre del Encargado 1*)	**Mtro. Jorge Pantaleón Martínez.**
Cargo*:	**Técnico Académico del Departamento de Cómputo.**
Funciones*:	• Mantener actualizado el sistema. • Mantener actualizada a su última versión la base de datos. • Revisión de servidores, así como respaldos de bases y sistemas.
Obligaciones*:	• Dar de alta a los usuarios. • Ingresar información a la base de datos. • Continuar con el desarrollo del sistema en base a las necesidades del CEIICH. • Verificar vulnerabilidades y actualización de los servidores.

(Nombre del Encargado 2*)	**Paulina Gallegos Vera.**
Cargo*:	**Programadora del Departamento de Cómputo.**
Funciones*:	• Programación del sistema virtual de espacios. • Corrección de errores. • Actualización de datos y características del sistema
Obligaciones*:	• Dar de alta a usuarios. • Revisar consistencia del sistema. • Determinar si se necesitan cambios del mismo.

Centro de Investigaciones Interdisciplinarias en Ciencias y Humanidades- Departamento de Cómputo.	
Identificador único*	Página WEB del CEIICH
(Nombre del sistema A3) *	Página WEB del CEIICH_VPHP
Datos personales (sensibles o no) contenidos en el sistema*:	Datos de identificación: Nombre, teléfono de oficina, correo electrónico institucional. Datos personales sensibles: ninguno.
Responsable*:	
Nombre*:	**Ing. Fidel Adrián Pineda Bedolla**
Cargo*:	**Jefe del Departamento de Cómputo.**
Funciones*:	• Apoyar a las áreas académico-administrativas del CEIICH para el almacenamiento, procesamiento y consulta de información a través del desarrollo de este sistema de cómputo.
Obligaciones*:	• Garantizar el correcto almacenamiento de la información en la base de datos de los sistemas. • Garantizar el correcto procesamiento y consulta de la información. • Administrar las cuentas de acceso al sistema para el procesamiento y consulta de información. • Establecer niveles de permisos a usuarios, relacionados con el procesamiento y consulta de datos • Realizar respaldos periódicos de la información, para garantizar su disponibilidad ante posibles fallos o eventualidades que se lleguen a presentar.
	Encargados:
(Nombre del Encargado 1*)	**Mtro. Jorge Pantaleón Martínez.**
Cargo*:	**Técnico Académico del Departamento de Cómputo.**
Funciones*:	• Mantener actualizadas las versiones de trabajo de los servicios WEB de la página.

	• Mantener actualizada a su última versión la base de datos. • Respaldos de bases y sistemas.
Obligaciones*:	• Dar de alta a los usuarios. • Ingresar información a la base de datos. • Continuar con el desarrollo del sistema en base a las necesidades del CEIICH. • Verificar vulnerabilidades y actualización de los servidores.
(Nombre del Encargado 2*)	**Paulina Gallegos Vera.**
Cargo*:	**Programadora del Departamento de Cómputo.**
Funciones*:	• Actualización de contenido digital de la página WEB
Obligaciones*:	• Verificar la consistencia de la información que se encuentra en la página Web.

II.I. Estructura y descripción de los sistemas de tratamiento de datos personales.

Centro de Investigaciones Interdisciplinarias en Ciencias y Humanidades-Departamento de Cómputo	
Identificador único¨*	PlataformaSIICH
(Nombre del sistema A1*)	PlataformaSIICH_01
Tipo de soporte: *	Soporte electrónico
Descripción: *	Base de datos relacional en el servidor Filemaker Server
Características del lugar donde se resguardan los soportes: *	Alojamiento en Servidor del departamento de Cómputo-CEIICH

Centro de Estudios Interdisciplinarios en Ciencias y Humanidades-Departamento de Cómputo	
Identificador único¨*	Sistema de Gestión de Espacios del CEIICH
(Nombre del sistema A2*)	SGE
Tipo de soporte: *	Soporte electrónico
Descripción: *	Base de datos SQLITE y sistema en RAILS
Características del lugar donde se resguardan los soportes: *	Alojamiento en Servidor del departamento de Cómputo-CEIICH

Centro de Investigaciones Interdisciplinarias en Ciencias y Humanidades-Departamento de Cómputo	
Identificador único¨*	Página WEB del CEIICH
(Nombre del sistema A3*)	Página WEB del CEIICH_VPHP
Tipo de soporte:*	Soporte electrónico
Descripción: *	Base de datos relacional MYSQL, PHP , APACHE
Características del lugar donde se resguardan los soportes: *	Alojamiento en servidor de UNAM-DGTICx.

ANEXO III. Análisis de riesgos.

[redacted]

Eliminado: Análisis de Riesgos contenidos en el documento de seguridad, toda vez que dar a conocer dicha información hace latente el nivel de vulnerabilidad de las medidas de seguridad de los datos personales en posesión del Centro de Investigaciones Interdisciplinarias en Ciencias y Humanidades de la Universidad Nacional Autónoma de México, lo que ocasionaría una posible comisión de delitos previstos por el Código Penal Federal, como son: Acceso no autorizado a los sistemas, robo de información, suplantación de identidades entre otros. **Fundamento legal:** Artículo 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública; artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en correlación con el artículo 41 del Reglamento de Transparencia y Acceso a la información Pública de la Universidad Nacional Autónoma de México y los numerales Quincuagésimo Sexto y Sexagésimo Primero de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como para la elaboración de versiones públicas. **Periodo de Reserva:** Cinco años a partir del 24 de agosto de 2022.

[redacted]

[redacted]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]

[redacted]

[redacted]

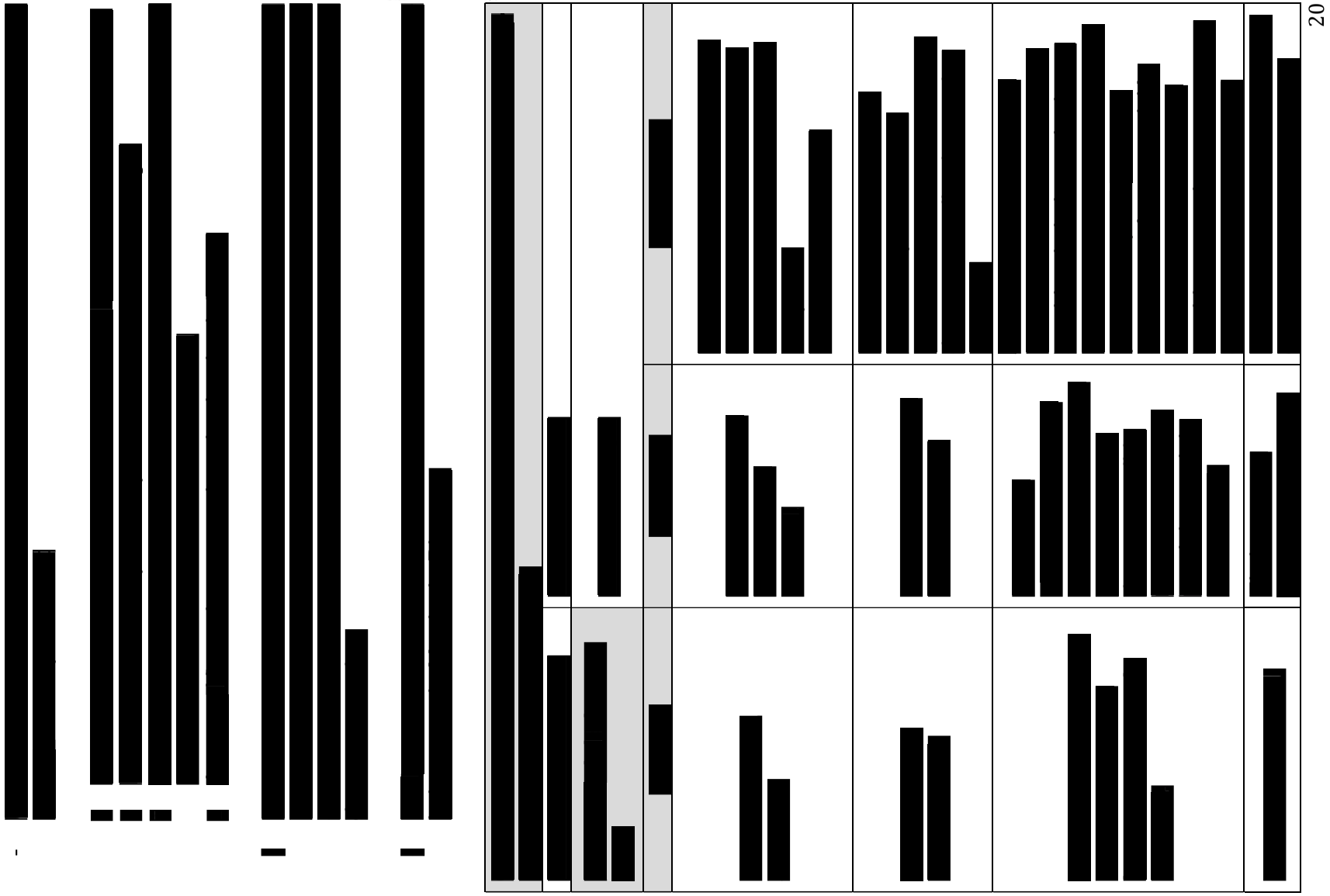
[redacted]			
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]

[redacted]

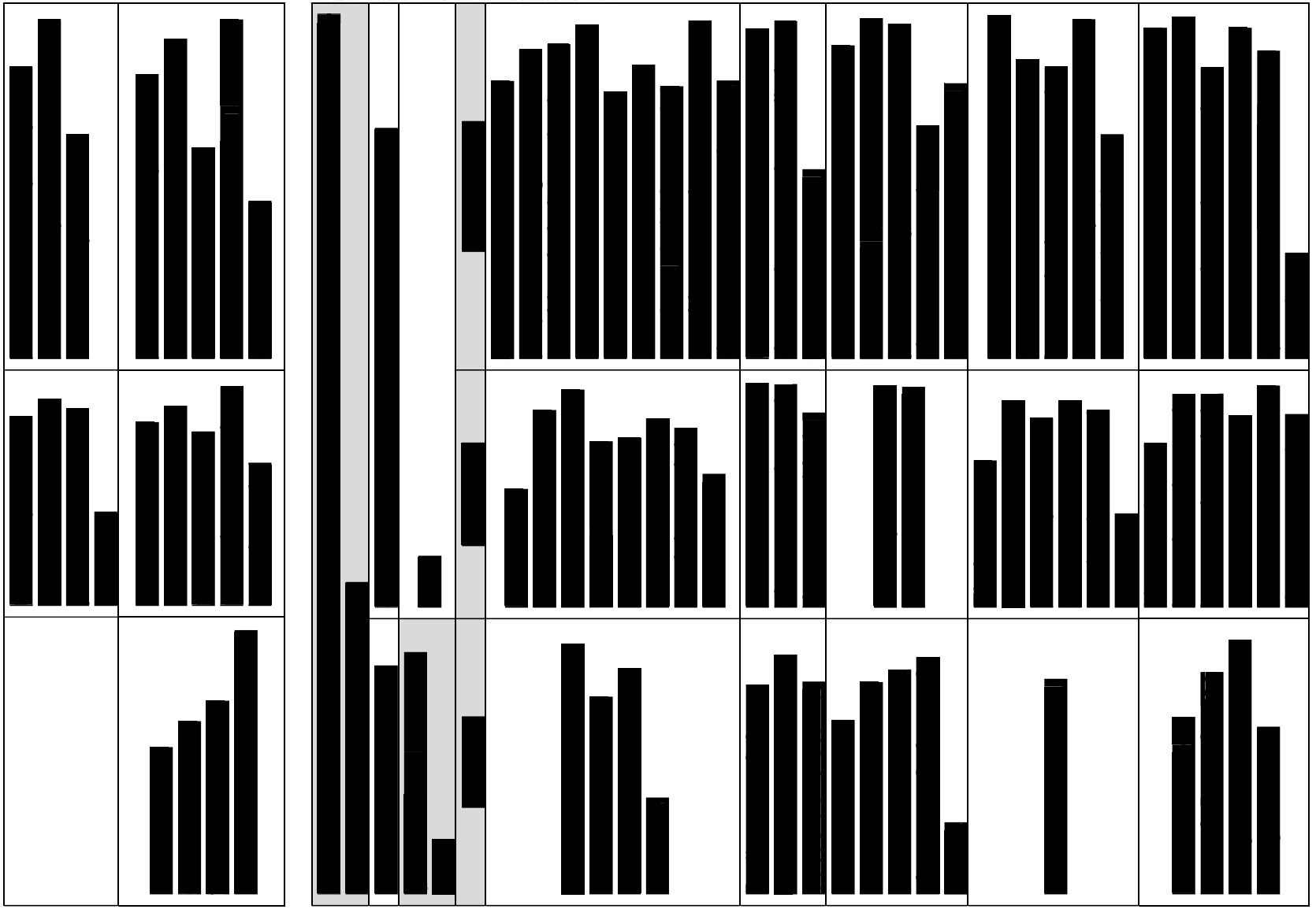
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

Eliminado: Análisis de Riesgo: contenidos en el documento de seguridad, toda vez que dar a conocer dicha información hace latente el nivel de vulnerabilidad de las medidas de seguridad de los datos personales en posesión del Centro de Investigaciones Interdisciplinarias en Ciencias y Humanidades de la Universidad Nacional Autónoma de México, lo que ocasionaría una posible comisión de delitos previstos por el Código Penal Federal, como son: Acceso no autorizado a los sistemas, robo de información, suplantación de identidades entre otros. **Fundamento legal:** Artículo 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública; artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en correlación con el artículo 41 del Reglamento de Transparencia y Acceso a la información Pública de la Universidad Nacional Autónoma de México y los numerales Quincuagésimo Sexto y Sexagésimo Primero de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como para la elaboración de versiones públicas. **Periodo de Reserva:** Cinco años a partir del 24 de agosto de 2022.

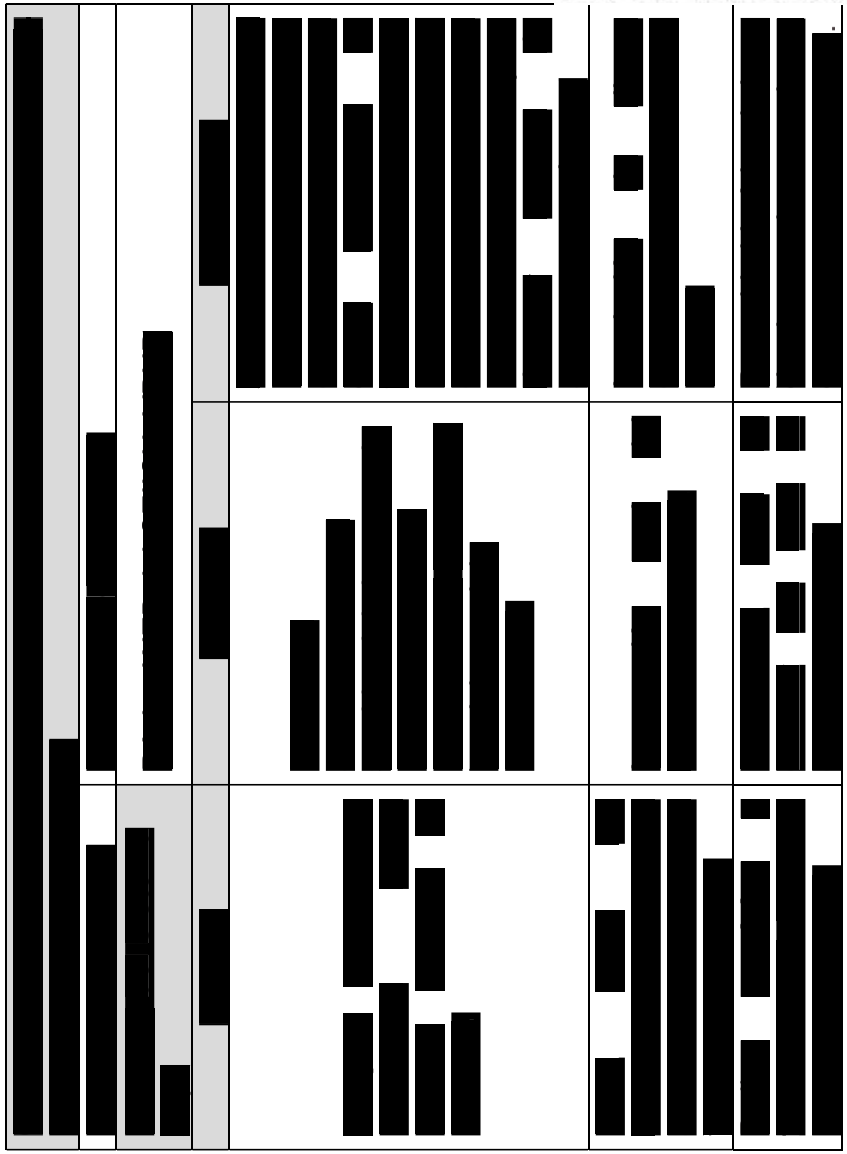
Eliminado: **Análisis de Riesgos** contenidos en el documento de seguridad, toda vez que dar a conocer dicha información hace latente el nivel de vulnerabilidad de las medidas de seguridad de los datos personales en posesión del Centro de Investigaciones Interdisciplinarias en Ciencias y Humanidades de la Universidad Nacional Autónoma de México, lo que ocasionaría una posible comisión de delitos previstos por el Código Penal Federal, como son: Acceso no autorizado a los sistemas , robo de información, suplantación de identidades entre otros. **Fundamento legal**: Artículo 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública; artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en correlación con el artículo 41 del Reglamento de Transparencia y Acceso a la información Pública de la Universidad Nacional Autónoma de México y los numerales Quincuagésimo Sexto y Sexagésimo Primero de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como para la elaboración de versiones públicas. **Periodo de Reserva**: Cinco años a partir del 24 de agosto de 2022.



Eliminado: **Análisis de Riesgos** contenidos en el documento de seguridad, toda vez que dar a conocer dicha información hace latente el nivel de vulnerabilidad de las medidas de seguridad de los datos personales en posesión del Centro de Investigaciones Interdisciplinarias en Ciencias y Humanidades de la Universidad Nacional Autónoma de México, lo que ocasionaría una posible comisión de delitos previstos por el Código Penal Federal, como son: Acceso no autorizado a los sistemas , robo de información, suplantación de identidades entre otros. **Fundamento legal**: Artículo 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública; artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en correlación con el artículo 41 del Reglamento de Transparencia y Acceso a la información Pública de la Universidad Nacional Autónoma de México y los numerales Quincuagésimo Sexto y Sexagésimo Primero de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como para la elaboración de versiones públicas. **Periodo de Reserva**: Cinco años a partir del 24 de agosto de 2022.



Eliminado: **Análisis de Riesgos** contenidos en el documento de seguridad, toda vez que dar a conocer dicha información hace latente el nivel de vulnerabilidad de las medidas de seguridad de los datos personales en posesión del Centro de Investigaciones Interdisciplinarias en Ciencias y Humanidades de la Universidad Nacional Autónoma de México, lo que ocasionaría una posible comisión de delitos previstos por el Código Penal Federal, como son: Acceso no autorizado a los sistemas , robo de información, suplantación de identidades entre otros. **Fundamento legal**: Artículo 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública; artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en correlación con el artículo 41 del Reglamento de Transparencia y Acceso a la información Pública de la Universidad Nacional Autónoma de México y los numerales Quincuagésimo Sexto y Sexagésimo Primero de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como para la elaboración de versiones públicas. **Periodo de Reserva**: Cinco años a partir del 24 de agosto de 2022.



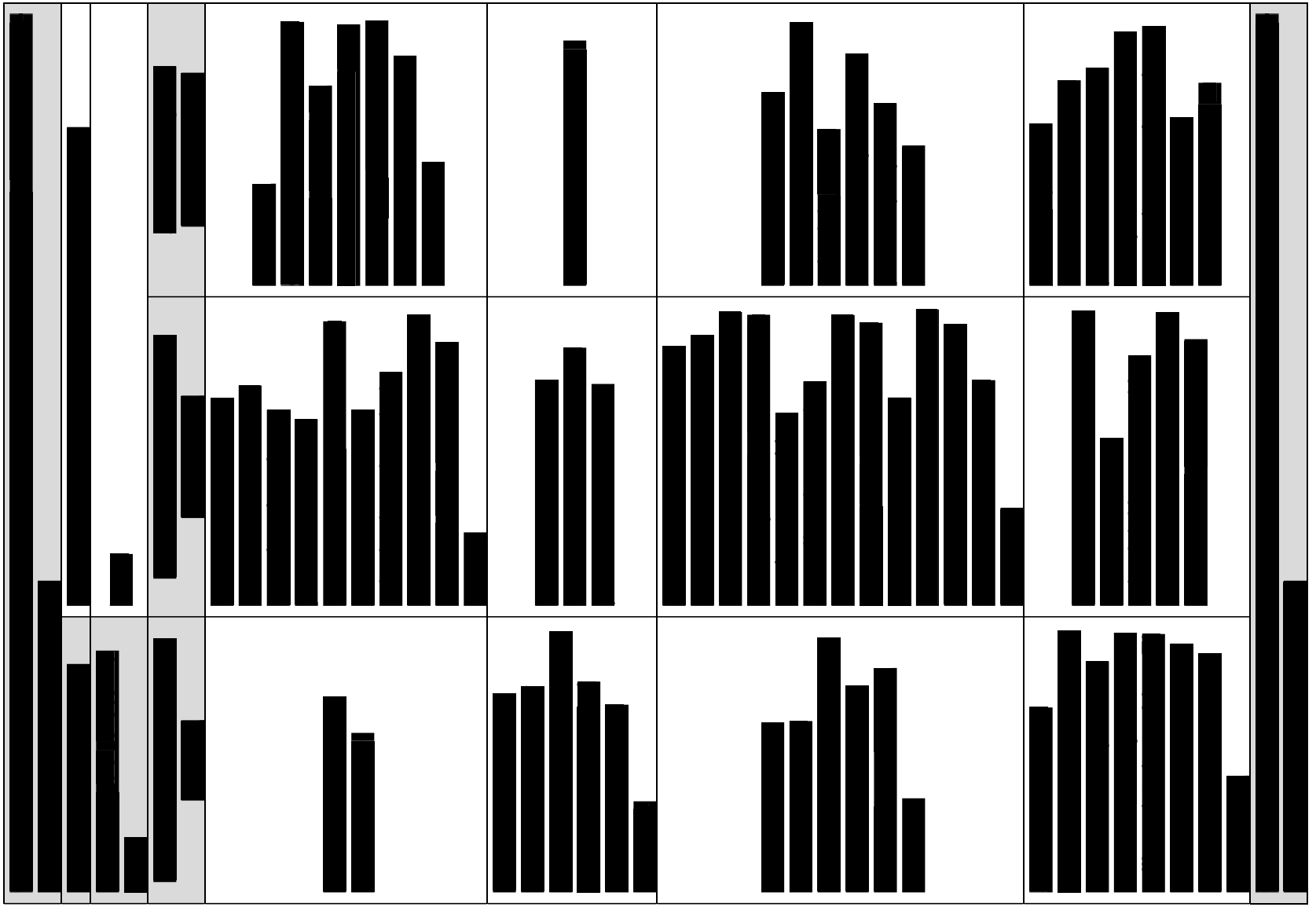
ANEXO IV. Análisis de brecha.

[redacted]

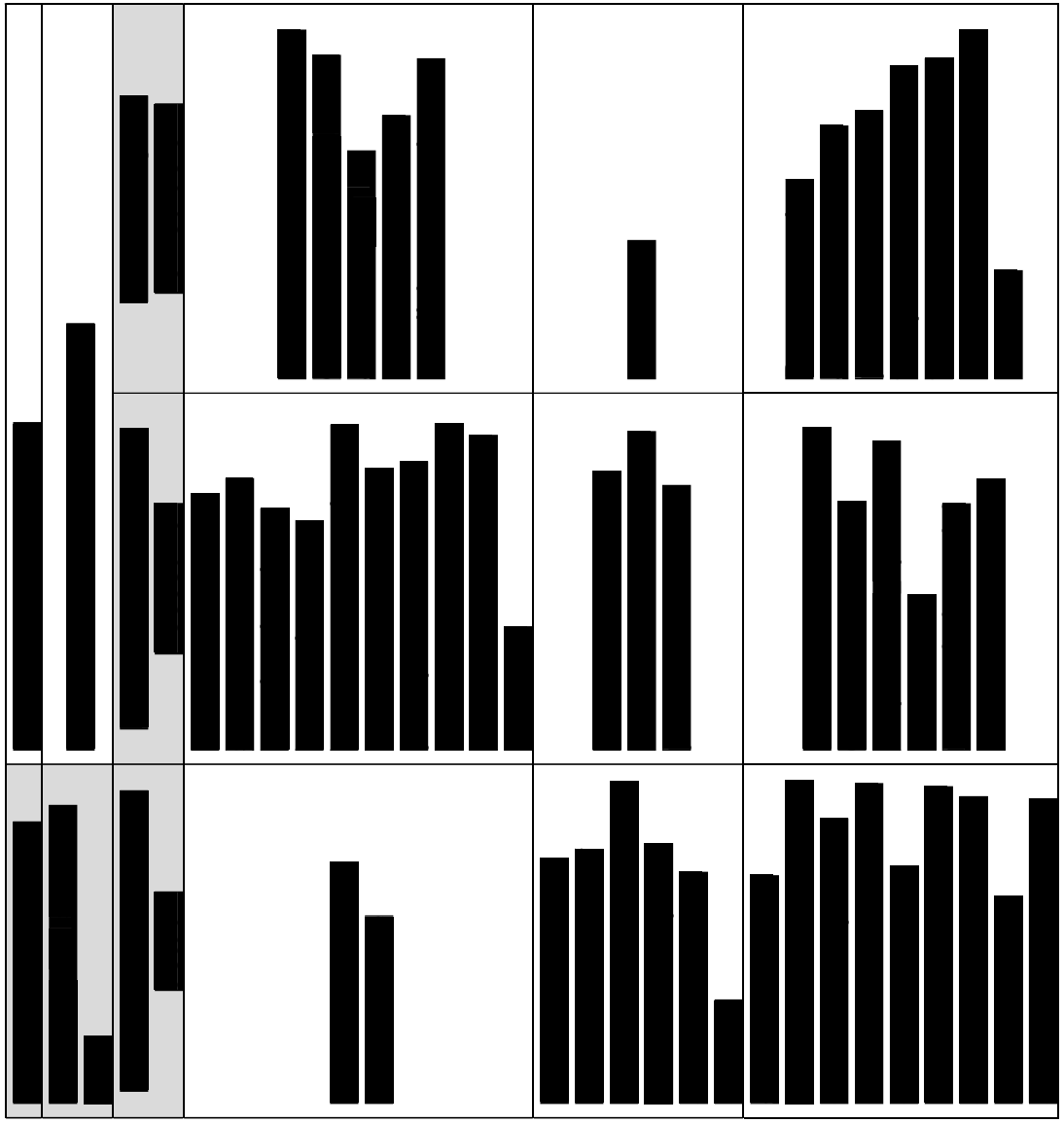
[redacted]

[redacted]

Eliminado: **Análisis de brecha** contenidos en el documento de seguridad, toda vez que dar a conocer dicha información hace latente el nivel de vulnerabilidad de las medidas de seguridad de los datos personales en posesión del Centro de Investigaciones Interdisciplinarias en Ciencias y Humanidades de la Universidad Nacional Autónoma de México, lo que ocasionaría una posible comisión de delitos previstos por el Código Penal Federal, como son: Acceso no autorizado a los sistemas , robo de información, suplantación de identidades entre otros. **Fundamento legal**: Artículo 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública; artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en correlación con el artículo 41 del Reglamento de Transparencia y Acceso a la información Pública de la Universidad Nacional Autónoma de México y los numerales Quincuagésimo Sexto y Sexagésimo Primero de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como para la elaboración de versiones públicas. **Periodo de Reserva**: Cinco años a partir del 24 de agosto de 2022.



Eliminado: **Análisis de brecha** contenidos en el documento de seguridad, toda vez que dar a conocer dicha información hace latente el nivel de vulnerabilidad de las medidas de seguridad de los datos personales en posesión del Centro de Investigaciones Interdisciplinarias en Ciencias y Humanidades de la Universidad Nacional Autónoma de México, lo que ocasionaría una posible comisión de delitos previstos por el Código Penal Federal, como son: Acceso no autorizado a los sistemas , robo de información, suplantación de identidades entre otros. **Fundamento legal**: Artículo 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública; artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en correlación con el artículo 41 del Reglamento de Transparencia y Acceso a la información Pública de la Universidad Nacional Autónoma de México y los numerales Quincuagésimo Sexto y Sexagésimo Primero de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como para la elaboración de versiones públicas. **Periodo de Reserva**: Cinco años a partir del 24 de agosto de 2022.



ANEXO V. Plan de trabajo.

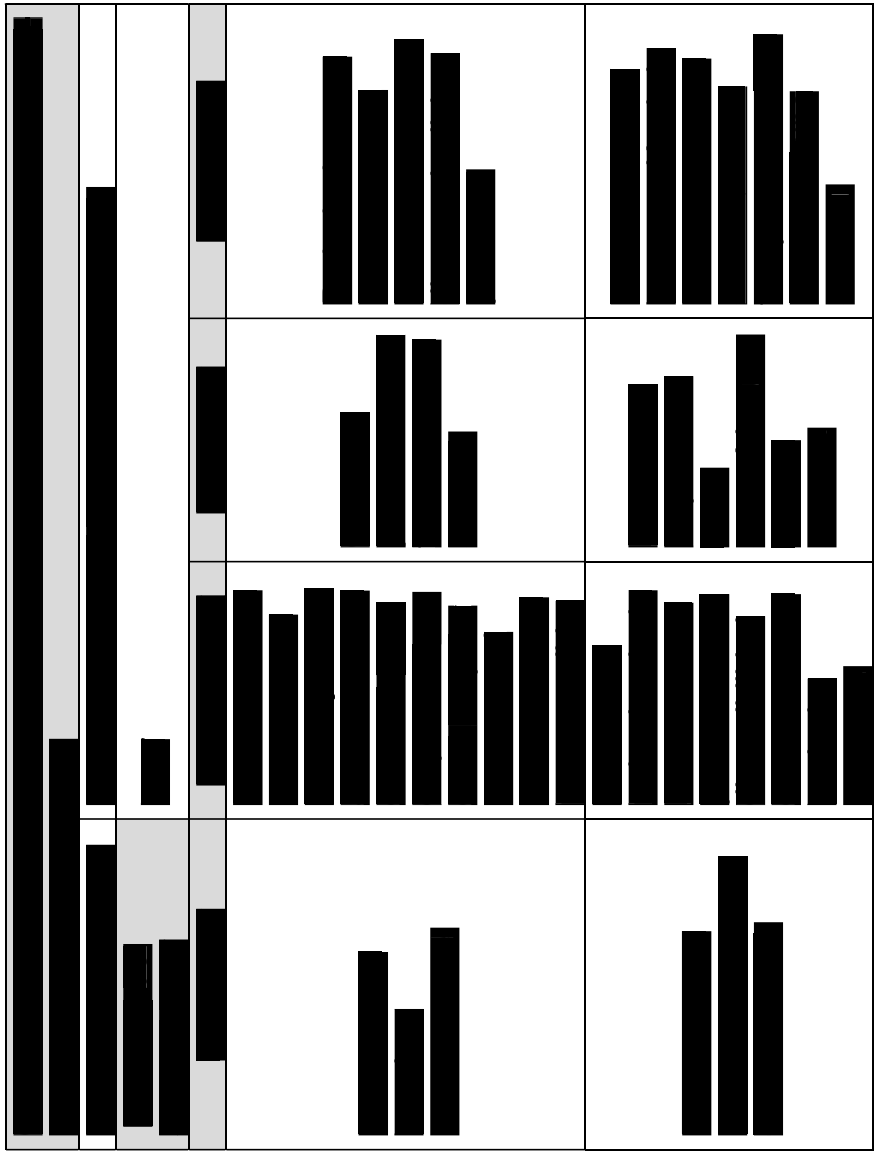
[redacted]

[redacted]

[redacted]			
[redacted]	[redacted]		
[redacted]	[redacted]		
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

Eliminado: Plan de trabajo contenidos en el documento de seguridad, toda vez que dar a conocer dicha información hace latente el nivel de vulnerabilidad de las medidas de seguridad de los datos personales en posesión del Centro de Investigaciones Interdisciplinarias en Ciencias y Humanidades de la Universidad Nacional Autónoma de México, lo que ocasionaría una posible comisión de delitos previstos por el Código Penal Federal, como son: Acceso no autorizado a los sistemas , robo de información, suplantación de identidades entre otros. **Fundamento legal**: Artículo 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública; artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en correlación con el artículo 41 del Reglamento de Transparencia y Acceso a la información Pública de la Universidad Nacional Autónoma de México y los numerales Quincuagésimo Sexto y Sexagésimo Primero de los Lineamientos Generales en materia de Clasificación y Desclasificación de la información, así como para la elaboración de versiones públicas. **Periodo de Reserva**: Cinco años a partir del 24 de agosto de 2022.

Eliminado: **Plan de trabajo** contenidos en el documento de seguridad, toda vez que dar a conocer dicha información hace latente el nivel de vulnerabilidad de las medidas de seguridad de los datos personales en posesión del Centro de Investigaciones Interdisciplinarias en Ciencias y Humanidades de la Universidad Nacional Autónoma de México, lo que ocasionaría una posible comisión de delitos previstos por el Código Penal Federal, como son: Acceso no autorizado a los sistemas , robo de información, suplantación de identidades entre otros. **Fundamento legal**: Artículo 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública; artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en correlación con el artículo 41 del Reglamento de Transparencia y Acceso a la información Pública de la Universidad Nacional Autónoma de México y los numerales Quincuagésimo Sexto y Sexagésimo Primero de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como para la elaboración de versiones públicas. **Periodo de Reserva**: Cinco años a partir del 24 de agosto de 2022.



[redacted]

Eliminado: Plan de trabajo contenidos en el documento de seguridad, toda vez que dar a conocer dicha información hace latente el nivel de vulnerabilidad de las medidas de seguridad de los datos personales en posesión del Centro de Investigaciones Interdisciplinarias en Ciencias y Humanidades de la Universidad Nacional Autónoma de México, lo que ocasionaría una posible comisión de delitos previstos por el Código Penal Federal, como son: Acceso no autorizado a los sistemas , robo de información, suplantación de identidades entre otros. Fundamento legal: Artículo 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública; artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en correlación con el artículo 41 del Reglamento de Transparencia y Acceso a la información Pública de la Universidad Nacional Autónoma de México y los numerales Quincuagésimo Sexto y Sexagésimo Primero de los Lineamientos Generales en materia de Clasificación y Desclasificación de la información, así como para la elaboración de versiones públicas. Periodo de Reserva. Cinco años a partir del 24 de agosto de 2022.

Anexo VI. Capacitación.

Dentro de la capacitación para la comunidad del CEIICH, se contemplan:

- Charlas informativas sobre temas de protección de datos personales.
- Correos masivos con información del tema.
- Generación de elementos gráficos con información de protección de datos personales.

Esta capacitación deberá incluir los siguientes temas:

I. Los requerimientos y actualizaciones del sistema de gestión;
II. La legislación vigente en materia de protección de datos personales y las mejores prácticas relacionadas con el tratamiento de éstos;
III. Las consecuencias del incumplimiento de los requerimientos legales o requisitos organizacionales, y
IV. Las herramientas tecnológicas relacionadas o utilizadas para el tratamiento de los datos personales y para la implementación de las medidas de seguridad.

Anexo VII. Formato universitario de “Solicitud de ejercicio de derechos ARCO”.

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

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

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

2. Datos del Titular de los Datos Personales*:

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

3. Datos del solicitante:

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

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

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

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

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

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

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

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

☐ACCESO

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

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

_____
Firma o huella dactilar*

Plazos y procedimiento para la atención de las solicitudes de ejercicio de derechos ARCO:
Una vez que se presentó la solicitud, esta área universitaria cuenta con:

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

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

Anexo VIII. Carta de confidencialidad

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

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

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

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

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

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

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

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

a) Cuando la información se encuentre en el dominio público en el momento en que me sea suministrada o, una vez suministrada, ésta se haga pública.

b) Cuando la legislación vigente o un mandato judicial exija su divulgación.

c) Cuando la información se desarrolle o reciba legítimamente de terceros, de forma totalmente independiente a mi relación con la Universidad.

A t e n t a m e n t e

_____

Firma o huella dactilar