DOCUMENTO DE SEGURIDAD DEL COLEGIO DE CIENCIAS Y HUMANIDADES, PLANTEL NAUCALPAN

MAYO 2022

ÍNDICE

INTRODUCCIÓN 3
PRESENTACIÓN 4
AVISO DE PRIVACIDAD 4
I. INVENTARIO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO. 8
II. FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATAN DATOS PERSONALES. 9
III. ANÁLISIS DE RIESGOS EN EL TRATAMIENTO DE DATOS PERSONALES. 10
IV. ANÁLISIS DE BRECHA. 10
V. PLAN DE TRABAJO. 10
VI. MEDIDAS DE SEGURIDAD. 11
VII. PROGRAMA GENERAL DE CAPACITACIÓN. 12
VIII. MEJORA CONTINUA 12
IX. RUTA CRÍTICA PARA CUMPLIMIENTO DE LAS MEDIDAS DE SEGURIDAD TÉCNICAS (MST) 12

ANEXOS 14

ANEXO 1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES 14
ANEXO 2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES 15
ANEXO 3. ANÁLISIS DE RIESGOS 22
ANEXO 4. ANÁLISIS DE BRECHA 25
ANEXO 5. PLAN DE TRABAJO 27
ANEXO 6. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD 29
ANEXO 7. PROGRAMA ESPECIFICO DE CAPACITACIÓN 39
ANEXO 8. MEJORA CONTINUA 42
ANEXO 9. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD 49

INTRODUCCIÓN

El presente documento de seguridad contiene las medidas de seguridad administrativa, física y técnica aplicables a los sistemas de tratamiento de datos personales de la esta área universitaria 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.

Este modelo pretende brindar a las áreas universitarias homogeneidad en la redacción, organización y contenido para que elaboren su propio documento de seguridad en el que se describan las tres medidas de seguridad para la protección de los datos personales.

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 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, lo cual se encuentran contemplado en el estándar internacional en materia de seguridad de la información ISO/IEC 27002:2013 "*Tecnología de la información - Técnicas de seguridad - Código de práctica para los controles de seguridad de la información".*

PRESENTACIÓN

El CCH Naucalpan, ha mantenido reglas de protección de datos personales incluso antes de que se constituyera de manera legal este concepto, el resguardo documental de los alumnos se hacía en las instalaciones del Local de Registro a Aspirantes, con medidas de seguridad que mantenían sus documentos personales a buen resguardo, Ciudad Universitaria. Ya en el plantel, los datos se conservaban en tarjetones guardados bajo llave y con la llegada de la era digital, los datos en este formato tuvieron preponderancia, por lo cual, se siguen normas específicas para mantener la privacidad de la información personal de alumnos y profesores.

Este documento tiene el objetivo de documentar las actividades realizadas para integrar nuestro Sistema de Gestión de la Seguridad de Datos Personales en el CCH Naucalpan. Se trata de la primera versión del documento, el cual se enriquecerá conforme se vayan cumpliendo las tareas trazadas en el mismo, se hagan verificaciones de medidas implantadas o se cree o modifique sustancialmente algún sistema de tratamiento de datos personales. El alcance de este sistema se centra en proteger “Todos los datos personales y datos personales sensibles que recibe de instancias externas, los que recabe y use el CCH Naucalpan” de accesos no autorizados ni de tratamientos distintos a los fines para los que fueron destinados.

AVISO DE PRIVACIDAD

De conformidad con lo establecido en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, La Escuela Nacional Colegio de Ciencias y Humanidades, Plantel Naucalpan pone a su disposición el siguiente aviso de privacidad.

La Escuela Nacional Colegio de Ciencias y Humanidades, Plantel Naucalpan es responsable del uso y protección de sus datos personales, en este sentido y atendiendo las obligaciones legales establecidas en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, a través de este instrumento se informa a los titulares de los datos, la información que de ellos se recaba y los fines que se le darán a dicha información.

Además de lo anterior, informamos a usted que La Escuela Nacional Colegio de Ciencias y Humanidades, Plantel Naucalpan tiene su domicilio ubicado en Calzada de los Remedios número 10, colonia Bosque de los Remedios, Naucalpan, Estado de México, entre Avenida Norteamérica y Calle Morelos, código postal 53400.

Los datos personales que recabamos de usted serán utilizados para las siguientes finalidades, las cuales son necesarias para concretar nuestra relación con usted, así como para atender los servicios y pedidos que solicite:

En el caso de los datos del alumnado,

-Para registrar su inscripción.

-Para generar su credencial.

-Para generar su horario

-Para generar su constancia de inscripción

-Para generar su tira de materias

-Para generar la lista de asistencia para cada profesor

-Si solicita una baja temporal

-Si solicita una baja definitiva

-Para inscribirlo a cursos extracurriculares

-Para generar constancias de asistencia a cursos

-Para generar diplomas de cursos o de aprovechamiento

-Para generar reconocimientos

-Para comunicarle eventos o trámites importantes

-Para contactar a su familia si sufre algún accidente o hecho delictivo

-Para generar estadísticas internas

-Para la aplicación de instrumentos de evaluación de ingreso, egreso y especiales.

-Para mantener su historia académica

-Para usar los servicios de la biblioteca del Plantel y de la UNAM

-Para acceder a beneficios de apoyo de software licenciado.

-Para permitirle ingresar a opciones técnicas y obtener una cédula.

-Para generar su certificado de estudios oficial.

-Para tramitar su pase a facultad

-Para tramitar su beca

-Para darse de alta en recursamientos

-Para inscribirse a cursos de Apoyo al Egreso (PAE) o en línea (PAL)

-Para solicitar exámenes extraordinarios.

-Para poder participar en las elecciones internas.

-Para solicitar permisos para prácticas foraneas.

-Para participar en concursos académicos o deportivos.

En el caso del profesorado:

-Para dar ingreso a su solicitud de alta

-Para trámite del SAT

-Para que Dirección General de Personal le genere su cheque o depósito

-Para permitirle seleccionar grupos boletinados

-Para llevar el control de sus permisos económicos e incidencias de asistencia

-Para asignarle grupos solicitados

-Para emitirle sus listas de asistencia

-Para emitirle su horario de impartición de clases

-Para capturar sus puntajes de lista jerarquizada

-Para votar y ser votado en las elecciones internas de los diferentes órganos académicos

-Para llamarle a un familiar en caso de accidente o incidencia de salud

-Para sus trámites ante el Sindicado de Académicos UNAM

Para llevar a cabo las finalidades descritas en el presente aviso de privacidad, utilizaremos los siguientes datos personales:

Apellido paterno, apellido materno, nombre(s), número de cuenta, curp, domicilio con calle y número, colonia, alcaldía o municipio, entidad federativa, código postal, fotografía, número de teléfono celular, número de teléfono de casa o de algún conocido para dejar recados, correo electrónico personal, nombre del padre o tutor, datos médicos del examen que le practica la UNAM para el alumnado y para docentes, Nombre, apellidos, RFC, curp, fecha de nacimiento, domicilio, calle y número, colonia, código postal, correo personal, teléfono de casa y celular, escuela de procedencia y fotografía.

Por otra parte, informamos a usted, que sus datos personales no serán compartidos con ninguna autoridad, empresa, organización o persona distintas a nosotros y serán utilizados exclusivamente para los fines señalados.

Usted tiene en todo momento el derecho a conocer qué datos personales tenemos de usted, para qué los utilizamos y las condiciones de uso que les damos (Acceso). Asimismo, es su derecho solicitar la corrección de su información personal en caso de que esté desactualizada, sea inexacta o incompleta (Rectificación); de igual manera, tiene derecho a que su información se elimine de nuestros registros o bases de datos cuando considere que la misma no está siendo utilizada adecuadamente (Cancelación); así como también a oponerse al uso de sus datos personales para fines específicos (Oposición). Estos derechos se conocen como derechos ARCO.

Para el ejercicio de cualquiera de los derechos ARCO, se deberá presentar la solicitud respectiva a través de los formatos que estarán a su disposición en:

http://www.cch-naucalpan.unam.mx/arco/

Lo anterior también servirá para conocer el procedimiento y requisitos para el ejercicio de los derechos ARCO.

En todo caso la respuesta a la solicitud se dará en los siguientes 30 días hábiles siguientes.

Los datos de contacto de la persona o departamento de datos personales, que está a cargo de dar trámite a las solicitudes de derechos ARCO son los siguientes:

Secretaría de Administración Escolar para el alumnado, C.P. Guadalupe Sánchez Chávez, con Domicilio de trabajo en Calzada de los Remedios número 10, colonia Bosque de los Remedios, Naucalpan, Estado de México, entre Avenida Norteamérica y Calle Morelos, código postal 53400. y teléfono 5553600323 extensión 273

Personal Académico, para la planta docente. Lic. María Teresa Díaz Navarro, con Domicilio de trabajo en Calzada de los Remedios número 10, colonia Bosque de los Remedios, Naucalpan, Estado de México, entre Avenida Norteamérica y Calle Morelos, código postal 53400. y teléfono 5553600323 extensión 258

Cabe mencionar, que en cualquier momento usted puede revocar su consentimiento para el uso de sus datos personales. Del mismo modo, usted puede revocar el consentimiento que, en su caso, nos haya otorgado para el tratamiento de sus datos personales.

Así mismo, usted deberá considerar que para ciertos fines la revocación de su consentimiento implicará que no podamos seguir prestando el servicio que nos solicitó, o la conclusión de su relación con nosotros.

Para revocar el consentimiento que usted otorga en este acto o para limitar su divulgación, se deberá presentar la solicitud respectiva a través de los formatos que estarán a su disposición en:

http://www.cch-naucalpan.unam.mx/revocacion/

Del mismo modo, podrá solicitar la información para conocer el procedimiento y requisitos para la revocación del consentimiento, así como limitar el uso y divulgación de su información personal.

En cualquier caso, la respuesta a las peticiones se dará a conocer en un plazo de 30 días hábiles a partir de la fecha de recepción de la petición.

Si llegara a haber un cambio en nuestros procedimientos internos o por otras causas, nos comprometemos a mantenerlo informado sobre los cambios que pueda sufrir el presente aviso de privacidad, sin embargo, usted puede solicitar información sobre si el mismo ha sufrido algún cambio a través de la siguiente dirección electrónica:

http://www.cch-naucalpan.unam.mx/avisoprivacidad/

I. INVENTARIO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO.

Uno de los procesos más importantes en el CCH Naucalpan es la de recibir, por parte de la Dirección General del Colegio de Ciencias y Humanidades los datos personales del alumnado, sus fotografías, así como su número de cuenta y grupo asignado para realizar su trámite de inscripción y trámites posteriores de acuerdo con la trayectoria escolar del alumnado.

De igual manera, el ingreso de profesores que desean atender grupos en el CCH, requieren de sus datos personales para realizar los trámites de alta en diferentes instancias para cuadrar su alta en la UNAM y en la Secretaría de Hacienda y Crédito Público. Incluida la toma de fotografías para la credencialización, estos datos son manejados por Dirección General de Personal y del propio CCH mientras se mantenga el vínculo laboral en la Institución.

El Departamento de Sistemas con la finalidad del tratamiento de información, ha creado un conjunto de programas de trámites que usan los datos personales del profesorado y alumnado para realizar los trámites internos durante su estancia en el Plantel. Así como los datos personales mencionados en el anexo 1. Para el alumnado, existe el sistema MENUCE, para la inscripción, reinscripción, generación de horarios, ingreso a cursos especiales de recuperación como PAE (programa de apoyo al egreso), PAI (programa de acreditación inmediata), Recursamiento y Repetidores, exámenes extraordinarios, cursos extracurriculares, becas, expedición de reconocimientos, diplomas, constancias de inscripción y credenciales. Las asignaciones de sinodales (profesores) para los procesos de exámenes extraordinarios, PAE y PAI para generar los avisos de pago correspondientes a la DGP (Dirección General de Personal). Para los casos en que se presenta un accidente o percance hay un sistema de consulta para contactar al padre o tutor y todos sus datos personales. Los usuarios de estos programas de este sistema son los miembros del Departamento de Control Escolar, que pertenece a la Secretaría de Administración Escolar.

De manera paralela, el sistema MENUSA de programas para trámites, permiten al profesorado la solicitud de grupos boletinados, la generación de boletines, la asignación de grupos, control de asistencia e incidencias académicas como permisos económicos, citas médicas y faltas justificadas, prórrogas, reanudaciones, generación de listas de asistencia, horarios de grupos, listas de alumnos tanto para grupos regulares, recursamientos, de exámenes extraordinarios y cursos especiales de PAE y PAI. También los procesos de consulta y alta para documentos de la lista jerarquizada, relativa a las acreditaciones de estudios y cursos. Los usuarios de este sistema son miembros de la Secretaría Académica, que, además, para trámites a otras instancias universitarias, tienen la consulta de cobertura de grupos, por muchos criterios diferentes, listas de profesores, datos de

profesores, puntaje desglosado de lista jerarquizada, propuesta global de horarios, permutas, comisiones, licencias y padrón vehicular.

El formato de almacenamiento para los sistemas MENUSA y MENUCE se combinan 5 entidades de programación, HTML, PHP, JavaScript, CSS y Base de datos MySQL tipo cliente servidor de trámites escolares y control de datos de alumnos. Ubicados físicamente Centro de cómputo, disco duro de respaldo, dentro de archivero metálico con llave. Puerta de alta seguridad de metal rígido de doble chapa, con láminas calibre 13 de ambos lados, mencionado en el Anexo 2: Estructura y descripción de los sistemas de tratamiento de datos personales

El detalle de los datos personales que se manejan en cada componente de los sistemas mencionados se describe en el Anexos 1: Inventario de sistemas de tratamiento de datos personales

La descripción general de la ubicación física de los datos, así como su forma de almacenaje que se manejan en cada componente de los sistemas mencionados, se describe en el Anexos 2: Estructura y descripción de los sistemas de tratamiento de datos personales.

II. FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATAN DATOS PERSONALES.

Para el sistema MENUCE, son los siguientes:

Titular de la Secretaría de Administración Escolar. Supervisa que los trámites del alumnado se lleven a cabo en tiempo y forma, soluciona los incidentes y problemáticas que se presenten, atiende a padres de familia, profesores y alumnos que los soliciten.

Personal de Control Escolar. Se encargan de la parte operativa del los trámites, de solucionar dudas y llevar a cabo los trámites que no están en línea o los híbridos.

Para el sistema MENUSA, son los siguientes:

Titular de la Secretaría Académica. Supervisa la correcta ejecución de los trámites del profesorado, asigna grupos conforme al puntaje de la lista jerarquizada, que actualiza el personal de esta entidad. Soluciona problemas relacionados con los procesos cíclicos de cada semestre que le solicite el profesorado del Plantel.

Apoyo a Cuerpos Colegiados. Se encarga de mantener los trámites de cambio de categoría, concursos de oposición, definitividades y otros procesos del profesorado.

Control de Asistencia Docente. Llevan el control de la asistencia del profesorado, contabilizan estadísticas para otras instancias de la UNAM, como DGP (Dirección General de Personal), generan las listas y capturan incidencias.

El detalle con las funciones y responsabilidades de cada perfil está descrito en el Anexo 2 Funciones y obligaciones de quienes traten datos personales

III. ANÁLISIS DE RIESGOS EN EL TRATAMIENTO DE DATOS PERSONALES.

El manejo de datos personales y sus procesos están sujetos a riesgos, los cuales amenazan con explotar las vulnerabilidades de los sistemas de información. Por este motivo, hay que tomar medidas adicionales de protección, además de las normales, como hacer firmar a todos los que tienen acceso cartas de confidencialidad de datos personales, mantener actualizados los sistemas de protección como antivirus, firewall y evitar las malas prácticas que podrían poner en riesgo la seguridad de los datos personales.

El detalle del análisis de riesgos está descrito en el Anexo 3 Análisis de riesgos en el tratamiento de datos personales

IV. ANÁLISIS DE BRECHA.

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

I. Las medidas de seguridad existentes y efectivas;
II. El nivel óptimo de medidas de seguridad
III. Las medidas de seguridad adicionales a las existentes para alcanzar el nivel óptimo.

El detalle de las actividades de este análisis está descrito en el Anexo 4 Análisis de Brecha

V. PLAN DE TRABAJO.

Una vez realizado el análisis de riesgos y haber identificado los controles faltantes para mitigar cada riesgo, se hace un plan para implementar los controles de seguridad faltantes, en cual se identifican estos controles, las actividades a realizar para implementar el control, el tiempo estimado

para completar las actividades, la prioridad que se dará a dicho control y finalmente, las áreas responsable(s) de su implementación.

El detalle de las actividades de este plan está descrito en el Anexo 5 Plan de Trabajo

VI. MEDIDAS DE SEGURIDAD.

Las medidas de seguridad para la gestión de datos personales en base a la legislación en la materia, tanto nacional como local, definen un conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos, que permiten proteger los datos tanto de trabajadores como de alumnos y profesores.

Las acciones realizadas en esta materia dentro de los sistemas MENUSA y MENUCE son:

- Restringir los accesos a personal no autorizado, debido a la posibilidad de ingresos no autorizados en la zona de trabajo del plantel.
- Claves personalizadas y modificación de programas para registrar los accesos, para el control de las actividades, horarios y modificaciones que se puedan realizar en los sistemas.
- En caso de una toma de instalaciones, se pone en operación un servidor virtual en DGCCH y se carga el último respaldo.
- En el escenario de que exista alguna alteración de la información, se procede a la recarga de la información total del respaldo más reciente.
- Cuando haya daño total o parcial a la base de datos, se recargará la estructura de las bases, junto con el contenido, por comandos MySQL.
- Cunado se detecte un daño físico al servidor, se procederá a la instalación de un servidor en virtualizado en la DGCCH.
- Para evitar ataques informáticos realizados desde lugares remotos de Internet, e internos en el plantel, se mantiene la actualización continua de paquetes de seguridad en el servidor de la base de datos y actualización del firewall de este.

MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD.

Para mantener los sistemas funcionando de manera adecuada y proteger los datos personales que están contenidos, se mantiene un monitoreo constante de los sistemas, mediante protocolos y normas, actualización de componentes de software de protección y manteniéndose al día respecto a la instalación de los parches de seguridad y nuevas amenazas a la seguridad.

El detalle de las actividades de este apartado está en el Anexo 6 Mecanismos de monitoreo y revisión de las medidas de seguridad.

VII. PROGRAMA ESPECIFICO DE CAPACITACIÓN.

Para lograr el objetivo de proteger los datos personales del alumnado y el profesorado, se tiene que mantener una capacitación constante al personal sobre las nuevas amenazas y formas de ataque a la seguridad, para prevenir ataques de ingeniería social, pues los humanos somos el eslabón más débil en los procesos de seguridad.

El detalle del este apartado está en el Anexo 7 Programa específico de capacitación.

VIII. MEJORA CONTINUA

Todos los sistemas y las personas que los manejan se pueden mejorar, unos, con la incorporación de nuevas tecnologías, como sistemas de contraseñas más seguras, códigos QR, lectores biométricos, chaptcha, algoritmos de encriptación de 128 o 256 bits, túneles privados virtuales, etc. Y para el caso del personal, cursos sobre nuevas herramientas para facilitar su trabajo, modificaciones a los sistemas para mejorar la usabilidad de los mismos.

Los detalles sobre este apartado están en el Anexo 8 Mejora Continua.

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

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

A) 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.

B) 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.

C) 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 del documento se registran las actividades realizadas para cumplir con lo dispuesto para la etapa 1 en el Anexo 4. Análisis de Brecha y los Formatos para cumplimiento de las MST se encuentran en el anexo 12 Ruta Crítica para cumplimiento de las medidas de seguridad técnicas (mst).

ANEXO 1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

ESCUELA NACIONAL COLEGIO DE CIENCIAS Y HUMANIDADES, PLANTEL NAUCALPAN	
Identificador único*	**menuce**
Nombre del sistema *	**Menú de sistemas para tramites de Control Escolar**
Datos personales (sensibles o no) contenidos en el sistema*:	**Datos personales de los alumnos**: Apellidos, Nombre, número de cuenta, fotografía, domicilio, calle y número, colonia, municipio o alcaldía, código postal, curp, fecha de nacimiento, género, número de teléfono celular, de casa, del padre o tutor y su nombre. Correo electrónico personal y fotografía. Puntaje de ingreso, promedio de secundaria, resultado del EDI (Exámen de Diagnóstico de Ingreso) y escuela de procedencia. Discapacidades detectadas por el EMA (Examen Médico Automatizado) **Datos académicos de los alumnos**: Semestre, asignaturas inscritas, horario, calificaciones, número de asignaturas reprobadas, salón o laboratorio donde cursa las asignaturas, cursos especiales PAE, PAI, PAL, exámenes extraordinarios, estatus de repetidor o recursador, correo electrónico institucional.
Responsable*:	Sistemas
Nombre*:	**Ing. Julio Eugenio Navarro Córdova**
Cargo*:	**Jefe del Departamento de Sistemas CCHN**

Identificador único	**menusa**
Nombre del sistema*	**Menú de sistemas para trámites de la Secretaría Académica**
Datos personales contenidos en el sistema*:	**Datos personales:** Nombre, apellidos, RFC, curp, fecha de nacimiento, domicilio, calle y número, colonia, código postal, correo personal, teléfono de casa y celular, escuela de procedencia y fotografía **Datos académicos:** Antigüedad CCH, antigüedad UNAM, definitividad, grado escolar, categoría, asignaturas que imparte, horario, propuesta global, horas de apoyo, número de plaza, carrera, boletines solicitados, permutas, reanudaciones, grupos asignados, lista jerarquizada que contiene constancias de todo tipo, cursos, tutorías, PAE, diplomados, certificados.
Responsable:	Sistemas
Nombre*:	**Ing. Julio Eugenio Navarro Córdova**
Cargo*:	**Jefe del Departamento de Sistemas.**

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

ESCUELA NACIONAL COLEGIO DE CIENCIAS Y HUMANIDADES, PLANTEL NAUCALPAN	
Identificador único¨*	**menuce**
(Nombre del sistema A1*)	**Menú de sistemas para tramites de Control Escolar**
Tipo de soporte[1]:*	El sistema se encuentra en soporte físico y electrónico
Descripción[2]:*	Sistema combina 5 entidades de programación, HTML, PHP, JavaScript, CSS y Base de datos MySQL tipo cliente servidor de trámites escolares y control de datos de alumnos. Protegido por firewall, se aloja en el servidor principal del plantel, unidad de almacenamiento de estado sólido, acceso por identificador y contraseña para cada trámite.
Características del lugar donde se resguardan los soportes[3]:*	Centro de cómputo, disco duro de respaldo, dentro de archivero metálico con llave. Puerta de alta seguridad de metal rígido de doble chapa, con láminas calibre 13 de ambos lados.
Identificador único¨*	**menusa**
(Nombre del sistema A2*)	**Menú de sistemas para trámites de la Secretaría Académica**
Tipo de soporte*:	El sistema se encuentra en soporte físico y electrónico
Descripción*:	Sistema combina 5 entidades de programación, HTML, PHP, JavaScript, CSS y Base de datos MySQL tipo cliente servidor para trámites y control de datos académicos, protegido por firewall, se aloja en el servidor principal del plantel, unidad de almacenamiento de estado sólido, acceso por identificador y contraseña para cada trámite.
Características del lugar donde se resguardan los soportes*:	Centro de cómputo, disco duro de respaldo, dentro de archivero metálico con llave. Puerta de alta seguridad de metal rígido de doble chapa, con láminas calibre 13 de ambos lados.

FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATAN DATOS PERSONALES.

ESCUELA NACIONAL COLEGIO DE CIENCIAS Y HUMANIDADES, PLANTEL NAUCALPAN	
Identificador único*	**menuce**

[1] En caso de que el área universitaria prevea cambiar el tipo de soporte que utiliza el sistema de tratamiento de datos personales por ejemplo de físico a electrónico o en el supuesto de que prevea en el futuro utilizar ambos tipos de soportes, deberá indicarse en este rubro.

[2] Describir el soporte en el que se encuentran los datos por ejemplo para soportes físicos podrían ser formatos, listados, documentos o expedientes, entre otros y para soportes electrónicos, hoja de cálculo o base de datos relacional, entre otros.

[3] Para describir las características del lugar donde se resguardan los soportes, se deberá considerar lo siguiente:

a) Para soportes físicos, el área universitaria deberá incluir una descripción escrita con detalles sobre las características físicas de la oficina, almacén o bodega donde resguarda dichos soportes;

b) Para soportes electrónicos, la descripción ofrecida por el área universitaria deberá incluir un diagrama de la arquitectura de seguridad en el cual sea posible apreciar el flujo de datos a través de la o las redes electrónicas que interconectan los equipos (clientes, servidores, cortafuegos, unidades de almacenamiento, entre otros) del sistema de tratamiento de datos personales. Además, deberá describir las medidas de seguridad física que ha implementado para la protección del centro de datos donde residen tales soportes.

c) En caso de que el sistema de tratamiento de datos personales ocupe ambos tipos de soportes, deberá presentar las descripciones correspondientes a cada uno, en términos de lo señalado en los incisos a) y b) anteriores.

Nombre del sistema *	**Menú de sistemas para tramites de Control Escolar**
Nombre del Encargado 1*	**Lic. María Guadalupe Sánchez Chávez**
Cargo*:	**Secretaria de Administración Escolar.**
Funciones*:	Usar adecuadamente los los sistemas de trámites de control escolar para dar un servicio eficiente a los alumnos y profesores que lo necesiten, atender a padres de familia y autoridades que soliciten información de alumnos.
Obligaciones*:	Captura de datos para trámites de todo tipo con alumnos, apertura de periodos de inscripción, reinscripción, para semestres ordinarios, repetidores y recursadores. Envío de archivos en formato SIAE a la DGCCH, control de los datos para asignación de sinodales en exámenes extraordinario. Toma de fotografías y recopilación de documentos.
	Usuarios:
Nombre del Usuario 1*	Sr. Ismael Eduardo Contreras González
Cargo*:	Jefe de oficina
Funciones*:	Ayudar al personal de base que apoya a la Secretaría de Administración Escolar a cumplir con las tareas encomendadas
Obligaciones*:	Supervisar el correcto proceso de los trámites de control escolar, capturar y verificar los datos de alumnos y profesores relacionados con los trámites de la Secretaría de Administración Escolar.
Nombre del Usuario 2	Sra. María Guadalupe Limón Trujillo
Cargo*:	Oficinista de servicios escolares
Funciones*:	Apoyar a los sistemas de control de trámites para que concluyan de manera eficiente, Atender a alumnos y profesores.
Obligaciones*:	Dar cumplimiento en tiempo y forma a la captura de datos necesarios para hacer funcionar correctamente los sistemas de control de trámites de alumnos y profesores. Proporcionar atención relacionada con trámites de control escolar a los alumnos y profesores que la soliciten.
Nombre del Usuario 3	Sra. Margarita Limón Trujillo
Cargo*:	Oficinista de servicios escolares
Funciones*:	Apoyar a los sistemas de control de trámites para que concluyan de manera eficiente, Atender a alumnos y profesores.
Obligaciones*:	Dar cumplimiento en tiempo y forma a la captura de datos necesarios para hacer funcionar correctamente los sistemas de control de trámites de alumnos y profesores. Proporcionar atención relacionada con trámites de control escolar a los alumnos y profesores que la soliciten.
Nombre del Usuario 4*	Sra. Martha Mejía Mejía
Cargo*:	Oficinista de servicios escolares
Funciones*:	Apoyar a los sistemas de control de trámites para que

	concluyan de manera eficiente, Atender a alumnos y profesores.
Obligaciones*:	Dar cumplimiento en tiempo y forma a la captura de datos necesarios para hacer funcionar correctamente los sistemas de control de trámites de alumnos y profesores. Proporcionar atención relacionada con trámites de control escolar a los alumnos y profesores que la soliciten.
Nombre del Usuario 5*	Sr. Alberto García Carrillo
Cargo*:	Oficinista de servicios escolares
Funciones*:	Apoyar a los sistemas de control de trámites para que concluyan de manera eficiente, Atender a alumnos y profesores.
Obligaciones*:	Dar cumplimiento en tiempo y forma a la captura de datos necesarios para hacer funcionar correctamente los sistemas de control de trámites de alumnos y profesores. Proporcionar atención relacionada con trámites de control escolar a los alumnos y profesores que la soliciten.
Nombre del Usuario 6*	Sra. Corina Ramírez Peralta
Cargo*:	Oficinista de servicios escolares
Funciones*:	Apoyar a los sistemas de control de trámites para que concluyan de manera eficiente, Atender a alumnos y profesores.
Obligaciones*:	Dar cumplimiento en tiempo y forma a la captura de datos necesarios para hacer funcionar correctamente los sistemas de control de trámites de alumnos y profesores. Proporcionar atención relacionada con trámites de control escolar a los alumnos y profesores que la soliciten.
Nombre del Usuario 7*	Sra. Adriana Mendez Bardales
Cargo*:	Oficinista de servicios escolares
Funciones*:	Apoyar a los sistemas de control de trámites para que concluyan de manera eficiente, Atender a alumnos y profesores.
Obligaciones*:	Dar cumplimiento en tiempo y forma a la captura de datos necesarios para hacer funcionar correctamente los sistemas de control de trámites de alumnos y profesores. Proporcionar atención relacionada con trámites de control escolar a los alumnos y profesores que la soliciten.
Nombre del Usuario 8*	Sra. Ana María Toledo Arriaga
Cargo*:	Oficinista de servicios escolares
Funciones*:	Apoyar a los sistemas de control de trámites para que concluyan de manera eficiente, Atender a alumnos y profesores.
Obligaciones*:	Dar cumplimiento en tiempo y forma a la captura de datos necesarios para hacer funcionar correctamente los sistemas de control de trámites de alumnos y profesores. Proporcionar atención relacionada con trámites de control escolar a los alumnos y profesores que la soliciten.
Nombre del Usuario 9*	Sra. Areli Hernández Jiménez
Cargo*:	Oficinista de servicios escolares
Funciones*:	Apoyar a los sistemas de control de trámites para que concluyan de manera eficiente, Atender a alumnos y profesores.
Obligaciones*:	Dar cumplimiento en tiempo y forma a la captura de datos necesarios para hacer funcionar correctamente los sistemas

	de control de trámites de alumnos y profesores. Proporcionar atención relacionada con trámites de control escolar a los alumnos y profesores que la soliciten.
Nombre del Usuario 10*	Sra. Martha Patricia Camarena González
Cargo*:	Oficinista de servicios escolares
Funciones*:	Apoyar a los sistemas de control de trámites para que concluyan de manera eficiente, Atender a alumnos y profesores.
Obligaciones*:	Dar cumplimiento en tiempo y forma a la captura de datos necesarios para hacer funcionar correctamente los sistemas de control de trámites de alumnos y profesores. Proporcionar atención relacionada con trámites de control escolar a los alumnos y profesores que la soliciten.
Nombre del Usuario 11*	Sra. Ana María Fernández Vaca
Cargo*:	Oficinista de servicios escolares
Funciones*:	Apoyar a los sistemas de control de trámites para que concluyan de manera eficiente, Atender a alumnos y profesores.
Obligaciones*:	Dar cumplimiento en tiempo y forma a la captura de datos necesarios para hacer funcionar correctamente los sistemas de control de trámites de alumnos y profesores. Proporcionar atención relacionada con trámites de control escolar a los alumnos y profesores que la soliciten.
Nombre del Usuario 12*	Sr. Jesús Rafaél Ayala Rodríguez
Cargo*:	Oficinista de servicios escolares
Funciones*:	Apoyar a los sistemas de control de trámites para que concluyan de manera eficiente, Atender a alumnos y profesores.
Obligaciones*:	Dar cumplimiento en tiempo y forma a la captura de datos necesarios para hacer funcionar correctamente los sistemas de control de trámites de alumnos y profesores. Proporcionar atención relacionada con trámites de control escolar a los alumnos y profesores que la soliciten.
Nombre del Usuario 13*	Sra. Paola Janet Bernal Sánchez
Cargo*:	Oficinista de servicios escolares
Funciones*:	Apoyar a los sistemas de control de trámites para que concluyan de manera eficiente, Atender a alumnos y profesores.
Obligaciones*:	Dar cumplimiento en tiempo y forma a la captura de datos necesarios para hacer funcionar correctamente los sistemas de control de trámites de alumnos y profesores. Proporcionar atención relacionada con trámites de control escolar a los alumnos y profesores que la soliciten.
Nombre del Usuario 14*	Sra. Sonia Chávez Carrillo
Cargo*:	Oficinista de servicios escolares
Funciones*:	Apoyar a los sistemas de control de trámites para que concluyan de manera eficiente, Atender a alumnos y profesores.
Obligaciones*:	Dar cumplimiento en tiempo y forma a la captura de datos necesarios para hacer funcionar correctamente los sistemas de control de trámites de alumnos y profesores. Proporcionar atención relacionada con trámites de control escolar a los alumnos y profesores que la soliciten.
Nombre del Usuario 15*	Sra. Sofía Gabriela Chávez Robles
Cargo*:	Oficinista de servicios escolares
Funciones*:	Apoyar a los sistemas de control de trámites para que concluyan de manera eficiente, Atender a alumnos y

	profesores.
Obligaciones*:	Dar cumplimiento en tiempo y forma a la captura de datos necesarios para hacer funcionar correctamente los sistemas de control de trámites de alumnos y profesores. Proporcionar atención relacionada con trámites de control escolar a los alumnos y profesores que la soliciten.
Nombre del Usuario 16*	Sra. María Guadalupe González Martínez
Cargo*:	Oficinista de servicios escolares
Funciones*:	Apoyar a los sistemas de control de trámites para que concluyan de manera eficiente, Atender a alumnos y profesores.
Obligaciones*:	Dar cumplimiento en tiempo y forma a la captura de datos necesarios para hacer funcionar correctamente los sistemas de control de trámites de alumnos y profesores. Proporcionar atención relacionada con trámites de control escolar a los alumnos y profesores que la soliciten.
Nombre del Usuario 17*	Sra. Carmen Martínez Ramírez
Cargo*:	Oficinista de servicios escolares
Funciones*:	Apoyar a los sistemas de control de trámites para que concluyan de manera eficiente, Atender a alumnos y profesores.
Obligaciones*:	Dar cumplimiento en tiempo y forma a la captura de datos necesarios para hacer funcionar correctamente los sistemas de control de trámites de alumnos y profesores. Proporcionar atención relacionada con trámites de control escolar a los alumnos y profesores que la soliciten.
Nombre del Usuario 18*	Sra. Samantha Adriana Mills Pérez
Cargo*:	Oficinista de servicios escolares
Funciones*:	Apoyar a los sistemas de control de trámites para que concluyan de manera eficiente, Atender a alumnos y profesores.
Obligaciones*:	Dar cumplimiento en tiempo y forma a la captura de datos necesarios para hacer funcionar correctamente los sistemas de control de trámites de alumnos y profesores. Proporcionar atención relacionada con trámites de control escolar a los alumnos y profesores que la soliciten.
Nombre del Usuario 19*	Sra. Yosselyn Serna González
Cargo*:	Oficinista de servicios escolares
Funciones*:	Apoyar a los sistemas de control de trámites para que concluyan de manera eficiente, Atender a alumnos y profesores.
Obligaciones*:	Dar cumplimiento en tiempo y forma a la captura de datos necesarios para hacer funcionar correctamente los sistemas de control de trámites de alumnos y profesores. Proporcionar atención relacionada con trámites de control escolar a los alumnos y profesores que la soliciten.
Nombre del Usuario 20*	Sra. Gabriela Vázquez García
Cargo*:	Oficinista de servicios escolares
Funciones*:	Apoyar a los sistemas de control de trámites para que concluyan de manera eficiente, Atender a alumnos y profesores.
Obligaciones*:	Dar cumplimiento en tiempo y forma a la captura de datos necesarios para hacer funcionar correctamente los sistemas de control de trámites de alumnos y profesores. Proporcionar atención relacionada con trámites de control escolar a los alumnos y profesores que la soliciten.

Identificador único	**menusa**
Nombre del sistema*:	**Menú de sistemas para trámites de la Secretaría Académica**
	Encargados:
Nombre del Encargado 1*	**Damián Feltrin Rodríguez**
Cargo*:	**Secretario Académico**
Funciones*:	Mantener los servicios académicos del plantel hacia los docentes en los mejores términos.
Obligaciones*:	Solucionar problemas académicos que tengan que ver con la tramitología, comunicarse con los profesores en conflicto, asignar los grupos solicitados por el proceso de boletinaje, con base en la captura de lista jerarquizada. Supervisar la actualización de la lista jerarquizada. Eliminar traslapes de horarios o de salones, con apoyo de los sistemas de información. Validar la propuesta global de horarios ante el sindicato del AAPAUNAM
	Usuarios:
Nombre del Usuario 1*	Ing. Gustavo Contreras Pérez
Cargo*:	Apoyo a Cuerpos Colegiados
Funciones*:	Ayudar a los profesores en trámites académicos varios.
Obligaciones*:	Mantener actualizado el sistema de control de datos académicos sobre cambios de categoría, Apoyar para mantener actualizado el sistema de lista jerarquizada.
Nombre del Usuario 2*	Ing. Daniel Soriano Varela
Cargo*:	Control de Asistencia Docente
Funciones*:	Llevar el control de asistencia y de las incidencias del personal académico
Obligaciones*:	Mantener actualizado el sistema de control de incidencias, permisos médicos, faltas, prácticas externas y otros trámites del personal académico.
Nombre del Usuario 3*	Lic. Marisol Zamudio López
Cargo*:	Control de Asistencia Docente
Funciones*:	Llevar el control de asistencia y de las incidencias del personal académico
Obligaciones*:	Mantener actualizado el sistema de control de incidencias, permisos médicos, faltas, prácticas externas y otros trámites del personal académico. Resolver dudas de alumnos sobre localización de profesores.
Nombre del Usuario 4*	Lic. Selene Cruz Flores
Cargo*:	Vinculación Académica
Funciones*:	Ayudar a los profesores en trámites académicos varios
Obligaciones*:	Mantener actualizado el sistema de control de datos académicos sobre cambios de categoría, Apoyar para mantener actualizado el sistema de lista jerarquizada.

Nombre del Usuario 5*	C. María Soledad García Morales
Cargo*:	Control de Asistencia Docente
Funciones*:	Llevar el control de asistencia y de las incidencias del personal académico
Obligaciones*:	Mantener actualizado el sistema de control de incidencias, permisos médicos, faltas, prácticas externas y otros trámites del personal académico. Resolver dudas de alumnos sobre localización de profesores.

ANEXO 3. ANÁLISIS DE RIESGOS

ESCUELA NACIONAL COLEGIO DE CIENCIAS Y HUMANIDADES, PLANTEL NAUCALPAN		
Identificador único*	**menuce**	
Nombre del sistema*	**Menú de sistemas para tramites de Control Escolar**	
Riesgo*	**Impacto***	**Mitigación***
CONTENIDO	CONTENIDO	CONTENIDO
CONTENIDO	CONTENIDO	CONTENIDO
CONTENIDO	CONTENIDO	CONTENIDO
CONTENIDO	CONTENIDO	CONTENIDO
CONTENIDO	CONTENIDO	CONTENIDO
CONTENIDO	CONTENIDO	CONTENIDO
CONTENIDO	CONTENIDO	CONTENIDO

ESCUELA NACIONAL COLEGIO DE CIENCIAS Y HUMANIDADES, PLANTEL NAUCALPAN		
Identificador único*	**menusa**	
Nombre del sistema*	**Menú de sistemas para trámites de la Secretaría Académica**	
Riesgo*	**Impacto***	**Mitigación***
CONTENIDO	CONTENIDO	CONTENIDO
CONTENIDO	CONTENIDO	CONTENIDO
CONTENIDO	CONTENIDO	CONTENIDO
CONTENIDO	CONTENIDO	CONTENIDO
CONTENIDO	CONTENIDO	CONTENIDO
CONTENIDO	CONTENIDO	CONTENIDO

CONTENIDO	CONTENIDO	CONTENIDO

ANEXO 4. ANÁLISIS DE BRECHA

ESCUELA NACIONAL COLEGIO DE CIENCIAS Y HUMANIDADES, PLANTEL NAUCALPAN		
Identificador único*	**menuce**	
Nombre del sistema *	**Menú de sistemas para tramites de Control Escolar**	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
CONTENIDO	CONTENIDO	CONTENIDO
CONTENIDO	CONTENIDO	CONTENIDO
CONTENIDO	CONTENIDO	CONTENIDO
CONTENIDO	CONTENIDO	CONTENIDO

ESCUELA NACIONAL COLEGIO DE CIENCIAS Y HUMANIDADES, PLANTEL NAUCALPAN		
Identificador único*	**menusa**	
Nombre del sistema*	**Menú de sistemas para trámites de la Secretaría Académica**	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
CONTENIDO	CONTENIDO	CONTENIDO

CONTENIDO	CONTENIDO	CONTENIDO
CONTENIDO	CONTENIDO	CONTENIDO
CONTENIDO	CONTENIDO	CONTENIDO

ANEXO 5. PLAN DE TRABAJO

ESCUELA NACIONAL COLEGIO DE CIENCIAS Y HUMANIDADES, PLANTEL NAUCALPAN			
Identificador único*	**menuce**		
Nombre del sistema *	**Menú de sistemas para tramites de Control Escolar**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
CONTENIDO	CONTENIDO	CONTENIDO	CONTENIDO
CONTENIDO	CONTENIDO	CONTENIDO	CONTENIDO
CONTENIDO	CONTENIDO	CONTENIDO	CONTENIDO
ESCUELA NACIONAL COLEGIO DE CIENCIAS Y HUMANIDADES, PLANTEL NAUCALPAN			

Identificador único*	menusa		
Nombre del sistema *	Menú de sistemas para trámites de la Secretaría Académica		
Actividad*	Descripción*	Duración*	Cobertura*
CONTENIDO	CONTENIDO	CONTENIDO	CONTENIDO
CONTENIDO	CONTENIDO	CONTENIDO	CONTENIDO
CONTENIDO	CONTENIDO	CONTENIDO	CONTENIDO

ANEXO 6. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

I. TRANSFERENCIAS DE DATOS PERSONALES

ESCUELA NACIONAL COLEGIO DE CIENCIAS Y HUMANIDADES, PLANTEL NAUCALPAN	
Identificador único*	**menuce**
Nombre del sistema *	**Menú de sistemas para tramites de Control Escolar**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:[4]	No aplica
Transferencias mediante el traslado de soportes electrónicos:	No aplica
Transferencias mediante el traslado sobre redes electrónicas:	No aplica
ESCUELA NACIONAL COLEGIO DE CIENCIAS Y HUMANIDADES, PLANTEL NAUCALPAN	
Identificador único*	**menusa**
Nombre del sistema *	**Menú de sistemas para trámites de la Secretaría Académica**
Transferencias mediante el traslado de soportes físicos:[5]	No aplica

[4] **Ejemplo de medidas de seguridad para transmisiones mediante el traslado de soportes físicos:**

a) La transmisión de datos personales mediante el traslado de soportes físicos se lleva a cabo por la vía elegida de común acuerdo entre las partes: mensajero oficial, asistente secretarial, visita personal, servicio de mensajería externo, entre otras posibles. Se define un destinatario primario y otro secundario por si el mensajero no encuentra al primero.

b) El paquete con datos personales en soportes físicos viaja debidamente sellado, de forma tal que sea perceptible cualquier violación o apertura no autorizada del mismo.

c) La entrega del paquete se realiza sólo si el destinatario acredita su identidad. Para ello, el destinatario presenta una identificación oficial con fotografía y el mensajero recaba nombre, firma y un número de referencia que aparezca en tal identificación, además de la fecha de entrega.

d) El mensajero no entrega el paquete si el destinatario no puede acreditar su identidad. En este caso, el mensajero devuelve el paquete al transmisor.

e) El transmisor verifica que el mensajero haya entregado el paquete al destinatario. Si el transmisor detecta que dicho paquete fue entregado a otra persona, da inicio al proceso de atención de un incidente.

f) Se registran estas transmisiones en el Sistema de tratamiento de datos personales.

[5] **Ejemplo de medidas de seguridad para transmisiones mediante el traslado de soportes físicos:**

g) La transmisión de datos personales mediante el traslado de soportes físicos se lleva a cabo por la vía elegida de común acuerdo entre las partes: mensajero oficial, asistente secretarial, visita personal, servicio de mensajería externo, entre otras posibles. Se define un destinatario primario y otro secundario por si el mensajero no encuentra al primero.

h) El paquete con datos personales en soportes físicos viaja debidamente sellado, de forma tal que sea perceptible cualquier violación o apertura no autorizada del mismo.

i) La entrega del paquete se realiza sólo si el destinatario acredita su identidad. Para ello, el destinatario presenta una identificación oficial con fotografía y el mensajero recaba nombre, firma y un número de referencia que aparezca en tal identificación, además de la fecha de entrega.

j) El mensajero no entrega el paquete si el destinatario no puede acreditar su identidad. En este caso, el mensajero devuelve el paquete al transmisor.

k) El transmisor verifica que el mensajero haya entregado el paquete al destinatario. Si el transmisor detecta que dicho paquete fue entregado a otra persona, da inicio al proceso de atención de un incidente.

Transferencias mediante el traslado de soportes electrónicos:	No aplica
Transferencias mediante el traslado sobre redes electrónicas:	No aplica

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

1. Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.[6]
2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.[7]

II. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

a) Los datos que se registran en las bitácoras:[8] No se cuenta con bitácoras de ese tipo.

l) Se registran estas transmisiones en el Sistema de tratamiento de datos personales.

[6] Por ejemplo, se espera que precise si los formatos impresos, documentos, listados o expedientes están foliados, cosidos o engargolados, si los muebles o la estantería donde residen cuentan con cerradura, si existen mecanismos para regular la temperatura y la humedad, si existen sistemas de tratamiento de datos personales de detección y/o supresión de incendios, si cuenta con mecanismos para regular y mantener el suministro continuo de energía eléctrica, entre otras posibles medidas.

[7] En caso de ser muchas personas, se sugiere agregar el listado como Anexo al Documento de seguridad.

[8] Las áreas de informática y seguridad de la información han designado una persona que se encarga de realizar un análisis de las bitácoras generadas. Las siguientes características aplican al caso:

a) Se cuenta con la ayuda de una herramienta informática adquirida para tal propósito.
b) Cada semana se llevan a cabo análisis de bitácoras, pero no de todas ellas. Depende de la bitácora y de las amenazas detectadas en el entorno.
Ejemplo de medidas de seguridad aplicables a bitácoras para sistema de tratamiento de datos personales en soportes físicos: El responsable del sistema procurará un estricto control y registro de:
a) Las autorizaciones emitidas para facultar el acceso a un funcionario universitario a fin de que éste, en el ejercicio de sus funciones, pueda interactuar con uno o más de los sistemas de tratamiento de datos personales a su cargo.
b) La asignación, actualización y reemplazo de las llaves que entrega a los autorizados para que éstos puedan abrir el mecanismo de apertura de la puerta en la zona de acceso restringido. Las acciones que los autorizados llevan a cabo en el área de resguardo. Para ello, designa a un Encargado quien anota lo siguiente: Quién solicita el acceso, cuándo se lleva a cabo (fecha y hora de entrada y salida), la razón que lo motiva y número del expediente utilizado.
c) El préstamo de expedientes es asistido por un sistema de tratamiento de datos personales de cómputo que utiliza códigos de barras en los gafetes del personal autorizado y en los expedientes.
d) El sistema de tratamiento de datos personales de préstamo de expedientes genera una bitácora electrónica que se respalda diariamente en un servidor dentro del centro de cómputo que administra el área de informática. Su integridad se garantiza copiando dicha bitácora en un CD-R diariamente.
e) El Encargado del sistema de tratamiento de datos personales es la persona designada para analizar la bitácora cada mes mediante una herramienta adquirida para tal fin.
Ejemplo de medidas de seguridad aplicables a bitácoras para sistema de tratamiento de datos personales en soportes electrónicos:
I. El responsable del sistema de tratamiento de datos personales -en coordinación con las áreas de informática y seguridad de la información- lleva un estricto control y registro de:
a) Las bitácoras de eventos ocurridos a nivel *sistema de tratamiento de datos personales operativo* en los equipos (servidores, cortafuegos, almacenamiento masivo) que habilitan la operación del sistema de tratamiento de datos personales. Entre otras, se generan bitácoras para desempeño del servidor: intentos de acceso (exitosos y fallidos); accesos denegados a usuarios y terminales; uso de herramientas para administración del servidor, y fecha y hora de los eventos anteriores.
b) Las bitácoras de eventos generados a nivel *software aplicativo* del sistema de tratamiento de datos personales. Entre otras, se generan bitácoras para mensajes de error; apertura, modificación y cierre de archivos; violaciones de seguridad detectadas por el software aplicativo, y fecha y hora de estos eventos.
c) Las bitácoras de eventos relativos a las actividades de usuarios (capturistas, Encargados, el propio responsable y el administrador del servidor) en su interacción con el sistema de tratamiento de datos personales. Entre otras, se generan bitácoras para: archivos servicios y recursos utilizados; intentos de acceso (exitosos y fallidos); comandos y operaciones iniciadas, y fecha y hora de dichos eventos.

b) Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida;

c) Para soportes físicos: Número o clave del expediente utilizado, y

d) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.

2. Si las bitácoras están en soporte físico o en soporte electrónico;[9]

3. Lugar dónde almacena las bitácoras y por cuánto tiempo;

4. La manera en que asegura la integridad de las bitácoras, y

5. Respecto del análisis de las bitácoras:

a) Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza, y

b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.

III. REGISTRO DE INCIDENTES:

Describir el procedimiento de atención de incidentes que tiene implementado el área universitaria y especificar si lleva registro de los incidentes relativos a soportes físicos, como lo son la pérdida o alteración no autorizada de expedientes, y para el caso de soportes electrónicos, ofrecer detalles sobre el registro de incidentes en el cual consigne los procedimientos realizados para la recuperación de los datos o para permitir la disponibilidad del proceso.

El NOC de la UNAM (Network Operation Center) se encarga de la detección de incidentes, nos notifica vía correo electrónico y nos otorga una clave de acceso al incidente, solo se puede acceder a través de una IP previamente registrada en el NOC para el ingreso al sistema de seguimiento de incidentes. Una vez que es abierto, el sistema nos indica que tipo de incidente es, (Bots, generadores de Spam, zombies,etc.) y el número de la dirección IP que lo está causando. Se procede a dar solución al problema, que puede ser desde actualizar un antivirus hasta formateo completo del disco duro, luego se ingresa en el sistema del NOC la solución aplicada y se solicita el cierre del ticket de la incidencia. Desde el momento que el NOC levanta el ticket con el problema y lo envía, queda registrado el nombre de la persona que lo resolverá, en este caso, el Ing. Julio Eugenio Navarro Córdova.

1. Los datos que registra:

a) La persona que resolvió el incidente;

b) La metodología aplicada;[10]

d) El conjunto de bitácoras permite registrar, entre otros, los siguientes datos: Quién accede a los datos personales, desde dónde y con qué; accesos (intentos exitosos y fallidos) y salidas; propósito del acceso (sólo para modificaciones en el software aplicativo); operaciones llevadas a cabo; datos personales (registros y campos) utilizados de la base de datos, y fecha y hora de estos eventos.

e) Las bitácoras arriba mencionadas están todas en soportes electrónicos y se almacenan al menos por dos años en CD-R. Se tiene una copia en el centro de datos y otra se lleva a una bóveda bancaria subcontratada también para los respaldos.

II. La integridad de las bitácoras se garantiza copiándolas en un servidor del centro de datos el cual las graba en CD-R. Algunas se copian cada hora, otras a diario. La integridad de las copias se garantiza además con "resúmenes" creados por un algoritmo "digestor". Se cuenta con una herramienta de software que automatiza estas operaciones.

III. Se pueden realizar análisis focalizados a mayor profundidad en caso de presentarse un incidente que así lo requiera.

[9] En caso de tener las bitácoras en soportes físicos, debe señalar si en el futuro planea incorporarlas a soportes electrónicos.

[10] **Ejemplo de procedimiento en caso de presentarse un incidente:**

a) El Encargado elabora y entrega un informe al responsable a más tardar al día siguiente de haber ocurrido el incidente. Dicho informe precisa los soportes físicos o electrónicos afectados y, en su caso, los recuperados.

b) El incidente se registra en una hoja de cálculo anotando quién resolvió el incidente y los soportes dañados y recuperados. Dicha hoja está protegida con una contraseña de acceso. Su integridad se garantiza generando y almacenando un resumen creado por un algoritmo digestor en un servidor del centro de datos y respaldándola en un CD-R después de registrar un incidente.

c) En caso de robo o extravío de datos personales, el responsable del sistema de tratamiento de datos personales, al tener conocimiento del incidente, da vista al titular de la dependencia o entidad para su conocimiento y al titular del área jurídica o aquél que tenga facultades para presentar denuncias o querellas ante el Ministerio Público para que, en el ámbito de sus atribuciones, determine lo conducente.

d) A no más de 3 días naturales de haber ocurrido el incidente, el responsable del sistema de tratamiento de datos personales da aviso al público mediante un desplegado de prensa que difunde el hecho por diversos medios, según la gravedad del caso, a escala local, regional o nacional.

e) En caso de robo o extravío de datos personales, se alerta a los titulares de los datos afectados para que

c) Para soportes físicos: No aplica
d) Para soportes electrónicos: No aplica.

2. Si el registro está en soporte físico o en soporte electrónico: Electrónico;
3. Cómo asegura la integridad de dicho registro, y
4. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos: Está a cargo del NOC

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior (las instalaciones del área universitaria):

¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones? Por ejemplo, se espera que describa si cuenta con uno o más puntos de control de acceso y quienes los operan, si tiene vigilancia las 24 horas, si ha levantado bardas o cercas, si existe un sistema de tratamiento de datos personales de videovigilancia, entre otras posibles medidas.

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?
b) ¿Cómo las autentifica?
c) ¿Cómo les autoriza el acceso?

Los alumnos que ingresan presentan una credencial para su identificación, puede ser la credencial interna del CCH, la credencial de la UNAM o si ya son exalumnos o vienen a asesorías o a trámites extemporáneos, presentan su credencial electoral INE y se registran en una libreta en el módulo de vigilancia de la puerta principal del Plantel, para el caso de padres o madres de familia, se les pide credencial electoral y proveedores o trabajadores externos eventuales, también se les solicita INE y anotarse en la libreta, en caso de ser trabajos de semanas o meses, se le solicita a la compañía que le mande a vigilancia un memorándum indicando los nombres de las personas autorizadas para ingresar y sus vehículos.
La vigilancia en el módulo de seguridad esta a cargo por el personal de base con el apoyo de funcionarios al exterior desde las 6:30 am y hasta que se retira el último alumno del turno vespertino. Personal de base esta en vigilancia 24 horas al día.
Los accesos de personas ajenas son concedidos por funcionarios de acuerdo a visitas programadas previamente. El personal de base identifica por rostro a sus compañeros y a los profesores que trabajan en el plantel.

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema? Por ejemplo, se espera que precise el tipo de puertas y cerraduras instaladas, si tiene instalados controles biométricos, si administra la asignación de llaves y/o claves de acceso para abrir puertas y/o estantería, si cuenta con vigilancia las 24 horas, si hay un sistema de tratamiento de datos personales de videovigilancia, entre otras medidas.

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica? Solo tiene acceso el personal autorizado
2. ¿Cómo las autentifica? Solo tiene acceso el personal autorizado

tomen sus precauciones ante el posible uso ilegal de su información. Para tal efecto, el responsable del sistema de tratamiento de datos personales da aviso por escrito a dichos titulares, a más tardar cinco días naturales de haber ocurrido el incidente, recabando el acuse de recibo de esta notificación. Adicionalmente, se da aviso por correo electrónico o por teléfono.

3. ¿Cómo les autoriza el acceso? Se les da la llave o llaves para abrir las puertas.

En el caso de los accesos a los soportes físicos No Aplica
En el caso de los accesos a soportes electrónicos de los sistemas, están bajo resguardo, con puertas blindadas colocados en espacios que resguardan diferentes clases de personas, personal de base, profesores comisionados o funcionarios. De haber intentos de acceso a dichas áreas, el personal que labora ahí lo reporta directamente a el Departamento de Sistemas.
El SITE principal tiene una puerta blindada con chapa de seguridad y además una segunda puerta de cristal con llave tetra. La autorización se hace conforme lo determina la Secretaría General con base en las necesidades del personal y de los procesos relacionados con cada área, como mantenimiento y sustitución de equipo, configuración, ampliación de servicios de red o servicios nuevos.

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

En este apartado se deberá establecer un mecanismo o procedimiento institucional para la actualización de la información personal contenida en el sistema, en donde se establezca la frecuencia con la que se efectúa y la forma en que se está solicitando al titular acreditar de manera idónea sus requerimientos de rectificación de datos inexactos.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.

1. Modelo de control de acceso (alguno de los siguientes):

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)? Si
b) ¿Es discrecional (matriz de control de acceso)? Si
c) ¿Está basado en roles (perfiles) o grupos? Algunas
d) ¿Está basado en reglas? No.

2. Perfiles de usuario y contraseñas en el sistema operativo de red:
- **a)** ¿Cuenta con un sistema operativo de red instalado en sus equipos? Si
- **b)** ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas? No
- **c)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? Solo la contraseña

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:
- **a)** ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas? No
- **b)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? No

4. Administración de perfiles de usuario y contraseñas:
- **a)** ¿Quién da de alta nuevos perfiles? El jefe del Departamento de Sistemas
- **b)** ¿Quién autoriza la creación de nuevos perfiles? Los Secretarios de la Dirección
- **c)** ¿Se lleva registro de la creación de nuevos perfiles? Si

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema? Si

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento? Si

c) ¿Cómo se evita el acceso remoto no autorizado? Usando software de terceros. Deshabilitando el del sistema operativo.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos

a) Completos_X_, diferenciales ___ o incrementales___;

b) De forma automática ____ o Manual __X___,

c) Periodicidad con que los realiza: _a la conclusión de cada trámite_____

2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad: SE UTILIZAN DISCOS DUROS;[11]

3. Cómo y dónde archiva esos medios, y SE ARCHIVAN EN EL DEPARTAMENTO DE SISTEMAS

4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero). El jefe del Departamento de Sistemas.

IX. PLAN DE CONTINGENCIA

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.

2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.

3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:

a) El tipo de sitio (caliente, tibio o frío);[12]

b) Si el sitio es propio o subcontratado con un tercero;

c) Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio y

d) Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia.

El plan consiste en dar de alta un servicio en casa con el servidor o solicitar un espacio en el servidor de la DGCCH para virtualizar el servidor completo. El tipo de sitio es frio, El sitio es similar al propio, Los procedimientos consisten en llevar los respaldos del servidor a la DGCCH y que nos asignen personal

[11] Es deseable que precise si para almacenar dichos medios cuenta con al menos dos lugares distintos que cumplan con las condiciones de seguridad especificadas en el articulado del Capítulo V de los Lineamientos, conforme a la fracción III del Trigésimo primero de los Lineamientos; o bien, si utiliza un espacio externo seguro para guardar de manera sistemática dichos respaldos, según la fracción VIII del Trigésimo séptimo de tales Lineamientos.

[12] El tipo de sitio caliente, tibio o frío se refiere a la infraestructura, el equipo y el software disponibles en el sitio alterno; por lo que a mayor disponibilidad de dichos elementos resulta una menor demora para restablecer las operaciones de uno o más sistema de tratamiento de datos personales. Ejemplos de lo anterior son, en cuanto a **infraestructura:** aire acondicionado, cableado, suministro de energía eléctrica y enlaces de comunicaciones; en cuanto al **equipo**: servidores, almacenamiento y periféricos, y por lo que se refiere al **software:** sistema de tratamiento de datos personales operativos, manejadores de bases de datos y aplicaciones. Por lo tanto:

i) En un **sitio alterno caliente** se mantienen disponibles en todo momento la infraestructura, el equipo y el software; lo único que hace falta para iniciar operaciones son los datos y el personal. Este tipo de sitios alternos es el más costoso, pero supone tan solo unas cuantas horas para restaurar operaciones.

ii) El **sitio alterno tibio** cuenta con infraestructura no configurada y equipos equivalentes que pueden estar disponibles en pocas horas, pero no contienen software ni datos. Este tipo de sitios alternos es el punto medio en costo y tiempo para restaurar operaciones.

iii) El **sitio alterno frío** cuenta con un ambiente mínimo de infraestructura y no cuenta con el equipo. Este tipo de sitios alternos es el menos costoso, pero supone demora de algunos días para restablecer operaciones.

para virtualizar el servidor, posteriormente llamar a DGTIC para redirigir el sitio a otra dirección IP y termina con las pruebas de operación. Todo el proceso puede tardar de unas horas a 2 días.

Transferencias de datos personales

I. Resguardo de sistemas de tratamiento de datos personales con soportes físicos
II. Bitácoras para accesos y operación cotidiana
III. Registro de incidentes
IV. Acceso a las instalaciones
V. Actualización del sistema de tratamiento de datos personales
VI. Perfiles de usuario y contraseñas
VII. Procedimientos de respaldo y recuperación de datos
VIII. Plan de contingencia

Herramientas y recursos para monitoreo de la protección de datos personales

ESCUELA NACIONAL COLEGIO DE CIENCIAS Y HUMANIDADES, PLANTEL NAUCALPAN		
Identificador único*	**menuce**	
Nombre del sistema *	**Menú de sistemas para tramites de Control Escolar**	
Recurso*	**Descripción***	**Control***
Formulario de atención a alumnos	Cuando un trámite de control escolar está en línea, el alumno se puede comunicar con un equipo de gente asignada para atender problemas de ingreso o de otro tipo relacionados con el trámite para darle solución lo más pronto posible. Si deducen que puede ser un problema de un trámite en línea, lo reportan al Departamento de Sistemas o si es de otro tipo, lo canalizan con el área responsable de darle solución.	Cuanto un ingreso no es permitido y el alumno lo reporta, se le explica con más detalle la respuesta que el sistema le proporcionó, si no le quedó clara del porqué no se le permitió el ingreso o la condición que solicitaba o si se trata de un error se le da cause a la Secretaría de Administración Escolar y al Departamento de Sistemas. Licencia gratuita de Google.

ESCUELA NACIONAL COLEGIO DE CIENCIAS Y HUMANIDADES, PLANTEL NAUCALPAN		
Identificador único*	**menusa**	
Nombre del sistema *	**Menú de sistemas para trámites de la Secretaría Académica**	
Recurso*	**Descripción***	**Control***
Formulario de atención a profesores	Cuando un trámite del área Académica está en línea, el profesor se puede comunicar con un equipo de gente asignada para atender problemas relacionados con el trámite para darle solución lo más pronto posible. Si deducen que puede ser un problema de un trámite en línea, lo reportan al Departamento de Sistemas o si es de otro tipo, lo canalizan con el área responsable de darle solución	Cuando un profesor no puede emitir sus listas de asistencia o no puede solicitar grupos de dos áreas diferentes en un boletín o su nombre está mal escrito o se le asignaron menos grupos a los que tenía derecho o cualquier otro trámite vigente le genera dificultades, se le da solución por esta vía. Los mecanismos de seguridad implantada demuestran que mantienen el control de las aplicaciones. Licencia gratuita de Google.

Procedimiento para la revisión de las medidas de seguridad

ESCUELA NACIONAL COLEGIO DE CIENCIAS Y HUMANIDADES, PLANTEL NAUCALPAN		
Identificador único*	**menuce**	
Nombre del sistema*	**Menú de sistemas para tramites de Control Escolar**	
Medida de seguridad*	**Procedimiento***	**Responsable***
Comprobación de actualizaciones de paquetes de seguridad	Se revisan periódicamente los paquetes de seguridad disponibles para el sistema operativo del servidor, con la finalidad de evitar tener agujeros de seguridad en los servidores donde está funcionando el sistema	Responsable del procedimiento: Ing. Julio Eugenio Navarro Córdova, Jefe de Sistemas. Tiempo de ejecución en días: 1. Se hace en horarios que no afectan la operación.

Revisión de estabilidad del sistema	Se revisan de forma periódica las bitácoras de errores en la ejecución del código del sistema, así como las relacionadas a la ejecución de consultas MySQL que consuman mucho tiempo para su ejecución.	Responsable del procedimiento: Ing. Julio Eugenio Navarro Córdova, Jefe de Sistemas Tiempo de ejecución en días: 1. Se hace en horarios que no afectan la operación
ESCUELA NACIONAL COLEGIO DE CIENCIAS Y HUMANIDADES, PLANTEL NAUCALPAN		
Identificador único*	**menusa**	
Nombre del sistema*	**Menú de sistemas para trámites de la Secretaría Académica**	
Medida de seguridad*	**Procedimiento***	**Responsable***
Comprobación de actualizaciones de paquetes de seguridad	Se revisan periódicamente los paquetes de seguridad disponibles para el sistema operativo del servidor, con la finalidad de evitar tener agujeros de seguridad en los servidores donde está funcionando el sistema	Responsable del procedimiento: Ing. Julio Eugenio Navarro Córdova, Jefe de Sistemas. Tiempo de ejecución en días: 1. Se hace en horarios que no afectan la operación.
Revisión de estabilidad del sistema	Se revisan de forma periódica las bitácoras de errores en la ejecución del código del sistema, así como las relacionadas a la ejecución de consultas MySQL que consuman mucho tiempo para su ejecución.	Responsable del procedimiento: Ing. Julio Eugenio Navarro Córdova, Jefe de Sistemas Tiempo de ejecución en días: 1. Se hace en horarios que no afectan la operación

Resultados de la evaluación y pruebas a las medidas de seguridad

ESCUELA NACIONAL COLEGIO DE CIENCIAS Y HUMANIDADES, PLANTEL NAUCALPAN		
Identificador único*	**menuce**	
Nombre del sistema*	**Menú de sistemas para tramites de Control Escolar**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***

Comprobaciones de actualizaciones de paquetes de seguridad	Se han detectado paquetes de seguridad que han necesitado instalarse, el reinicio del servidor se hace en horas y días con baja afluencia de usuarios.	Responsable del procedimiento: Ing. Julio Eugenio Navarro Córdova, Jefe de Sistemas. Fecha de conclusión: aplicación continua.
Revisión de estabilidad del sistema	Se han llegado a detectar errores de ejecución en varios programas por diversas causas, todos y cada uno de ellos fue arreglado y regresado a la operación el trámite o servicio que estaba dando problemas. En ocasiones por cosas tan sutiles que fueron complicadas de detectar.	Responsable del procedimiento: Ing. Julio Eugenio Navarro Córdova, Jefe de Sistemas. Fecha de conclusión: aplicación continua.

ESCUELA NACIONAL COLEGIO DE CIENCIAS Y HUMANIDADES, PLANTEL NAUCALPAN		
Identificador único*	**menusa**	
Nombre del sistema*	**Menú de sistemas para trámites de la Secretaría Académica**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Comprobaciones de actualizaciones de paquetes de seguridad	Se han detectado paquetes de seguridad que han necesitado instalarse, el reinicio del servidor se hace en horas y días con baja afluencia de usuarios.	Responsable del procedimiento: Ing. Julio Eugenio Navarro Córdova, Jefe de Sistemas. Fecha de conclusión: aplicación continua.
Revisión de estabilidad del sistema	Se han llegado a detectar errores de ejecución en varios programas por diversas causas, todos y cada uno de ellos fue arreglado y regresado a la operación el trámite o servicio que estaba dando problemas. En ocasiones por cosas tan sutiles que fueron complicadas de detectar.	Responsable del procedimiento: Ing. Julio Eugenio Navarro Córdova, Jefe de Sistemas. Fecha de conclusión: aplicación continua.

ANEXO 7. PROGRAMA ESPECIFICO DE CAPACITACIÓN

Programa de capacitación a los responsables de seguridad de datos personales

ESCUELA NACIONAL COLEGIO DE CIENCIAS Y HUMANIDADES, PLANTEL NAUCALPAN			
Identificador único*	**menuce**		
Nombre del sistema*	**Menú de sistemas de tramites de Control Escolar**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Capacitación personalizada para los nuevos elementos de la Secretaría de Administración Escolar	Se aborda cada aspecto del procedimiento para usar cada sistema de trámites, pantalla por pantalla y dato por dato, previo al inicio del trámite y hasta concluirlo al sacar las listas de comprobación. Se les instruye con detalle la importancia de no divulgar datos personales ni académicos de la población estudiantil o del profesorado.	Un año escolar, es decir, dos semestres, ya que aunque tienen similitudes, hay procesos que solo se realizan una vez al año, la fecha de inicio es con el ingreso del personal y termina cuando recorre todo el conjunto de trámites que forzosamente se realizan en ese periodo de tiempo.	Capacitación a cargo de la C.P. María Guadalupe Sánchez Chávez, Secretaria de Administración Escolar. Solo para personal del área de control escolar. Es vigente durante todo el tiempo de su estancia en ese departamento. Solo si hay modificaciones a los procedimientos, datos o secuencias del trámite que requieran de cambios sustanciales, se realiza una nueva capacitación

ESCUELA NACIONAL COLEGIO DE CIENCIAS Y HUMANIDADES, PLANTEL NAUCALPAN			
Identificador único*	**menusa**		
Nombre del sistema*	**Menú de sistemas para trámites de la Secretaría Académica**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Capacitación personalizada para los nuevos elementos	Se aborda cada aspecto del procedimiento para	Un año escolar, es decir, dos semestres, ya que	Capacitación a cargo del Ing. Damián Feltrín

de la Secretaría Académica	usar cada sistema de trámites, pantalla por pantalla y dato por dato, previo al inicio del trámite y hasta concluirlo. Se les instruye con detalle la importancia de no divulgar datos personales del profesorado o del alumnado, a través de las listas de asistencia, que debido a la pandemia tuvieron que incluir correos electrónicos, números telefónicos y para las listas de exámenes extraordinarios, además fotografías.	aunque tienen similitudes, hay procesos que solo se realizan una vez al año, la fecha de inicio es con el ingreso del personal y termina cuando recorre todo el conjunto de trámites que forzosamente se realizan en ese periodo de tiempo.	Rodríguez, Secretario Académico. Solo para personal del área de control escolar. Es vigente durante todo el tiempo de su estancia en ese departamento. Solo si hay modificaciones a los procedimientos, datos o secuencias del trámite que requieran de cambios sustanciales, se realiza una nueva capacitación

Programa de difusión de la protección a los datos personales

ESCUELA NACIONAL COLEGIO DE CIENCIAS Y HUMANIDADES, PLANTEL NAUCALPAN			
Identificador único*	**menuce**		
Nombre del sistema*	**Menú de sistemas de tramites de Control Escolar**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Incluido dentro del programa de capacitación para el uso correcto del sistema	Generalidades sobre la protección de datos personales y las implicaciones legales. El objetivo es impedir la difusión de datos personales	Dura un año, lo mismo que la capacitación, inicia de manera individualizadas cuando ingresa nuevo personal	Se menciona la existencia de la ley de protección de datos personales y los problemas legales que se pueden presentar si hay filtraciones de información Solo si hay modificaciones importantes a la ley, que

	Se imparte de manera presencial		haya nuevos datos personales que manejar se difunde dicha actualización

ESCUELA NACIONAL COLEGIO DE CIENCIAS Y HUMANIDADES, PLANTEL NAUCALPAN			
Identificador único*	**menusa**		
Nombre del sistema*	**Menú de sistemas para trámites de la Secretaría Académica**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Incluido dentro del programa de capacitación para el uso correcto del sistema	Generalidades sobre la protección de datos personales y las implicaciones legales. El objetivo es impedir la difusión de datos personales Se imparte de manera presencial	Dura un año, lo mismo que la capacitación, inicia de manera individualizadas cuando ingresa nuevo personal	Se menciona la existencia de la ley de protección de datos personales y los problemas legales que se pueden presentar si hay filtraciones de información Solo si hay modificaciones importantes a la ley, que haya nuevos datos personales que manejar se difunde dicha actualización

ANEXO 8. MEJORA CONTINUA

Actualización y mantenimiento de sistemas de información

ESCUELA NACIONAL COLEGIO DE CIENCIAS Y HUMANIDADES, PLANTEL NAUCALPAN			
Identificador único*	**menuce**		
Nombre del sistema*	**Menú de sistemas de tramites de Control Escolar**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización de las necesidades de cada trámite	Las necesidades de la información recopilada cambian de acuerdo a varios factores, entre ellos, normatividad, adición de datos, modificación de datos, adición de funciones o modificación de funciones. Por ejemplo en la Pandemia, se requirió la recopilación de comprobantes escaneados porque no era posible la entrega personal en papel. El objetivo fue evitar contagios de Sarscov2 Se impactó el tiempo para completar el trámite de inscripción o reinscripción.	La actualización se realiza cuando es requerida, la duración depende de la magnitud de la actualización.	Se solucionan necesidades para cada trámite, por ejemplo, durante la pandemia se requirieron más números telefónicos y nombre del padre o tutor legal de los alumnos, así que se modifica el sistema para incluirlos. Se le da solución total.

ESCUELA NACIONAL COLEGIO DE CIENCIAS Y HUMANIDADES, PLANTEL NAUCALPAN			
Identificador único*	**menusa**		
Nombre del sistema*	**Menú de sistemas para trámites de la Secretaría Académica**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización de las necesidades de cada trámite	Las necesidades de la información recopilada cambian de acuerdo a varios factores, entre ellos, normatividad, adición de datos, modificación de datos, adición de funciones o modificación de funciones. En la Pandemia, se requirió la recopilación de correos electrónicos a los estudiantes y a los profesores para que se pudieran comunicar y para las altas en las aulas virtuales. El objetivo fue evitar contagios de Sarscov2 Se impactó el tiempo para habilitar en un aula virtual a un alumno.	La actualización se realiza cuando es requerida, la duración depende de la magnitud de la actualización.	Se solucionan necesidades para cada trámite, por ejemplo, durante la pandemia se requirieron modificaciones a los trámites como listas de grupo, que además del número de cuenta y el nombre debían tener el correo electrónico y los número de teléfono de los estudiantes, así que se modifica el sistema para incluirlos. Se le da solución total.

Actualización y mantenimiento de equipo de cómputo

ESCUELA NACIONAL COLEGIO DE CIENCIAS Y HUMANIDADES, PLANTEL NAUCALPAN			
Identificador único*	**menuce**		
Nombre del sistema*	**Menú de sistemas de tramites de Control Escolar**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Sustitución de equipo de cómputo.	Cuando la operación de los sistemas de trámites se ve comprometida por la obsolescencia del equipo, es sustituido mientras el presupuesto de la institución lo permita. El objetivo es mantener la correcta operación de trámites esolares. El impacto es evidente cuando se reducen los tiempos de espera para la captura de datos se hace más eficiente el servicio al alumnado.	Generalmente lleva 1 dia. Se lleva a cabo cuando no hay trámite en operación.	Esto resuelve problemas de velocidad, compatibilidad de aplicaciones, como máquinas virtuales o versiones de navegadores demasiado exigentes en características de hardware o que no funcionan bien en sistemas operativos antiguos.
Reparación de equipo de cómputo.	Si el equipo presenta anomalías en su funcionamiento, se usa otro en sustitución de funciones y se traslada a el Departamento de Sistemas, ahí es reparado, se le da limpieza, se sustituyen piezas dañadas y se actualizan parches	Generalmente lleva 1 dia a menos que sean necesarias refacciones, en ese caso puede tardar de 1 a dos semanas. Se lleva a cabo haya o no trámite en operación.	Esto resuelve problemas de funcionamiento anormal.

	de seguridad o antivirus El objetivo es mantener la correcta operación de trámites esolares. El impacto es mínimo pues las otras máquinas tienen capacidades similares y se sustituye de inmediato.		

ESCUELA NACIONAL COLEGIO DE CIENCIAS Y HUMANIDADES, PLANTEL NAUCALPAN			
Identificador único*	**menusa**		
Nombre del sistema*	**Menú de sistemas para trámites de la Secretaría Académica**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Sustitución de equipo de cómputo.	Cuando la operación de los sistemas de trámites se ve comprometida por la obsolescencia del equipo, es sustituido mientras el presupuesto de la institución lo permita. El objetivo es mantener la correcta operación de trámites esolares. El impacto es evidente cuando se reducen los tiempos de espera para la captura de datos se hace más	Generalmente lleva 1 dia. Se lleva a cabo cuando no hay trámite en operación.	Esto resuelve problemas de velocidad, compatibilidad de aplicaciones, como máquinas virtuales o versiones de navegadores demasiado exigentes en características de hardware o que no funcionan bien en sistemas operativos antiguos.

	eficiente el servicio al profesorado.		
Reparación de equipo de cómputo.	Si el equipo presenta anomalías en su funcionamiento, se usa otro en sustitución de funciones y se traslada a el Departamento de Sistemas, ahí es reparado, se le da limpieza, se sustituyen piezas dañadas y se actualizan parches de seguridad o antivirus El objetivo es mantener la correcta operación de trámites esolares. El impacto es mínimo pues las otras máquinas tienen capacidades similares y se sustituye de inmediato.	Generalmente lleva 1 dia a menos que sean necesarias refacciones, en ese caso puede tardar de 1 a dos semanas. Se lleva a cabo haya o no trámite en operación.	Esto resuelve problemas de funcionamiento anormal.

Procesos para la conservación, preservación y respaldos de información

ESCUELA NACIONAL COLEGIO DE CIENCIAS Y HUMANIDADES, PLANTEL NAUCALPAN		
Identificador único*	**Menuce**	
Nombre del sistema*	**Menú de sistemas de tramites de Control Escolar**	
Proceso*	**Descripción***	**Responsable***

Tanto los sistemas como las bases de datos se respaldan en su totalidad al final de cada semestre, cuando han terminado todos los trámites.	Se hace una copia completa de los sistemas depositados en el servidor, además se saca un respaldo de la base de datos. El respaldo se copia a un disco duro externo.	Nombre del responsable del proceso: Ing. Julio Eugenio Navarro Córdova Tiempo máximo de ejecución en días: 1
Se hace un respaldo incremental diario de todos los sistemas diariamente	El respaldo se realiza a las 3 am, se usa la versión gratuita del software EASUS backup en un disco duro conectado al servidor.	Nombre del responsable del proceso: Ing. Julio Eugenio Navarro Córdova Tiempo de ejecución: 2 horas.

ESCUELA NACIONAL COLEGIO DE CIENCIAS Y HUMANIDADES, PLANTEL NAUCALPAN		
Identificador único*	**Menusa**	
Nombre del sistema*	**Menú de sistemas para trámites de la Secretaría Académica**	
Proceso*	**Descripción***	**Responsable***
Tanto los sistemas como las bases de datos se respaldan en su totalidad al final de cada semestre, cuando han terminado todos los trámites.	Se hace una copia completa de los sistemas depositados en el servidor, además se saca un respaldo de la base de datos. El respaldo se copia a un disco duro externo.	Nombre del responsable del proceso: Ing. Julio Eugenio Navarro Córdova Tiempo máximo de ejecución en días: 1
Se hace un respaldo incremental diario de todos los sistemas diariamente	El respaldo se realiza a las 3 am, se usa la versión gratuita del software EASUS backup en un disco duro conectado al servidor.	Nombre del responsable del proceso: Ing. Julio Eugenio Navarro Córdova Tiempo de ejecución: 2 horas.

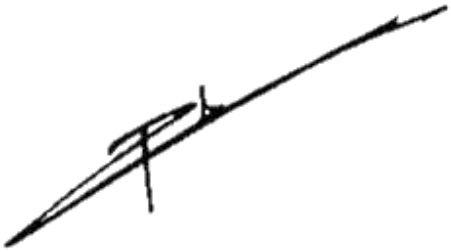
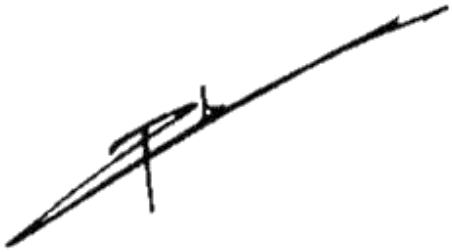
Procesos de borrado seguro y disposición final de equipos y componentes informáticos

ESCUELA NACIONAL COLEGIO DE CIENCIAS Y HUMANIDADES, PLANTEL NAUCALPAN	
Identificador único*	**Menuce**

Nombre del sistema*	**Menú de sistemas para trámites de la Secretaría Académica**	
Proceso*	**Descripción***	**Responsable***
Cuando presentan del documento de baja de equipo, el jefe del Departamento de Sistemas tiene que firmar de conformidad, para que proceda la baja, así que el equipo se traslada para el procedimiento de borrado seguro.	Usando el software libre Darik's Boot And Nuke o CBL Data Shredder se inicia desde una memoria USB y se procede al borrado seguro del disco duro del equipo.	Nombre del responsable del proceso: Ing. Julio Eugenio Navarro Córdova Tiempo máximo de ejecución en días: 1

ESCUELA NACIONAL COLEGIO DE CIENCIAS Y HUMANIDADES, PLANTEL NAUCALPAN		
Identificador único*	**Menusa**	
Nombre del sistema*	**Menú de sistemas para trámites de la Secretaría Académica**	
Proceso*	**Descripción***	**Responsable***
Cuando presentan del documento de baja de equipo, el jefe del Departamento de Sistemas tiene que firmar de conformidad, para que proceda la baja, así que el equipo se traslada para el procedimiento de borrado seguro.	Usando el software libre Darik's Boot And Nuke o CBL Data Shredder se inicia desde una memoria USB y se procede al borrado seguro del disco duro del equipo.	Nombre del responsable del proceso: Ing. Julio Eugenio Navarro Córdova Tiempo máximo de ejecución en días: 1

ANEXO 9. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

		Nombre y firma de quienes revisaron el presente documento:
Responsable del desarrollo:	Ing. Julio Eugenio Navarro Cordova Puesto: Jefe del Departamento de Sistemas CCHN Tel: 5544535372 Correo: julio.navarro@cch.unam.mx	 Ing. Julio Eugenio Navarro Cordova
Revisó:	Mtro. Keshava Rolando Quintanar Cano Puesto: Dir. CCH Naucalpan Tel: 53600323 Ext. 202 Correo: keshava.quintanar@cch.unam.mx	 Mtro. Keshava Rolando Quintanar Cano
Autorizó:	Mtro. Keshava Rolando Quintanar Cano Puesto: Dir. CCH Naucalpan Tel: 53600323 Ext. 202 Correo: keshava.quintanar@cch.unam.mx	 Mtro. Keshava Rolando Quintanar Cano
Fecha de aprobación:	3 de mayo de 2022	
Fecha de actualización:	5 de mayo de 2022	

COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/525/2022

Visto el expediente relativo a la clasificación de reserva total de una parte de la información, para la elaboración de la versión pública , que someten el **Instituto de Matemáticas**, el **Instituto de Fisiología Celular**, la **Dirección General de la Escuela Nacional Colegio de Ciencias y Humanidades**, la **Escuela Nacional Colegio de Ciencias y Humanidades Planteles Azcapotzalco, Vallejo, Naucalpan, Oriente y Sur**, la **Facultad de Filosofía y Letras**, la **Coordinación de Difusión Cultural**, la **Dirección General de Estudios de Legislación Universitaria**, el **Centro Universitario de Teatro**, la **Dirección General de Radio UNAM**, la **Secretaría de Desarrollo Institucional**, el **Instituto de Física**, el **Consejo Académico del Área de las Ciencias Biológicas, Químicas y de la Salud**, el **Comité de Análisis para las Intervenciones Urbanas, Arquitectónicas y de las Ingenierías**, el **Museo Universitario del Chopo**, la **Dirección General de Música**, la **Dirección de Danza**, el **Centro de Investigaciones en Geografía Ambiental, Campus Morelia**, el **Museo Universitario de Arte Contemporáneo**, la **Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género**, el **Instituto de Química**, la **Dirección de Literatura y Fomento a la Lectura**, la **Dirección General de Servicios Administrativos**, la **Dirección de Teatro UNAM**, el **Centro de Ciencias Genómicas**, la **Facultad de Artes y Diseño**, la **Dirección General de Televisión Universitaria**, el **Centro Cultural Universitario Tlatelolco**, la **Dirección General de Orientación y Atención Educativa**, el **Consejo Académico del Área de las Ciencias Sociales**, la **Escuela Nacional de Estudios Superiores, Unidad Mérida**, el **Instituto de Ecología**, la **Dirección General de Cooperación e Internacionalización**, el **Instituto de Investigaciones Biomédicas**, la **Casa del Lago "Mtro. Juan José Arreola"**, la **Coordinación para la Igualdad de Género**, la **Dirección General de la Escuela Nacional Preparatoria** y la **Escuela Nacional Preparatoria, Planteles 3 "Justo Sierra"** y **4 "Vidal Castañeda y Nájera"** y la **Dirección General del Deporte Universitario**, en relación con sus respectivos **Documentos de Seguridad**, se procede a dictar la presente resolución con base en los siguientes:

A N T E C E D E N T E S

I. Con fecha 26 de enero de 2017 se publicó en el Diario Oficial de la Federación el Decreto por el que se expide la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, reglamentaria de los artículos 6o., Base A y 16, segundo párrafo, de la Constitución Política de los Estados Unidos Mexicanos, en materia de protección de datos personales en posesión de sujetos obligados.

II. Mediante Acuerdo **ACT-PUB/19/12/2017.10**, de fecha 19 de diciembre de 2017, publicado en el Diario Oficial de la Federación con fecha 26 de enero de 2018, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales aprobó los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

III. A través del Acuerdo **ACT-PUB/11/11/2020.05**, de fecha 11 de noviembre de 2020, publicado en el Diario Oficial de la Federación con fecha 25 de noviembre de 2020, dicho Órgano Garante aprobó la adición de un Título Décimo a los Lineamientos Generales de Protección de Datos Personales para el Sector Público, a fin de establecer las disposiciones generales que permitirán desarrollar el procedimiento de diseño y aplicación del sistema y procedimiento para llevar a cabo la evaluación sobre el desempeño de los responsables

respecto al cumplimiento de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y demás disposiciones que resulten aplicables en la materia.

IV. Por Acuerdo **ACT-PUB/17/11/2021.05**, de fecha 17 de noviembre de 2021, publicado en el Diario Oficial de la Federación con fecha 26 de noviembre de 2021, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales aprobó los "Instrumentos Técnicos que refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en materia de evaluación del desempeño de los sujetos obligados del sector público federal en el cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados".

V. Los artículos 247 y 248 de Lineamientos Generales de Protección de Datos Personales para el Sector Público, así como las reglas Décima Tercera y Décima Cuarta del apartado "V. Reglas de Generales de Evaluación" del Documento Técnico de Evaluación y sus anexos de los Instrumentos Técnicos que refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en materia de Evaluación del Desempeño de los Sujetos Obligados del Sector Público Federal en el Cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, establecen que la información y documentos que se pongan a disposición de los titulares de datos personales y del Instituto, deberán ser revisados por el responsable a fin de verificar que no contengan información confidencial o reservada y, de ser el caso, deberá publicarse la versión pública de dicha documentación.

Por otra parte, en el apartado "VI. Metodología, criterios, formatos e indicadores en materia de evaluación del desempeño de los responsables respecto al cumplimiento de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y demás disposiciones que resulten aplicables en la materia", Capítulo II. Criterios y formatos, **Vertiente 2**: Deberes, **Variable 2.1** Deber de seguridad, se establece que el responsable, por ningún motivo, debe publicar el documento de seguridad de manera íntegra, por lo que deberá poner a disposición la versión pública del mismo, en la cual se deberá proteger la información relativa al plan de trabajo, el análisis de riesgo y el análisis de brecha.

VI. En términos de los artículos 106, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública; 98 fracción II de la Ley Federal de Transparencia y Acceso a la Información Pública, así como 34, fracción II del Reglamento de Transparencia y Acceso a la Información Púbica de la Universidad Nacional Autónoma de México, la clasificación de la información será procedente cuando, entre otros supuestos, se determiné mediante una resolución de autoridad competente.

VII. La Presidencia del Comité de Transparencia recibió diversos oficios, mediante los cuales las Áreas Universitarias sometieron a consideración de este Cuerpo Colegiado, la clasificación parcial de información reservada de sus Documentos de Seguridad, mismos que se enlistan a continuación:

COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/525/2022

Oficio	Área Universitaria	Fecha de presentación
IMAT/D048/2022	Instituto de Matemáticas	15/08/2022
IFCE/DIR/184/2022	Instituto de Fisiología Celular	
CCHDG/DIR/145/08/2022	Dirección General de la Escuela Nacional Colegio de Ciencias y Humanidades	
CCHA/DIR/415/VIII/2022	Plantel Azcapotzalco de la Escuela Nacional Colegio de Ciencias y Humanidades	
CCHN.91.20/580/2022	Plantel Naucalpan de la Escuela Nacional Colegio de Ciencias y Humanidades	
CCHO/DIR/445/2022	Plantel Oriente de la Escuela Nacional Colegio de Ciencias y Humanidades	
OF/CCHS/DIR/160/2022	Plantel Sur de la Escuela Nacional Colegio de Ciencias y Humanidades	
CCHV/OJ/135/2022	Plantel Vallejo de la Escuela Nacional Colegio de Ciencias y Humanidades	
FFLE/CP/034/2022	Facultad de Filosofía y Letras	
CODC/182/2022	Coordinación de Difusión Cultural	
DGEL/JT/3454/2022	Dirección General de Estudios de Legislación Universitaria	16/08/2022
CUTE/DIR/66/2022	Centro Universitario de Teatro	
DGRU/115/2022	Dirección General de Radio UNAM	
SDI/116/2022	Secretaría de Desarrollo Institucional	17/08/2022
IFIS/D/221/2022 IFIS/D/223/2022	Instituto de Física	
CJBS/112/22	Consejo Académico del Área de las Ciencias Biológicas, Químicas y de la Salud	
CAI/063/2022	Comité de Análisis para las Intervenciones Urbanas, Arquitectónicas y de las Ingenierías	
DIR/MUCH/0160/2022	Museo Universitario del Chopo	
DGMU/114/08/2022	Dirección General de Música	
DDAN/0356/2022	Dirección de Danza	
CIGA/D/133/2022	Centro de Investigaciones en Geografía Ambiental, Campus Morelia	
DiGAV/D/2315/2022	Museo Universitario de Arte Contemporáneo	
DDUIAVG/T/2427/2022	Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género	
IQUI 427/2022	Instituto de Química	
DLFL/208/2022	Dirección de Literatura y Fomento a la	

	Lectura	
DGSA/0381/2022	Dirección General de Servicios Administrativos	
DTEA/107/2022	Dirección de Teatro UNAM	
ENP3/DIRE/239/2022	Escuela Nacional Preparatoria, Plantel 3	
CCG/DIR/293/2022	Centro de Ciencias Genómicas	
FAD/DIR/445/2022	Facultad de Artes y Diseño	
DGTV/DG/197/2022	Dirección General de Televisión Universitaria	
CCUT/139/2022	Centro Cultural Universitario Tlatelolco	
ENPDG/314/2022	Dirección General de la Escuela Nacional Preparatoria	
DGOAE/416/2022	Dirección General de Orientación y Atención Educativa	
CJCS/124/2022	Consejo Académico del Área de las Ciencias Sociales	
ENES/MID/OFJ/199/2022	Escuela Nacional de Estudios Superiores, Unidad Mérida	
IECO/DIR/327/2022	Instituto de Ecología	
DGECI/DG/0869/2022	Dirección General de Cooperación e Internacionalización	
IIB/DIR/309/2022	Instituto de Investigaciones Biomédicas	
DCLA/Of.096/2022	Casa del Lago "Mtro Juan José Arreola"	
ENP4/DIR/108/2022	Escuela Nacional Preparatoria, Plantel 4	
CIG/C/320/2022	Coordinación para la Igualdad de Género	
DGDU/CJ/930/2022	Dirección General del Deporte Universitario	

En dichos oficios, las Áreas Universitarias informaron lo siguiente:

> *"Los Instrumentos Técnicos a los que se refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público en materia de evaluación del desempeño de los sujetos obligados del sector público federal en el cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados[1]; exige elaborar versión pública del documento de seguridad de esta área universitaria.*
>
> *Una vez analizada la información que se solicitó en el primer punto del 'Documento de seguridad', se observó que la misma se ajusta al supuesto de reserva contemplado en los artículos 113, fracción VII de la Ley General de Transparencia y*

[1] *DOF: 26 de noviembre de 2021*

Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, ya que su divulgación obstruiría el deber de esta Universidad de establecer y mantener las medidas de seguridad técnica, administrativa y física de los datos personales que los titulares confían a esta institución.

En este contexto, la información puede ser clasificada como reservada en términos de los artículos 106, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública (Ley General) y 98 fracción II de la Ley Federal de Transparencia y Acceso a la Información Pública (Ley Federal), en relación con los artículos 247 y 248 de Lineamientos Generales de Protección de Datos Personales para el Sector Público y las reglas generales de evaluación Décima Tercera y Décima Cuarta del apartado V. Reglas de Generales de Evaluación, del Documento Técnico de Evaluación y sus anexos de los Instrumentos Técnicos que refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en materia de Evaluación del Desempeño de los Sujetos Obligados del Sector Público Federal en el Cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

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

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

Los fundamentos y motivos se exponen a continuación:

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

- *Divulgar el análisis de riesgo, el análisis de brecha ... y el plan de trabajo ... evidencian los nuevos controles que estamos pendientes de implementar, describen la forma en cómo almacenamos técnicamente los datos personales, cómo protegemos los sistemas automatizados de información, qué medidas de seguridad administrativas, físicas y técnicas planemos establecer de manera gradual y de conformidad con las prioridades y presupuestos otorgado.*

- *En este sentido la revelación de la información que obra el análisis de riesgo, el análisis de brecha, las políticas de respaldo y el plan de trabajo de esta área revela y hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales que obran en nuestros archivos y dejaría imposibilitada a esta área para reaccionar ante posibles amenazas.*

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

En esa inteligencia, el dar a conocer el análisis de riesgo, el análisis de brecha y el plan de trabajo de esta área universitaria, no podrían prevenirse actos ilícitos que pudieran realizarse en contra de los sistemas de información y tratamiento de datos personales, así como en contra de los activos e infraestructura crítica de esta

dependencia; por lo que es posible advertir que algunas de las posibles consecuencias de divulgar dicha información podrían derivar en la comisión de diversos delitos tipificados en el Código Penal Federal, como accesos no autorizados a los sistemas, robos de información, suplantación de identidades, entre otros. Es decir, se advierte que la negativa de acceso a la información se motiva en evitar o prevenir la comisión del delito al vulnerar las medidas de seguridad establecidas por esta Área Universitaria, con relación al cumplimiento de los principios de protección de datos personales previsto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

En tal sentido, proteger la información de los documentos relativos al análisis de riesgo, al análisis de brecha y al plan de trabajo de esta área se adecua al principio de proporcionalidad porque se justifica negar su divulgación, toda vez que la pretensión de fondo que persigue la reserva de la información consiste en prevenir las conductas antijurídicas tipificadas, aunado a que la restricción es temporal, hasta en tanto las medidas tomadas caduquen; de igual manera, con la no divulgación de la información se contribuye a garantizar la protección de los datos personales de no solo la comunidad universitaria sino de cualquiera que ponga la confianza en esta Universidad para resguardar sus datos personales.

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

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

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

C O N S I D E R A C I O N E S

PRIMERA. Con fundamento en lo dispuesto por los artículos 10 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, así como 8, fracción VI del Reglamento de Responsabilidades Administrativas de las y los Funcionarios y Empleados de la Universidad Nacional Autónoma de México, este Órgano Colegiado rige su funcionamiento, entre otros, bajo los principios de imparcialidad, certeza, legalidad, objetividad y profesionalismo. Por ello, al ser un asunto propuesto, entre otras Áreas Universitarias, por la **Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género**, así como por la **Dirección General de Estudios de Legislación Universitaria**, dependiente de la Oficina de la Abogacía General, en este acto, la Titular de la Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género e integrante de este Cuerpo Colegiado, Guadalupe Barrena Nájera, el Abogado General y Presidente del Comité de Transparencia, Alfredo Sánchez Castañeda, así como el Director General de Asuntos Jurídicos y

Secretario Técnico de este Comité, Lic. Jorge Barrera Gutiérrez, formalmente se excusan de conocer del caso, para no afectar la imparcialidad del mismo.

SEGUNDA. De conformidad con lo dispuesto en los artículos 1, 10 y 15, fracción X del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, el Comité de Transparencia de la Universidad Nacional Autónoma de México es competente para analizar la clasificación de reserva total de una parte de la información, para la elaboración de la versión pública de los Documentos de Seguridad, propuesta por el **Instituto de Matemáticas**, el **Instituto de Fisiología Celular**, la **Dirección General de la Escuela Nacional Colegio de Ciencias y Humanidades**, la **Escuela Nacional Colegio de Ciencias y Humanidades Planteles Azcapotzalco, Vallejo, Naucalpan, Oriente y Sur**, la **Facultad de Filosofía y Letras**, la **Coordinación de Difusión Cultural**, la **Dirección General de Estudios de Legislación Universitaria**, el **Centro Universitario de Teatro**, la **Dirección General de Radio UNAM**, la **Secretaría de Desarrollo Institucional**, el **Instituto de Física**, el **Consejo Académico del Área de las Ciencias Biológicas, Químicas y de la Salud**, el **Comité de Análisis para las Intervenciones Urbanas, Arquitectónicas y de las Ingenierías**, el **Museo Universitario del Chopo**, la **Dirección General de Música**, la **Dirección de Danza**, el **Centro de Investigaciones en Geografía Ambiental, Campus Morelia**, el **Museo Universitario de Arte Contemporáneo**, la **Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género**, el **Instituto de Química**, la **Dirección de Literatura y Fomento a la Lectura**, la **Dirección General de Servicios Administrativos**, la **Dirección de Teatro UNAM**, el **Centro de Ciencias Genómicas**, la **Facultad de Artes y Diseño**, la **Dirección General de Televisión Universitaria**, el **Centro Cultural Universitario Tlatelolco**, la **Dirección General de Orientación y Atención Educativa**, el **Consejo Académico del Área de las Ciencias Sociales**, la **Escuela Nacional de Estudios Superiores, Unidad Mérida**, el **Instituto de Ecología**, la **Dirección General de Cooperación e Internacionalización**, el **Instituto de Investigaciones Biomédicas**, la **Casa del Lago "Mtro. Juan José Arreola"**, la **Coordinación para la Igualdad de Género**, la **Dirección General de la Escuela Nacional Preparatoria** y la **Escuela Nacional Preparatoria, Planteles 3 "Justo Sierra" y 4 "Vidal Castañeda y Nájera"** y la **Dirección General del Deporte Universitario**, y determinar, en consecuencia, si la confirma, modifica o revoca.

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

En tal virtud, el **Instituto de Matemáticas**, el **Instituto de Fisiología Celular**, la **Dirección General de la Escuela Nacional Colegio de Ciencias y Humanidades**, la **Escuela Nacional Colegio de Ciencias y Humanidades Planteles Azcapotzalco, Vallejo, Naucalpan, Oriente y Sur**, la **Facultad de Filosofía y Letras**, la **Coordinación de Difusión Cultural**, la **Dirección General de Estudios de Legislación Universitaria**, el **Centro Universitario de Teatro**, la **Dirección General de Radio UNAM**, la **Secretaría de Desarrollo Institucional**, el **Instituto de**

Física, el **Consejo Académico del Área de las Ciencias Biológicas, Químicas y de la Salud**, el **Comité de Análisis para las Intervenciones Urbanas, Arquitectónicas y de las Ingenierías**, el **Museo Universitario del Chopo**, la **Dirección General de Música**, la **Dirección de Danza**, el **Centro de Investigaciones en Geografía Ambiental, Campus Morelia**, el **Museo Universitario de Arte Contemporáneo**, la **Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género**, el **Instituto de Química**, la **Dirección de Literatura y Fomento a la Lectura**, la **Dirección General de Servicios Administrativos**, la **Dirección de Teatro UNAM**, el **Centro de Ciencias Genómicas**, la **Facultad de Artes y Diseño**, la **Dirección General de Televisión Universitaria**, el **Centro Cultural Universitario Tlatelolco**, la **Dirección General de Orientación y Atención Educativa**, el **Consejo Académico del Área de las Ciencias Sociales**, la **Escuela Nacional de Estudios Superiores, Unidad Mérida**, el **Instituto de Ecología**, la **Dirección General de Cooperación e Internacionalización**, el **Instituto de Investigaciones Biomédicas**, la **Casa del Lago "Mtro. Juan José Arreola"**, la **Coordinación para la Igualdad de Género**, la **Dirección General de la Escuela Nacional Preparatoria** y la **Escuela Nacional Preparatoria, Planteles 3 "Justo Sierra"** y **4 "Vidal Castañeda y Nájera"** y la **Dirección General del Deporte Universitario**, clasificaron como información reservada, por un periodo de **cinco años**, la relativa al **Análisis de Riesgo**, al **Análisis de Brecha** y al **Plan de Trabajo**, conforme a lo expuesto en el antecedente VII de la presente resolución, por actualizarse el supuesto establecido en los artículos 113, fracción VII y 110, fracción VII de las Leyes General y Federal de Transparencia y Acceso a la Información Pública, respectivamente.

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

> *"... Como información reservada podrá clasificarse aquella cuya publicación:*
>
> *[...]*
>
> ***VII.** Obstruya la prevención o persecución de los delitos;*
>
> *[...]".*

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

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

...".

Énfasis añadido.

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

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

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

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

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

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

Por su parte, el artículo 30, fracción V de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, dispone como uno de los mecanismos que deberá adoptar el responsable para cumplir con el principio de responsabilidad establecido en dicha Ley General,

contar con un sistema de supervisión y vigilancia, interna y/o externa, incluidas auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales.

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

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

De conformidad con lo anterior, con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, para establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad, el responsable deberá monitorear y revisar de manera periódica dichas medidas, donde no podrá pasar inadvertidas las nuevas amenazas, las posibles vulnerabilidades, los riesgos en conjunto, los incidentes y las vulneraciones de seguridad ocurridas, entre otras.

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

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

continua, derivado del monitoreo y revisión del sistema de gestión; como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida; así como con la implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

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

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

En este sentido, de difundirse la información contenida en los apartados relativos al **Análisis de Riesgos, al Análisis de Brecha**, al **Plan de Trabajo**, así como a **toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados** o que **revele vulnerabilidades en la protección de los datos personales en poder de las Áreas Universitarias,** se haría del conocimiento público la falta o debilidad de seguridad en un activo o grupo de activos, físicos o electrónicos, que puede ser explotada por una o más amenazas, lo que conllevaría a la materialización de las mismas y ocasionar la pérdida, destrucción no autorizada o incluso la sustracción de los datos personales en posesión de la Universidad, así como el robo, extravío o copia no autorizada de los mismos, su uso, acceso o tratamiento no autorizado, además del daño, alteración o modificación no autorizada, incluso impidiendo su recuperación, vulnerando así la seguridad de los datos personales.

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

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

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

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

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

...".

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

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

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

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

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

> *"Artículo 104. En la aplicación de la prueba de daño, el sujeto obligado deberá justificar que:*
>
> *I. La divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público o a la seguridad nacional;*
> *II. El riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda, y*
> *III. La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio".*

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

De difundirse el plan de trabajo, el análisis de riesgos y el análisis de brecha del documento de seguridad, se afectarían las medidas y acciones implementadas por las Áreas Universitarias para reducir el riesgo de que se cometa una conducta o un comportamiento que pueda dañar o convertir a esta Universidad y su comunidad en sujetos o víctimas de conductas ilícitas.

Lo anterior, toda vez que la publicidad de la información contenida en el **análisis de riesgos, de brecha** y el **plan de trabajo**, así como **toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados** o **revele vulnerabilidades en la protección de los datos personales en poder de las Áreas Universitarias**, representa un riesgo potencial para las Áreas Universitarias, pues a través

de dicha información se podrían identificar vulnerabilidades que pueden ser aprovechadas para realizar conductas contrarias a derecho, tales como actos vandálicos, o bien, ataques informáticos de diversa índole, disminuyendo la capacidad de las Áreas Universitarias para responder ante posibles amenazas.

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

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

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

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

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

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

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

Por lo antes mencionado, se colman las hipótesis de las fracciones I, II y III, dispuestas en el artículo 104 de la Ley General de Transparencia y Acceso a la Información Pública, por lo que es procedente **CONFIRMAR** la reserva total de una parte de la información para la elaboración de la

versión pública propuesta por el **Instituto de Matemáticas**, el **Instituto de Fisiología Celular**, la **Dirección General de la Escuela Nacional Colegio de Ciencias y Humanidades**, la **Escuela Nacional Colegio de Ciencias y Humanidades Planteles Azcapotzalco, Vallejo, Naucalpan, Oriente y Sur**, la **Facultad de Filosofía y Letras**, la **Coordinación de Difusión Cultural**, la **Dirección General de Estudios de Legislación Universitaria**, el **Centro Universitario de Teatro**, la **Dirección General de Radio UNAM**, la **Secretaría de Desarrollo Institucional**, el **Instituto de Física**, el **Consejo Académico del Área de las Ciencias Biológicas, Químicas y de la Salud**, el **Comité de Análisis para las Intervenciones Urbanas, Arquitectónicas y de las Ingenierías**, el **Museo Universitario del Chopo**, la **Dirección General de Música**, la **Dirección de Danza**, el **Centro de Investigaciones en Geografía Ambiental, Campus Morelia**, el **Museo Universitario de Arte Contemporáneo**, la **Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género**, el **Instituto de Química**, la **Dirección de Literatura y Fomento a la Lectura**, la **Dirección General de Servicios Administrativos**, la **Dirección de Teatro UNAM**, el **Centro de Ciencias Genómicas**, la **Facultad de Artes y Diseño**, la **Dirección General de Televisión Universitaria**, el **Centro Cultural Universitario Tlatelolco**, la **Dirección General de Orientación y Atención Educativa**, el **Consejo Académico del Área de las Ciencias Sociales**, la **Escuela Nacional de Estudios Superiores, Unidad Mérida**, el **Instituto de Ecología**, la **Dirección General de Cooperación e Internacionalización**, el **Instituto de Investigaciones Biomédicas**, la **Casa del Lago "Mtro. Juan José Arreola"**, la **Coordinación para la Igualdad de Género**, la **Dirección General de la Escuela Nacional Preparatoria** y la **Escuela Nacional Preparatoria, Planteles 3 "Justo Sierra"** y **4 "Vidal Castañeda y Nájera"** y la **Dirección General del Deporte Universitario**, por un periodo de **cinco años**, que se computarán a partir de la fecha de la presente resolución, de conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

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

- Deberán testar las secciones o información correspondientes al "Análisis de Riesgo", al "Análisis de Brecha", al "Plan de Trabajo", así como toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados o revele vulnerabilidades en la protección de los datos personales en su poder; para lo cual deberán emplear un medio que no permita la visualización de la misma y que no impida la lectura de aquella información que no es considerada como reservada. Al respecto, es importante precisar que **no deberán suprimirse las secciones** donde se contenga la información objeto de reserva.

- Deberán insertar un cuadro de texto en el cual se indiquen:

  - Las partes o secciones reservadas.

- El fundamento legal que sustenta la reserva, así como el plazo de ésta, mismos que se encuentran indicados en el último párrafo de la consideración **TERCERA** de la presente resolución.

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

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

R E S U E L V E

PRIMERO. Con fundamento en lo dispuesto en los artículos 1, 10, 11, 15 fracción X y 31, fracción I del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, 137, inciso a) de la Ley General de Transparencia y Acceso a la Información Pública y 140, fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública, este Comité de Transparencia **CONFIRMA** la **CLASIFICACIÓN** de **RESERVA** total de una parte la información para la elaboración de la versión pública de los Documentos de Seguridad, propuesta por el **Instituto de Matemáticas**, el **Instituto de Fisiología Celular**, la **Dirección General de la Escuela Nacional Colegio de Ciencias y Humanidades**, la **Escuela Nacional Colegio de Ciencias y Humanidades Planteles Azcapotzalco, Vallejo, Naucalpan, Oriente y Sur**, la **Facultad de Filosofía y Letras**, la **Coordinación de Difusión Cultural**, la **Dirección General de Estudios de Legislación Universitaria**, el **Centro Universitario de Teatro**, la **Dirección General de Radio UNAM**, la **Secretaría de Desarrollo Institucional**, el **Instituto de Física**, el **Consejo Académico del Área de las Ciencias Biológicas, Químicas y de la Salud**, el **Comité de Análisis para las Intervenciones Urbanas, Arquitectónicas y de las Ingenierías**, el **Museo Universitario del Chopo**, la **Dirección General de Música**, la **Dirección de Danza**, el **Centro de Investigaciones en Geografía Ambiental, Campus Morelia**, el **Museo Universitario de Arte Contemporáneo**, la **Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género**, el **Instituto de Química**, la **Dirección de Literatura y Fomento a la Lectura**, la **Dirección General de Servicios Administrativos**, la **Dirección de Teatro UNAM**, el **Centro de Ciencias Genómicas**, la **Facultad de Artes y Diseño**, la **Dirección General de Televisión Universitaria**, el **Centro Cultural Universitario Tlatelolco**, la **Dirección General de Orientación y Atención Educativa**, el **Consejo Académico del Área de las Ciencias Sociales**, la **Escuela Nacional de Estudios Superiores, Unidad Mérida**, el **Instituto de Ecología**, la **Dirección General de Cooperación e Internacionalización**, el **Instituto de Investigaciones Biomédicas**, la **Casa del Lago "Mtro. Juan José Arreola"**, la **Coordinación para la Igualdad de Género**, la **Dirección General de la**

Escuela Nacional Preparatoria y la **Escuela Nacional Preparatoria, Planteles 3 "Justo Sierra" y 4 "Vidal Castañeda y Nájera"** y la **Dirección General del Deporte Universitario**, en relación con el **Análisis de Riesgos**, el **Análisis de Brecha** y el **Plan de Trabajo**, así como **toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados o revele vulnerabilidades en la protección de los datos personales en poder de las Áreas Universitarias**, por un periodo de **cinco años**, contados a partir de la fecha de la presente resolución, o bien, hasta en tanto se extingan las causas que dieron origen a la reserva de la información.

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

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

TERCERO. Con fundamento en los artículos 45, fracción V y 137, último párrafo de la Ley General de Transparencia y Acceso a la Información Pública: así como 53, fracción VI, inciso c) del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, notifíquese la presente resolución por correo institucional al **Instituto de Matemáticas**, al **Instituto de Fisiología Celular**, a la **Dirección General de la Escuela Nacional Colegio de Ciencias y Humanidades**, a la **Escuela Nacional Colegio de Ciencias y Humanidades Planteles Azcapotzalco, Vallejo, Naucalpan, Oriente y Sur**, a la **Facultad de Filosofía y Letras**, a la **Coordinación de Difusión Cultural**, a la **Dirección General de Estudios de Legislación Universitaria**, al **Centro Universitario de Teatro**, a la **Dirección General de Radio UNAM**, a la **Secretaría de Desarrollo Institucional**, al **Instituto de Física**, al **Consejo Académico del Área de las Ciencias Biológicas, Químicas y de la Salud**, al **Comité de Análisis para las Intervenciones Urbanas, Arquitectónicas y de las Ingenierías**, al **Museo Universitario del Chopo**, a la **Dirección General de Música**, a la **Dirección de Danza**, al **Centro de Investigaciones en Geografía Ambiental, Campus Morelia**, al **Museo Universitario de Arte Contemporáneo**, a la **Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género**, al **Instituto de Química**, a la **Dirección de Literatura y Fomento a la Lectura**, a la **Dirección General de Servicios Administrativos**, a la **Dirección de Teatro UNAM**, al **Centro de Ciencias Genómicas**, a la **Facultad de Artes y Diseño**, a la **Dirección General de Televisión Universitaria**, al **Centro Cultural Universitario Tlatelolco**, a la **Dirección General de Orientación y Atención Educativa**, al **Consejo Académico del Área de las Ciencias Sociales**, la **Escuela Nacional de Estudios Superiores, Unidad Mérida**, al **Instituto de Ecología**, a la **Dirección General de Cooperación e Internacionalización**, al **Instituto de Investigaciones Biomédicas**, a la **Casa del Lago "Mtro. Juan José Arreola"**, a la **Coordinación para la Igualdad de Género**, a la **Dirección General de la Escuela Nacional Preparatoria** y a la **Escuela Nacional Preparatoria, Planteles 3 "Justo Sierra" y 4 "Vidal Castañeda y Nájera"**, a la **Dirección General del Deporte Universitario**, así como a la Unidad de Transparencia de esta Universidad, para los efectos procedentes.

Así lo resolvió por unanimidad de votos de sus integrantes, el Comité de Transparencia de la Universidad Nacional Autónoma de México, en términos de los artículos 1, 11, 15, 20 y 53,

fracción VI del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

POR MI RAZA HABLARÁ EL ESPÍRITU"
Ciudad Universitaria, Cd. Mx., 19 de agosto de 2022