Casa abierta al tiempo
UNIVERSIDAD AUTÓNOMA METROPOLITANA

Casa abierta al tiempo
UNIVERSIDAD AUTÓNOMA METROPOLITANA

VERSIÓN PÚBLICA DEL DOCUMENTO DE SEGURIDAD EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

2025

RECTORÍA GENERAL
UNIDAD DE TRANSPARENCIA
Prolongación Canal de Miramontes No. 3855, Edificio “A” Planta Baja Col. Ex-Hacienda San Juan de Dios, Alcaldía Tlalpan, C.P. 14387, Ciudad de México, Tels. 5483 4000 ext. 1587 y 1588 e-mail transparencia@correo.uam.mx

Nota preliminar.

El artículo 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, establece que se deberá elaborar un documento de seguridad que contenga, al menos, lo siguiente:

I. El inventario de datos personales y de los sistemas de tratamiento;
II. Las funciones y obligaciones de las personas que traten datos personales;
III. El análisis de riesgos;
IV. El análisis de brecha;
V. El plan de trabajo;
VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad, y
VII. El programa general de capacitación.

Con el objetivo de garantizar la protección de los datos personales y los sistemas institucionales y de conformidad con las recomendaciones del Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (INAI), se elaboró la presente versión pública del documento de seguridad en el que se protege y no serán visibles, los siguientes elementos:

- El plan de trabajo
- El análisis de riesgo
- En análisis de brecha

Por las razones expuestas con antelación, las secciones presentarán la leyenda de clasificación.

Contenido

Introducción

El 26 de enero de 2017 se expidió la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (en lo sucesivo, la Ley General de Datos), la cual tiene como objetivo establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales que estén en posesión de los sujetos obligados.

De conformidad con lo dispuesto por los artículos 29 y 30, fracciones I y VII de la Ley General, se deberán implementar mecanismos para acreditar el cumplimiento de los principios, deberes y obligaciones que permiten garantizar un adecuado tratamiento de datos personales.

El 26 de enero de 2018, se publicaron en el Diario Oficial de la Federación los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales) cuyo objetivo es desarrollar las disposiciones previstas en la Ley General de Datos y, con ello, hacer más comprensible el cumplimiento de los principios, deberes y obligaciones exigidos en materia de protección de datos personales.

En específico, con relación al deber de seguridad, el artículo 31 de la Ley General de Datos señala que el responsable del tratamiento deberá establecer y mantener 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.

Por su parte, el artículo 35 de la Ley General de Datos establece como una obligación la elaboración de un documento de seguridad, que se define -según la fracción

XIV del artículo 3 de la Ley General- como 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 y que deberá contener, al menos, la siguiente información:

I. El inventario de datos personales y de los sistemas de tratamiento;
II. Las funciones y obligaciones de las personas que traten datos personales;
III. El análisis de riesgos;
IV. El análisis de brecha;
V. El plan de trabajo;
VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad, y
VII. El programa general de capacitación.

En ese sentido, en cumplimiento de las obligaciones antes descritas, a continuación, se presenta el documento de seguridad de la Universidad Autónoma Metropolitana con los elementos informativos que establece el artículo 35 de la Ley General de Datos.

I. El inventario de datos personales y de los sistemas de tratamiento.

El artículo 33, fracción I de la Ley General establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, la elaboración de un inventario de datos personales y de los sistemas de tratamiento.

Como se señaló, de acuerdo con la fracción I del artículo 35 de la Ley General, este inventario forma parte del documento de seguridad y que para mayor claridad debe observarse lo establecido en el artículo de los Lineamientos Generales .

En este contexto, se elaboraron los inventarios de los distintos tratamientos de datos personales que se realizan en la Universidad y que conforman las bases de datos del Sistema Integral de Información de la Universidad Autónoma Metropolitana, identificando los elementos informativos que señala el artículo 58 de los Lineamientos Generales y basados en el ciclo de vida de los datos personales, como lo requiere el artículo 59 de los Lineamientos Generales.

Es importante mencionar, que la Universidad Autónoma Metropolitana cuenta con un Sistema Integral de Información denominado “SIIUAM”, que es un desarrollo tecnológico propio diseñado con el objetivo de garantizar los procesos administrativos y operativos propios de la Universidad y que por mencionar algunas, presenta las siguientes características:

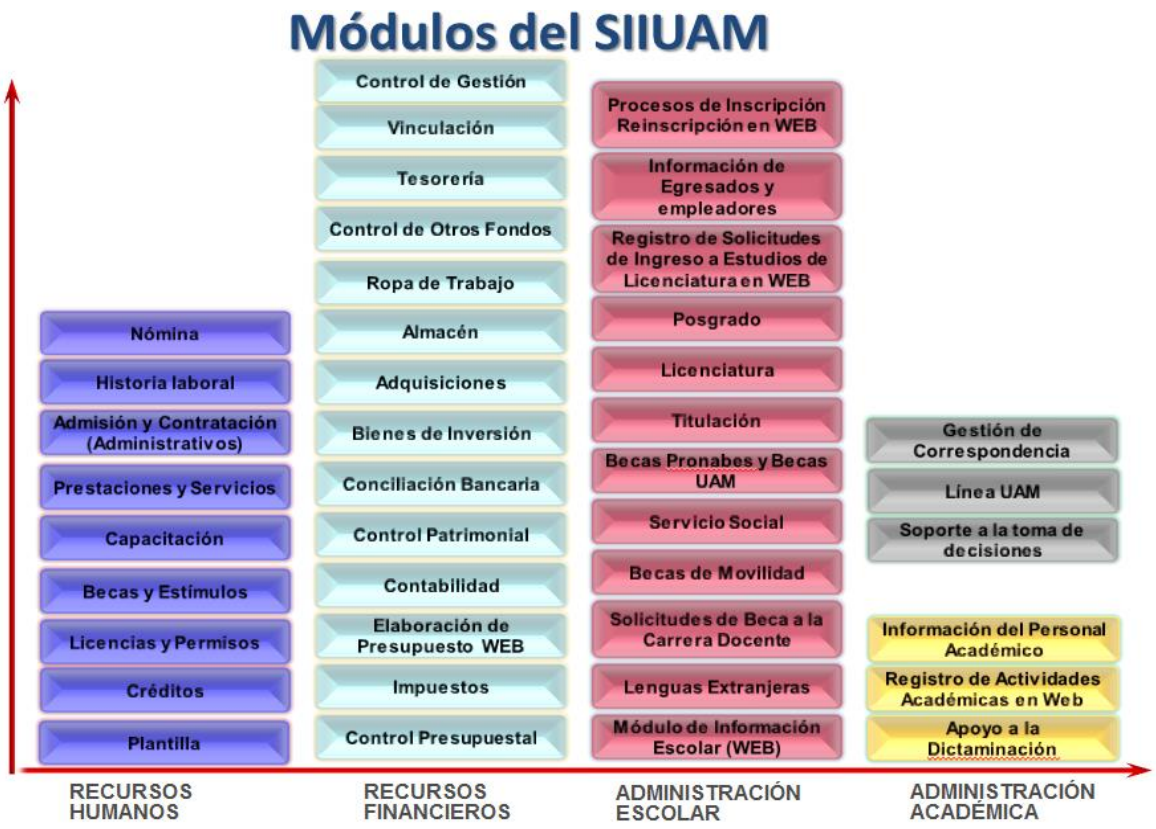
- Operación transaccional en línea
- Homogeneidad entre los sistemas
- Desarrollo diseñado con carácter institucional

- Control de información a todos los niveles de la estructura programática de la Universidad
- Control de acceso a aplicaciones por medio de perfiles de usuarios establecido por los dueños de los datos
- Acceso al SIIUAM (cliente/servidor, web y aplicaciones móviles)
- Tableros de control para toma de decisiones

En este sentido es importante mencionar que nuestro desarrollo tecnológico permite una verdadera integración de bases de datos que garantizan el ejercicio de los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO) y maximizan el umbral de protección de los datos personales.

Para lograr este objetivo se consideran cuatro grandes módulos:

De los módulos existentes se desprenden submódulos, que de acuerdo a sus características almacenan datos personales y que son los siguientes:



De manera pragmática, los inventarios presentados son:

Número	Nombre del módulo	Denominación del Inventario de Datos Personales
1	**Recursos Humanos**	Plantilla
		Créditos
		Licencias y permisos
		Becas y estímulos
		Capacitación
		Prestaciones y servicios
		Admisión y contratación
		Historia laboral

		Nómina
2	**Recursos Financieros**	Control presupuestal
		Impuestos
		Elaboración de presupuesto
		Contabilidad
		Control patrimonial
		Contabilidad
		Conciliación bancaria
		Bienes de inversión
		Adquisiciones
		Almacén
		Ropa de trabajo
		Control de fondos
		Tesorería
		Vinculación
		Control de gestión
3	**Administración escolar**	Módulo de información escolar
		Lenguas extranjeras
		Solicitudes de beca a la carrera docente
		Becas de movilidad
		Servicio social
		Becas Pronabes y Becas UAM
		Titulación
		Licenciatura
		Posgrado
		Registro de solicitudes de ingreso a estudios de licenciatura

		Información de egresados y empleadores
		Proceso de inscripción o reinscripción en web
4	**Administración académica**	Apoyo a la dictaminación
		Registro de actividades académicas en web
		Información del personal académico
		Línea UAM
		Gestión de correspondencia

II. Las funciones y obligaciones de las personas que traten datos personales.

El artículo 33, fracción II de la Ley General establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, la definición de las funciones y obligaciones del personal involucrado en el tratamiento de datos personales.

Como se señaló, de acuerdo con la fracción II del artículo 35 de la Ley General y 57 de los Lineamientos Generales, las obligaciones del personal que con motivo de sus facultades y atribuciones trata datos personales, se dividen en dos niveles:

I. A **nivel macro**, a través de la Política de Protección de Datos Personales, el Programa de Capacitación y los Sistemas de Supervisión y Vigilancia de la Universidad Autónoma Metropolitana, se describen todas las obligaciones que establece la Ley General y los Lineamientos Generales y estas se asociación con la dependencia universitaria responsable de su cumplimiento, y
II. A **nivel micro,** a través de los inventarios que se desarrollaron por cada uno de los tratamientos, en los cuales se identificó a las personas que realizan su tratamiento, la dependencia universitaria a la cual está adscrita y la finalidad de dicho tratamiento.

En este contexto, las funciones y obligaciones que deberán realizar las personas que con motivo de sus funciones y atribuciones realicen el tratamiento de datos personales, en estricta observancia de la Ley General y los Lineamientos Generales, se detallan en la Política de Protección de Datos Personales, a saber:

I. **Licitud:** El tratamiento de datos personales por parte de las dependencias universitarias debe ser realizado de conformidad con las atribuciones o facultades que previamente se otorgan en la normatividad aplicable.

II. **Finalidad:** Todo tratamiento de datos personales efectuado deberá estar justificado por finalidades concretas, explícitas, lícitas y legítimas.

III. **Lealtad.-** Las dependencias universitarias se abstendrán de obtener y tratar datos personales a través de medios engañosos o fraudulentos.

IV. **Consentimiento:** Previo al tratamiento de datos personales se deberá obtener el consentimiento de las y los titulares de datos personales de manera libre, específica, inequívoca e informada, salvo que se configuren las causales de excepción establecidas en el artículo 22 de la LGPDPPSO

V. **Calidad:** Las dependencias universitarias deberán mantener los datos personales conforme a la finalidad o finalidades para las que se hayan recabado y adoptarán las medidas necesarias para mantenerlos.

VI. **Proporcionalidad:** Se recabarán solo los datos personales que resulten necesarios, adecuados y relevantes para la finalidad que justifica su tratamiento y las finalidades que motivaron su obtención, de acuerdo con las facultades y atribuciones de cada dependencia universitaria.

VII. **Información:** La persona titular de los datos personales en todo momento puede conocer las características principales del tratamiento al que será sometida su información, lo que se materializa a través del aviso de privacidad integral y simplificado.

VIII. **Responsabilidad:** Las dependencias universitarias adoptarán las medidas necesarias para garantizar el adecuado tratamiento de datos personales.

Adicionalmente, las dependencias universitarias, cumplirán con los siguientes deberes:

I. **Deber de confidencialidad**: Las dependencias universitarias establecerán controles o mecanismos de observancia obligatoria para garantizar un adecuado tratamiento de datos personales y evitar que sean revelados a personas no autorizadas.

II. **Deber de Seguridad:** Las dependencias universitarias adoptarán e instrumentarán las medidas físicas, técnicas y administrativas a través de las cuales se garantice la protección de datos personales.

Adicionalmente, conviene señalar que las funciones y obligaciones del personal que trata datos personales se encuentran definidas en la legislación universitaria y en la normatividad específica en materia de protección de datos personales.

III. Análisis de Riesgo

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

APARTADO CORRESPONDIENTE AL ANÁLISIS DE RIESGO

Con el objetivo de garantizar la protección de los datos personales y los sistemas institucionales y de conformidad con las recomendaciones del Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personal (INAI), se elaboró la presente versión pública del documento de seguridad en el que se protege y no serán visibles, los siguie elementos:

El plan de trabajo

El análisis de riesgo

En análisis de brecha

Por las razones expuestas con antelación, las secciones presentaran la leyenda de clasificación.

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

Con el objetivo de garantizar la protección de los datos personales y los sistemas institucionales y de conformidad con las recomendaciones del Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personal (INAI), se elaboró la presente versión pública del documento de seguridad en el que se protege y no serán visibles, los siguie elementos:

El plan de trabajo

El análisis de riesgo

En análisis de brecha

Por las razones expuestas con antelación, las secciones presentaran la leyenda de clasificación

RECTORÍA GENERAL
UNIDAD DE TRANSPARENCIA
Prolongación Canal de Miramontes No. 3855, Edificio “A” Planta Baja Col. Ex-Hacienda San Juan de Dios, Alcaldía Tlalpan, C.P. 14387, Ciudad de México, Tels. 5483 4000 ext. 1587 y 1588 e-mail transparencia@correo.uam.mx

Casa abierta al tiempo

UNIVERSIDAD AUTÓNOMA METROPOLITANA

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

APARTADO CORRESPONDIENTE AL ANÁLISIS DE RIESGO

Con el objetivo de garantizar la protección de los datos personales y los sistemas institucionales y de conformidad con las recomendaciones del Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personal (INAI), se elaboró la presente versión pública del documento de seguridad en el que se protege y no serán visibles, los siguie elementos:

El plan de trabajo

El análisis de riesgo

En análisis de brecha

Por las razones expuestas con antelación, las secciones presentaran la leyenda de clasificación.

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

Con el objetivo de garantizar la protección de los datos personales y los sistemas institucionales y de conformidad con las recomendaciones del Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personal (INAI), se elaboró la presente versión pública del documento de seguridad en el que se protege y no serán visibles, los siguie elementos:

El plan de trabajo

El análisis de riesgo

En análisis de brecha

Por las razones expuestas con antelación, las secciones presentaran la leyenda de clasificación

RECTORÍA GENERAL
UNIDAD DE TRANSPARENCIA
Prolongación Canal de Miramontes No. 3855, Edificio “A” Planta Baja Col. Ex-Hacienda San Juan de Dios, Alcaldía Tlalpan, C.P. 14387, Ciudad de México, Tels. 5483 4000 ext. 1587 y 1588 e-mail transparencia@correo.uam.mx

Casa abierta al tiempo

UNIVERSIDAD AUTÓNOMA METROPOLITANA

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

APARTADO CORRESPONDIENTE AL ANÁLISIS DE RIESGO

Con el objetivo de garantizar la protección de los datos personales y los sistemas institucionales y de conformidad con las recomendaciones del Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personal (INAI), se elaboró la presente versión pública del documento de seguridad en el que se protege y no serán visibles, los siguie elementos:

El plan de trabajo

El análisis de riesgo

En análisis de brecha

Por las razones expuestas con antelación, las secciones presentaran la leyenda de clasificación.

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

Con el objetivo de garantizar la protección de los datos personales y los sistemas institucionales y de conformidad con las recomendaciones del Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personal (INAI), se elaboró la presente versión pública del documento de seguridad en el que se protege y no serán visibles, los siguie elementos:

El plan de trabajo

El análisis de riesgo

En análisis de brecha

Por las razones expuestas con antelación, las secciones presentaran la leyenda de clasificación

RECTORÍA GENERAL
UNIDAD DE TRANSPARENCIA
Prolongación Canal de Miramontes No. 3855, Edificio “A” Planta Baja Col. Ex-Hacienda San Juan de Dios, Alcaldía Tlalpan, C.P. 14387, Ciudad de México, Tels. 5483 4000 ext. 1587 y 1588 e-mail transparencia@correo.uam.mx

IV. Análisis de brecha

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

APARTADO CORRESPONDIENTE AL ANÁLISIS DE BRECHA

Con el objetivo de garantizar la protección de los datos personales y los sistemas institucionales y de conformidad con las recomendaciones del Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (INAI), se elaboró la presente versión pública del documento de seguridad en el que se protege y no serán visibles, los siguientes elementos:

El plan de trabajo

El análisis de riesgo

En análisis de brecha

Por las razones expuestas con antelación, las secciones presentaran la leyenda de clasificación.

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

Con el objetivo de garantizar la protección de los datos personales y los sistemas institucionales y de conformidad con las recomendaciones del Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (INAI), se elaboró la presente versión pública del documento de seguridad en el que se protege y no serán visibles, los siguientes elementos:

El plan de trabajo

El análisis de riesgo

En análisis de brecha

Por las razones expuestas con antelación, las secciones presentaran la leyenda de clasificación

RECTORÍA GENERAL
UNIDAD DE TRANSPARENCIA
Prolongación Canal de Miramontes No. 3855, Edificio “A” Planta Baja Col. Ex-Hacienda San Juan de Dios, Alcaldía Tlalpan, C.P. 14387, Ciudad de México, Tels. 5483 4000 ext. 1587 y 1588 e-mail transparencia@correo.uam.mx

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

APARTADO CORRESPONDIENTE AL ANÁLISIS DE BRECHA

Con el objetivo de garantizar la protección de los datos personales y los sistemas institucionales y de conformidad con las recomendaciones del Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (INAI), se elaboró la presente versión pública del documento de seguridad en el que se protege y no serán visibles, los siguiente elementos:

El plan de trabajo

El análisis de riesgo

En análisis de brecha

Por las razones expuestas con antelación, las secciones presentaran la leyenda de clasificación.

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

Con el objetivo de garantizar la protección de los datos personales y los sistemas institucionales y de conformidad con las recomendaciones del Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (INAI), se elaboró la presente versión pública del documento de seguridad en el que se protege y no serán visibles, los siguiente elementos:

El plan de trabajo

El análisis de riesgo

En análisis de brecha

Por las razones expuestas con antelación, las secciones presentaran la leyenda de clasificación

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

APARTADO CORRESPONDIENTE AL ANÁLISIS DE BRECHA

l objetivo de garantizar la protección de los datos personales y los sistemas institucionales y de conformidad con las ndaciones del Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales elaboró la presente versión pública del documento de seguridad en el que se protege y no serán visibles, los siguientes elementos:

El plan de trabajo

El análisis de riesgo

En análisis de brecha

Por las razones expuestas con antelación, las secciones presentaran la leyenda de clasificación.

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

l objetivo de garantizar la protección de los datos personales y los sistemas institucionales y de conformidad con las ndaciones del Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales elaboró la presente versión pública del documento de seguridad en el que se protege y no serán visibles, los siguientes elementos:

El plan de trabajo

El análisis de riesgo

En análisis de brecha

Por las razones expuestas con antelación, las secciones presentaran la leyenda de clasificación

V. Plan de trabajo

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

APARTADO CORRESPONDIENTE AL PLAN DE TRABAJO

Con el objetivo de garantizar la protección de los datos personales y los sistemas institucionales y de conformidad con las recomendaciones del Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (INAI), se elaboró la presente versión pública del documento de seguridad en el que se protege y no serán visibles, los siguiente elementos:

El plan de trabajo

El análisis de riesgo

En análisis de brecha

Por las razones expuestas con antelación, las secciones presentaran la leyenda de clasificación.

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

Con el objetivo de garantizar la protección de los datos personales y los sistemas institucionales y de conformidad con las recomendaciones del Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (INAI), se elaboró la presente versión pública del documento de seguridad en el que se protege y no serán visibles, los siguiente elementos:

El plan de trabajo

El análisis de riesgo

En análisis de brecha

Por las razones expuestas con antelación, las secciones presentaran la leyenda de clasificación

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

APARTADO CORRESPONDIENTE AL PLAN DE TRABAJO

Con el objetivo de garantizar la protección de los datos personales y los sistemas institucionales y de conformidad con las recomendaciones del Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (INAI), se elaboró la presente versión pública del documento de seguridad en el que se protege y no serán visibles, los siguiente elementos:

El plan de trabajo

El análisis de riesgo

En análisis de brecha

Por las razones expuestas con antelación, las secciones presentaran la leyenda de clasificación.

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

Con el objetivo de garantizar la protección de los datos personales y los sistemas institucionales y de conformidad con las recomendaciones del Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (INAI), se elaboró la presente versión pública del documento de seguridad en el que se protege y no serán visibles, los siguiente elementos:

El plan de trabajo

El análisis de riesgo

En análisis de brecha

Por las razones expuestas con antelación, las secciones presentaran la leyenda de clasificación

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

APARTADO CORRESPONDIENTE AL PLAN DE TRABAJO

Con el objetivo de garantizar la protección de los datos personales y los sistemas institucionales y de conformidad con las recomendaciones del Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (INAI), se elaboró la presente versión pública del documento de seguridad en el que se protege y no serán visibles, los siguiente elementos:

El plan de trabajo

El análisis de riesgo

En análisis de brecha

Por las razones expuestas con antelación, las secciones presentaran la leyenda de clasificación.

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD

Con el objetivo de garantizar la protección de los datos personales y los sistemas institucionales y de conformidad con las recomendaciones del Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (INAI), se elaboró la presente versión pública del documento de seguridad en el que se protege y no serán visibles, los siguiente elementos:

El plan de trabajo

El análisis de riesgo

En análisis de brecha

Por las razones expuestas con antelación, las secciones presentaran la leyenda de clasificación

VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad.

El artículo 33, fracción VII de la Ley General establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, el monitoreo y revisión de manera periódica de las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales.

De conformidad con la fracción VI del artículo 35 de la Ley General y el artículo 63 de los Lineamientos Generales los mecanismos de monitoreo y revisión forman parte del documento de seguridad y tienen el objetivo de fortalecer, a través de un ciclo de mejora continua, la protección de los datos personales que resguarda la institución.

A continuación, se desarrollan las acciones de monitoreo y supervisión periódica para las medidas de seguridad:

I.- Mecanismos de monitoreo

Para los tratamientos de datos personales, se consideran los siguientes tipos de monitoreo:

1) **Revisión de cumplimiento de las políticas internas, relacionadas con el tratamiento de datos personales.** Tiene el objetivo de asegurar que las personas que realicen los tratamientos de datos personales derivados de sus facultades y atribuciones, lo hagan en concordancia con el marco normativo universitario y el de protección de datos personales.

   Para ello, cuando se identifica algún cambio en los instrumentos antes mencionados, se deberán realizar las siguientes actividades:

a. Revisar y, en su caso, actualizar los procesos involucrados en el tratamiento de datos personales.
b. Revisar y, en su caso, actualizar los avisos de privacidad, las funciones y obligaciones del personal y los inventarios de datos personales, según corresponda.
c. Evaluar si hubo cambios en las amenazas, vulnerabilidades o impacto de los riesgos relacionados con las modificaciones a la normativa, para actualizar los análisis de riesgos, análisis de brecha y plan de trabajo.
d. Revisar y, en su caso, adecuar los sistemas de tratamiento para cumplir con los cambios normativos.

2) **Revisión del riesgo.** Tiene el objetivo de identificar modificaciones a los riesgos identificados en los tratamientos de datos personales, para ello, se implementarán los siguientes monitoreos:

a. **Monitoreo del entorno físico.** Para la detección continua de amenazas y vulnerabilidades en el entorno físico, se cuenta con: (i) personal de vigilancia en el acceso a todas las instalaciones de la Universidad Autónoma Metropolitana, (ii) control de acceso al estacionamiento del personal con tarjeta de proximidad, (iii) control de acceso a través de bitácoras para visitantes, y (iv) circuito cerrado de cámaras de vigilancia.
b. **Monitoreo del entorno electrónico.** Para la detección continua de amenazas y vulnerabilidades, la Dirección de Tecnologías de Información cuenta con herramientas automatizadas de monitoreo (activo y pasivo).
c. **Actualización del plan de trabajo.** Derivado del monitoreo del entorno físico o electrónico, se pueden realizar actualizaciones en el plan de trabajo en caso de que se identifiquen cambios en las amenazas, las vulnerabilidades o el impacto de los riesgos identificados.
d. **Revisión de avances del plan de trabajo.** A través de los mecanismos que determine el área que apoya en el análisis de riesgos, el Comité de

Transparencia revisa los avances en el plan de trabajo, identificando las acciones, fechas compromiso y, en su caso, las causas por las cuales no se está cumpliendo el plan de trabajo, para hacer los ajustes correspondientes al mismo.

e. **Actualización tecnológica.** Cuando se integren nuevos equipos de cómputo, servidores, aplicaciones o tenga lugar una migración tecnológica, se realizará una actualización del análisis de riesgo, análisis de brecha y plan de trabajo.

A continuación, se describen los mecanismos de monitoreo y revisión:

Elemento a revisar	Fundamento	Acciones
Los nuevos activos que se incluyan en la gestión de riesgos;	63, fracción I, de los Lineamientos Generales.	1. Revisión de cumplimiento de las políticas institucionales, relacionadas con el tratamiento de datos personales.
Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras;	63, fracción II, de los Lineamientos Generales.	
Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas;	63, fracción III, de los Lineamientos Generales.	
La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;	63, fracción IV, de los Lineamientos Generales.	1. Revisión de cumplimiento de las políticas institucionales, relacionadas con el tratamiento de datos personales.
Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;	63, fracción V, de los Lineamientos Generales.	Monitoreo del entorno físico Monitoreo del entorno electrónico 1

El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo	63, fracción VI, de los Lineamientos Generales.	1. Revisión de cumplimiento de las políticas institucionales, relacionadas con el tratamiento de datos personales. Actualización del plan de trabajo. Revisión de avances del plan de trabajo.
Los incidentes y vulneraciones de seguridad ocurridas.	63, fracción VII, de los Lineamientos Generales.	1. Revisión de cumplimiento de las institucionales, relacionadas con el tratamiento de datos personales. Vulneraciones a la seguridad de los datos personales.

II.- Mecanismos de supervisión o revisión

Además del monitoreo continuo de las medidas de seguridad, se requiere realizar una supervisión periódica de las medidas de seguridad, a través de auditorías, las cuales pueden ser internas o externas.

Hasta el momento no se han realizado auditorías específicas en materia de protección de datos personales.

Así, respecto del programa de auditoría mencionado en el último párrafo del artículo 63 de los Lineamientos Generales, se tiene contemplada la realización de una auditoría en materia de protección de datos personales, al menos una vez al año. Dicha auditoría se puede llevar a cabo por terceros según la disponibilidad presupuestal, o bien, conforme lo determine el Comité de Transparencia.

El programa de auditoría será aquél que determine el Comité de Transparencia en el Programa de Protección de Datos Personales.

VII. El programa general de capacitación.

Introducción

La Universidad Autónoma Metropolitana garantiza el ejercicio efectivo de la protección de datos personales, por lo que también debe dar cumplimiento a las obligaciones que establece el marco normativo en la materia, además de atender las verificaciones vinculantes que realiza el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Con el objetivo de facilitar el ejercicio de este derecho y dar cumplimiento a las obligaciones en la materia, de conformidad con la Ley General de Protección de Datos Personales y los Lineamientos Generales de Protección de Datos Personales en el Sector Público, se formuló el presente programa que contiene acciones específicas que permiten fortalecer también el ejercicio de los derechos de Acceso, Cancelación, Oposición y Rectificación de datos personales.

El programa se construyó considerando cuatro ejes a saber:

- Difusión institucional;
- Ejercicio efectivo de los derechos ARCO;
- Deber de seguridad y confidencialidad; y
- Tratamiento adecuado de datos personales.

Con la segmentación planteada, se pretende abordar de manera específica la familiarización en el tema y que de manera puntual abona al cumplimiento del marco normativo en la materia.

Desde una visión incluyente, inclusiva e itinerante se destinarán las acciones necesarias de familiarización a través de los ejes propuestos para garantizar el

cumplimiento irrestricto de las disposiciones legales y fomentar una cultura de la protección de datos personales.

Población Objetivo

La población objetivo del presente programa, se circunscribe principalmente a las dependencias a las que hace referencia el artículo 14 del Reglamento para la Transparencia Universitaria de la Universidad Autónoma Metropolitana y que son:

a) La Junta Directiva;
b) El Colegio Académico;
c) El Patronato;
d) Los consejos académicos;
e) Los consejos divisionales;
f) La Rectoría General;
g) Las rectorías de unidad;
h) Las divisiones académicas;
i) Los departamentos académicos;
j) La Secretaría General;
k) La Oficina del Abogado General;
l) La Tesorería General;
m) La Contraloría;
n) Las secretarías de unidad;
o) Las secretarías académicas de división;
p) Las coordinaciones de estudio;
q) Las jefaturas de área;
r) La Defensoría de los Derechos Universitarios, y
s) Las comisiones dictaminadoras de área, divisionales, y de Recursos.

Las cuales, por sus facultades y atribuciones podrían realizar un tratamiento de datos personales. Es importante mencionar que las acciones que se realicen para la difusión y ejercicio de los derechos de Acceso, Cancelación, Oposición y Rectificación se dirigen a toda la comunidad universitaria.

Glosario

Para la aplicación y ejecución de las acciones que contiene el presente programa, se entenderá:

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

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

III. **Bloqueo:** La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponda;

IV. **Comité de Transparencia**: Instancia a la que hace referencia el artículo 43 de la Ley General de Transparencia y Acceso a la Información Pública; y 6,7,8 y 9 del Reglamento para la Transparencia Universitaria de la Universidad Autónoma Metropolitana;

V. **Cómputo en la nube:** Modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente;

VI. **Consentimiento**: Manifestación de la voluntad libre, específica e informada del titular de los datos mediante la cual se efectúa el tratamiento de los mismos;

VII. **Datos personales**: Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando

su identidad pueda determinarse directa o indirectamente a través de cualquier información;

VIII. **Datos personales sensibles:** Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual;

IX. **Dependencias universitarias:** Instancias a las que hace referencia el artículo 14 del Reglamento para la Transparencia Universitaria de la Universidad Autónoma Metropolitana y que son:

a) La Junta Directiva;
b) El Colegio Académico;
c) El Patronato;
d) Los consejos académicos;
e) Los consejos divisionales;
f) La Rectoría General;
g) Las rectorías de unidad;
h) Las divisiones académicas;
i) Los departamentos académicos;
j) La Secretaría General;
k) La Oficina del Abogado General;
l) La Tesorería General;
m) La Contraloría;
n) Las secretarías de unidad;
o) Las secretarías académicas de división;
p) Las coordinaciones de estudio;
q) Las jefaturas de área;
r) La Defensoría de los Derechos Universitarios, y
s) Las comisiones dictaminadoras de área, divisionales, y de Recursos.

X. **Derechos ARCO:** Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales;

XI. **Disociación:** El procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo;

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

XIII. **Encargado:** La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable;

XIV. **Evaluación de impacto en la protección de datos personales:** Documento mediante el cual los sujetos obligados que pretendan poner en operación o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales, valoran los impactos reales respecto de determinado tratamiento de datos personales, a efecto de identificar y mitigar posibles riesgos relacionados con los principios, deberes y derechos de los titulares, así como los deberes de los responsables y encargados, previstos en la normativa aplicable;

XV. **Fuentes de acceso público:** Aquellas bases de datos, sistemas o archivos que por disposición de ley puedan ser consultadas públicamente cuando no exista impedimento por una norma limitativa y sin más exigencia que, en su caso, el pago de una contraprestación, tarifa o contribución. No se considerará fuente de acceso público cuando la información contenida en la misma sea obtenida o tenga una procedencia ilícita, conforme a las disposiciones establecidas por la presente Ley y demás normativa aplicable;

XVI. **Medidas compensatorias:** Mecanismos alternos para dar a conocer a los titulares el aviso de privacidad, a través de su difusión por medios masivos de comunicación u otros de amplio alcance;

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

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

XIX. **Medidas de seguridad físicas:** Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

a) Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;

b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;

c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y

d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad;

XX. **Medidas de seguridad técnicas:** Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

a) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;

b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;

c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y

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

XXI. **Plataforma Nacional**: La Plataforma Nacional de Transparencia a que hace referencia el artículo 49 de la Ley General de Transparencia y Acceso a la Información Pública;

XXII. **Programa Nacional de Protección de Datos Personales**: Programa Nacional de Protección de Datos Personales;

XXIII. **Remisión:** Toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado, dentro o fuera del territorio mexicano;

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

XXV. **Titular**: La persona física a quien corresponden los datos personales;

XXVI. **Transferencia:** Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado;

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

XXVIII. **Unidad de Transparencia:** Instancia a la que hace referencia el artículo 45 de la Ley General de Transparencia y Acceso a la Información Pública; y el artículo 11

del Reglamento para la Transparencia Universitaria de la Universidad Autónoma Metropolitana

Principios

Para garantizar un ejercicio adecuado de los derechos de Acceso, Rectificación, Cancelación y Oposición las dependencias universitarias, cuando realicen el tratamiento de datos personales, deberán observar los siguientes principios rectores:

IX. **Licitud:** El tratamiento de datos personales por parte de las dependencias universitarias debe ser realizado de conformidad con las atribuciones o facultades que previamente se otorgan en la normatividad aplicable.

X. **Finalidad:** Todo tratamiento de datos personales efectuado deberá estar justificado por finalidades concretas, explícitas, lícitas y legítimas.

XI. **Lealtad.-** Las dependencias universitarias se abstendrán de obtener y tratar datos personales a través de medios engañosos o fraudulentos.

XII. **Consentimiento:** Previo al tratamiento de datos personales se deberá obtener el consentimiento de las y los titulares de datos personales de manera libre, específica, inequívoca e informada, salvo que se configuren las causales de excepción establecidas en el artículo 22 de la LGPDPPSO

XIII. **Calidad:** Las dependencias universitarias deberán mantener los datos personales conforme a la finalidad o finalidades para las que se hayan recabado y adoptarán las medidas necesarias para mantenerlos.

XIV. **Proporcionalidad:** Se recabarán solo los datos personales que resulten necesarios, adecuados y relevantes para la finalidad que justifica su tratamiento y las finalidades que motivaron su obtención, de acuerdo con las facultades y atribuciones de cada dependencia universitaria.

XV. **Información:** La persona titular de los datos personales en todo momento puede conocer las características principales del tratamiento al que será sometida su información, lo que se materializa a través del aviso de privacidad integral y simplificado.

XVI. **Responsabilidad:** Las dependencias universitarias adoptarán las medidas necesarias para garantizar el adecuado tratamiento de datos personales.

Eje 1: Difusión Institucional

Objetivo General.

Difundir entre la comunidad universitaria la importancia de la protección de datos personales y las acciones que realiza la institución para garantizar su máximo umbral de protección.

Objetivo particular.

Que la Unidad de Transparencia en coordinación con el Comité de Transparencia impulse acciones relacionadas con el estudio y difusión de las acciones que fortalezcan la cultura de la protección de datos personales.

Acciones

1) Propiciar el involucramiento del alumnado y el personal en actos académicos de difusión que permitan socializar el derecho a la protección de datos personales.

2) Generar y visibilizar convenios de colaboración interinstitucional que fomenten la difusión de la protección de datos personales.

3) Organizar un foro-taller interinidades y anual con la intención de fortalecer la cultura de la transparencia y la protección de datos personales.

4) Promover y difundir todos los avances y logros que tenga la Universidad relacionados con la protección de datos personales.

5) Crear una página electrónica que compile todas las acciones y muestre la documentación necesaria para que la comunidad universitaria pueda ejercer su derecho a la protección de datos personales.

Cronograma de actividades del eje 1:

	Año 2025		Año 2026	
Acción	Semestre 1	Semestre 2	Semestre 1	Semestre 2
1	x	x	x	x
2		x	x	
3		x		x
4	x		x	
5	x			

Eje 2: Ejercicio Efectivo de los Derechos ARCO

Objetivo General.

Garantizar que la comunidad universitaria pueda ejercer sus derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO).

Objetivo particular.

Que la comunidad universitaria pueda ejercer sus derechos ARCO de manera eficiente.

Acciones

1) Establecer procedimientos que garanticen el ejercicio de los derechos ARCO.

2) Establecer la política en materia de protección de datos personales.

3) Establecer procedimientos para la gestión y trámite de las solicitudes de derechos ARCO.

4) Nombrar al oficial de protección de datos personales.

Cronograma de actividades del eje 2

	Año 2025		Año 2026	
Acción	Semestre 1	Semestre 2	Semestre 1	Semestre 2
1	**x**			
2	**x**			
3	**x**			**x**
4	**x**			

Eje 3: Deber de Seguridad y Confidencialidad

Objetivo General.

Establecer controles o mecanismos de observancia obligatoria para garantizar el adecuado tratamiento de los datos personales.

Objetivo particular.

Que las dependencias universitarias adopten e instrumenten medidas físicas en atención a los controles o mecanismos de observancia obligatoria que se implementen para garantizar el adecuado tratamiento de los datos personales.

Acciones

1) Generar el aviso de privacidad integral y simplificado en las dependencias universitarias que traten datos personales.

2) Establecer mecanismos de control y acceso a las bases de datos físicas o electrónicas en las que se concentren datos personales.

3) Establecer procedimientos para el adecuado tratamiento de datos personales.

4) Vigilar que los datos personales únicamente se traten de acuerdo a las finalidades informadas en el aviso de privacidad.

Cronograma de actividades del eje 3

	Año 2025		Año 2026	
Acción	Semestre 1	Semestre 2	Semestre 1	Semestre 2
1	x			
2	x			
3	x			

4		x		x

Eje 4: Tratamiento adecuado de Datos Personales

Objetivo General.

Garantizar el adecuado tratamiento de datos personales de la comunidad universitaria.

Objetivo particular.

Que las dependencias universitarias realicen un tratamiento adecuado de datos personales observando los principios de licitud, calidad, finalidad, proporcionalidad, lealtad, información, consentimiento y responsabilidad.

Acciones

1) Verificar que los avisos de privacidad informen todas las finalidades para las cuales se tratan los datos personales y que se describan de manera clara.

2) Recabar el consentimiento de los y las titulares para el tratamiento de datos personales, cuando el mismo se requiera.

3) Informar todas las finalidades del tratamiento que se describe en el aviso de privacidad.

4) Poner a disposición en el portal de Internet institucional, los avisos de privacidad de las dependencias universitarias que traten datos personales.

5) Familiarizar en las dependencias universitarias el contenido de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Cronograma de actividades del eje 4

	Año 2025		Año 2026	
Acción	Semestre 1	Semestre 2	Semestre 1	Semestre 2

1	X	X	X	X
2		X	X	
3		X		X
4	X		X	
5	X			

Actualización del documento de seguridad.

El artículo 36 de la Ley General establece la obligación de la actualización del documento de seguridad cuando ocurran los siguientes eventos:

I. Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;

II. Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;

III. Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida, y

IV. Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

En ese sentido, el Comité de Transparencia deberá estar atento a la actualización de alguno de los supuestos antes citado, para, en su caso, actualizar el presente documento de seguridad.

Hasta el momento, no se ha realizado la actualización del documento de seguridad porque no se han configurado las hipótesis necesarias.