DOCUMENTO DE SEGURIDAD

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 Ley General), 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.

La Ley General señala en su artículo primero, que son sujetos obligados en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, **órganos autónomos**, partidos políticos, fideicomisos y fondos públicos.

En ese sentido, la **Universidad Autónoma Chapingo** es sujeto obligado de la Ley General y, por ello, debe observar lo dispuesto por dicho instrumento normativo en el tratamiento de datos personales que lleve a cabo.

De acuerdo con lo dispuesto por los artículos 29 y 30, fracciones I y VII de la Ley General, la UACh deberá implementar mecanismos para acreditar el cumplimiento de los principios, deberes y obligaciones establecidos en dicha legislación. La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados dispone que el tratamiento de datos personales que realicen los sujetos obligados estará regido por ocho principios y dos deberes. Los ocho principios son: licitud, lealtad, información, consentimiento, finalidad, proporcionalidad, calidad y responsabilidad; mientras que los dos deberes son el de confidencialidad y seguridad. Estos principios, deberes y derechos imponen una serie de obligaciones para los sujetos regulados por la Ley General, cuya finalidad es que el tratamiento se realice garantizando la protección de los datos personales, con el objeto de respetar el derecho a la autodeterminación informativa de los titulares.

Asimismo, la Ley General detalla el alcance y los procedimientos para el ejercicio de los cuatro derechos que el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos reconoce a los titulares de los datos personales: acceso, rectificación, cancelación y oposición (derechos ARCO), y reconoce uno más, el de portabilidad.

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 (en los sucesivo Lineamientos Generales) cuyo objetivo es desarrollar las disposiciones previstas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados 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 Protección de Datos Personales en Posesión de Sujetos Obligados 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.

Al respecto, el artículo 33 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados señala lo siguiente:

> ***Artículo 33.*** *Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:*
>
> ***I.*** *Crear políticas internas para la gestión y tratamiento de los datos personales, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión;*
>
> ***II.*** *Definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales;*
>
> ***III.*** *Elaborar un inventario de datos personales y de los sistemas de tratamiento;*
>
> ***IV.*** *Realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros;*
>
> ***V.*** *Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable;*
>
> ***VI.*** *Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales;*

VII. *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, y*

VIII. *Diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.*

Por su parte, el artículo 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados establece como una obligación la elaboración de un documento de seguridad, que se define de acuerdo a 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.

De conformidad con el artículo 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, el documento 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 Chapingo con los elementos informativos que establece el artículo 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

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.

Sobre el particular, los artículos 58 y 59 de los Lineamientos Generales establecen lo siguiente:

Inventario de datos personales

Artículo 58. *Con relación a lo previsto en el artículo 33, fracción III de la Ley General, el responsable deberá elaborar un inventario con la información básica de cada tratamiento de datos personales, considerando, al menos, los siguientes elementos:*

- ***I.*** *El catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales;*
- ***II.*** *Las finalidades de cada tratamiento de datos personales;*
- ***III.*** *El catálogo de los tipos de datos personales que se traten, indicando si son sensibles o no;*
- ***IV.*** *El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales;*
- ***V.*** *La lista de servidores públicos que tienen acceso a los sistemas de tratamiento;*
- ***VI.*** *En su caso, el nombre completo o denominación o razón social del encargado y el instrumento jurídico que formaliza la prestación de los servicios que brinda al responsable, y*
- ***VII.*** *En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que justifican éstas.*

Ciclo de vida de los datos personales en el inventario de éstos

Artículo 59. *Aunado a lo dispuesto en el artículo anterior de los presentes Lineamientos generales, en la elaboración del inventario de datos personales el responsable deberá considerar el ciclo de vida de los datos personales conforme lo siguiente:*

- ***I.*** *La obtención de los datos personales;*
- ***II.*** *El almacenamiento de los datos personales;*
- ***III.*** *El uso de los datos personales conforme a su acceso, manejo, aprovechamiento, monitoreo y procesamiento, incluyendo los sistemas físicos y/o electrónicos utilizados para tal fin;*
- ***IV.*** *La divulgación de los datos personales considerando las remisiones y transferencias que, en su caso, se efectúen;*
- ***V.*** *El bloqueo de los datos personales, en su caso, y*
- ***VI.*** *La cancelación, supresión o destrucción de los datos personales.*

El responsable deberá identificar el riesgo inherente de los datos personales, contemplando su ciclo de vida y los activos involucrados en su tratamiento, como podrían ser hardware, software, personal, o cualquier otro recurso humano o material que resulte pertinente considerar.

En referencia de lo anterior, la Universidad Autónoma Chapingo se encuentra en la etapa de elaboración de los inventarios de los distintos tratamientos de datos personales que realiza, identificando los elementos informativos que señala el artículo 58 de los Lineamientos Generales, aunado a esto y respecto al ciclo de vida de los datos personales, la UACh se encuentra realizando acciones para dar cumplimiento a lo establecido en la Ley General de Archivos, y crear un catálogo de disposición documental, por tanto, será necesario actualizar la información en cada inventario en tanto el Grupo Interdisciplinario ponga en marcha los instrumentos para la clasificación documental, con la finalidad de dar cumplimiento como lo requiere el artículo 59 de los Lineamientos Generales.

Los inventarios forman parte integral del presente documento de seguridad y se encuentran contenidos en el **Anexo 1**.

Con independencia de lo anterior, el siguiente cuadro muestra un resumen de los inventarios elaborados:

Subdirección o Departamento	**Área**	**Denominación del Inventario de Tratamiento de Datos Personales**
Departamento de Relaciones Públicas	Relaciones Públicas	Ubicación del alumnado egresado en una vacante ofertada en la plataforma de bolsa de trabajo.
Unidad de Transparencia	Unidad de Transparencia	Solicitudes de Información, Solicitudes de derechos ARCO. Trámite de solicitudes de acceso y de protección de datos personales.
Contraloría	Departamento de Normatividad	Registro y seguimiento de la evolución de la situación patrimonial de los funcionarios de la UACh.
		Sistema Denuncia en línea
Subdirección de Administración Escolar	Servicios Escolares	Tramite de Examen Profesional y/o Grado con la finalidad de obtener un grado académico. Autenticación y validación de documentos.
Subdirección de Administración Escolar	Admisión, Promoción y Becas	Selección de aspirantes al Nivel Medio Superior
		Expedición de constancias
Subdirección de Administración Escolar	UCAME	Atención Psicológica.
		Atención Psicopedagógica.
		Atención Disciplinaria.
		Programas Educativos y Comunicación Social.
Subdirección de Apoyo Académico	Intercambio Académico	Intercambio Académico con movilidad entrante y saliente de estudiantes Nacionales e Internacionales.
Subdirección de Apoyo Académico	Centro de Idiomas	Inscripción a cursos de idiomas.
		Emisión de constancias de cursos de idiomas aprobados.

Subdirección o Departamento	Área	Denominación del Inventario de Tratamiento de Datos Personales
		Cumplimiento de requisito de idioma para educación superior y posgrado.
		Emisión de constancias de revisión de resúmenes de tesis para posgrado.
		Registro y aplicación del examen TOEFL ITP
Subdirección de Investigación y Servicios	CEC	Inscripción a los servicios de capacitación que ofrece el CEC.
		Evaluación y Certificación de competencias laborales
		Titulación
Subdirección Recursos Humanos	Desarrollo Humano	Procesamiento de información
		Trámites de Prestaciones
		Trámites de Prótesis
		Trámites de Seguros
		Fondo de ahorro para el retiro
Subdirección de Recursos Humanos	Departamento de Personal (Oficina de Empleo)	Proceso de Ingreso y Movimientos Escalafonarios
Subdirección de Recursos Humanos	Área de plantilla	Actualización de la plantilla del personal académico, administrativo y mandos medios y superiores de la Universidad.
Subdirección de Recursos Humanos	Oficina de contratación	Reclutamiento, selección e inducción del personal para su contratación y movimientos escalafonarios.
Subdirección de Recursos Humanos	Relaciones Laborales	Administración de los Sistemas de Capacitación para el fortalecimiento al desempeño, actualización y desarrollo de los trabajadores administrativos, y de funcionarios de la UACh.
		Recabación de datos para revisiones preventivas CLIDDA-ISSSTE.

Subdirección o Departamento	Área	Denominación del Inventario de Tratamiento de Datos Personales
Subdirección de Servicios Asistenciales	Servicio Médico	Registro para atención médica preventiva y transferencia para atención del IMSS
Subdirección de Servicios Asistenciales	CDI	Admisión, estancia y termino de estudios de nivel preescolar
		Atención médica
		Atención de Psicología Preventiva
Subdirección de Servicio y Extensión	Servicio Social	Gestión de aceptación y liberación de Servicio Social
Subdirección de Difusión Cultural	Concurso de cuentos campiranos	Registro de participación de Cuentos Campiranos
Subdirección de Difusión Cultural	Talleres Culturales	Registro de inscripción a Talleres Culturales
	Órgano Interno de Control	Declaraciones patrimoniales
	Jurídico	Integración de expedientes
	Dirección General de Investigación y Posgrado	Registro de aspirantes y alumnos

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, este elemento informativo forma parte del documento de seguridad.

Sobre el particular, el artículo 57 de los Lineamientos Generales señala lo siguiente:

> ***Funciones y obligaciones***
> ***Artículo 57.*** *Con relación a lo dispuesto en el artículo 33, fracción II de la Ley General, el responsable deberá establecer y documentar los roles y responsabilidades, así como la cadena de rendición de cuentas de todas las personas que traten datos personales en su organización, conforme al sistema de gestión implementado.*
>
> *El responsable deberá establecer mecanismos para asegurar que todas las personas involucradas en el tratamiento de datos personales en su organización conozcan sus funciones para el cumplimiento de los objetivos del sistema de gestión, así como las consecuencias de su incumplimiento.*

De conformidad con lo anterior, las funciones y obligaciones del personal de la UACh que trata datos personales se han identificado a nivel de servidor público, a través de los inventarios que se desarrollaron por cada uno de los tratamientos, en los cuales se identificó el personal que realiza el tratamiento, el área al que está adscrito y la finalidad de dicho tratamiento.

El Programa de Protección de Datos Personales forma parte integral de este documento de seguridad y se encuentra en el **Anexo 2**.

Por su parte, el inventario de tratamientos contiene las siguientes columnas, en las cuales se identifican las funciones del personal que interviene en el tratamiento de los datos personales:

Servidores públicos que tienen acceso a la base de datos (15)	*Área de adscripción (16)*	*Finalidad del acceso (17)*
Señalar los puestos de los servidores públicos que tienen acceso a la base de datos del tratamiento correspondiente. Uno por fila.	*Definir unidad administrativa a la que está adscrito el puesto*	*Señalar con qué fines tienen acceso los servidores públicos antes identificados. Uno por fila, según corresponda.*

Cabe señalar que la cadena de rendición de cuentas del personal se define en el análisis de riesgo respectivo.

Asimismo, el Comité de Transparencia es el área responsable de dar a conocer a las personas servidoras públicos de la UACh el Programa de Protección de Datos Personales, que se basa en un sistema de gestión, a fin de que el personal conozca sus funciones para el cumplimiento del sistema de gestión y las consecuencias de su incumplimiento.

Adicionalmente, conviene señalar que las funciones y obligaciones del personal que traten datos personales se encuentran definidas en la normatividad que rige el actuar de la UACh, por lo cual, para efectos del presente documento de seguridad, el marco normativo de referencia se encuentra establecido en el Manual de Organización de las áreas administrativas que integran la Universidad Autónoma Chapingo.

III, IV y V. Análisis de riesgos, análisis de brecha y Plan de Trabajo.

El artículo 33, fracciones IV, V y VI 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 realización del análisis de riesgo, análisis de brecha y plan de trabajo, en los siguientes términos:

> ***Artículo 33.*** *Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:*
>
> ***I.*** *[…]*
>
> ***IV.*** *Realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros;*
>
> ***V.*** *Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable;*
>
> ***VI.*** *Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales;*
>
> *[…]*

Como se señaló, de acuerdo con las fracciones III, IV y V del artículo 35 de la Ley General, los análisis de riesgo y brecha y el plan de trabajo forman parte del documento de seguridad.

Por su parte, los artículos 60, 61 y 62 de los Lineamientos Generales establecen lo siguiente:

> ***Análisis de riesgos***
> ***Artículo 60.*** *Para dar cumplimiento al artículo 33, fracción IV de la Ley General, el responsable deberá realizar un análisis de riesgos de los datos personales tratados considerando lo siguiente:*
>
> ***I.*** *Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico;*
>
> ***II.*** *El valor de los datos personales de acuerdo a su clasificación previamente definida y su ciclo de vida;*

III. *El valor y exposición de los activos involucrados en el tratamiento de los datos personales;*
IV. *Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida, y*
V. *Los factores previstos en el artículo 32 de la Ley General.*

Análisis de brecha
Artículo 61. *Con relación al artículo 33, fracción V de la Ley General, para la realización del análisis de brecha el responsable deberá considerar lo siguiente:*

I. *Las medidas de seguridad existentes y efectivas;*
II. *Las medidas de seguridad faltantes, y*
III. *La existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente.*

Plan de trabajo
Artículo 62. *De conformidad con lo dispuesto en el artículo 33, fracción VI de la Ley General, el responsable deberá elaborar un plan de trabajo que defina las acciones a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes e inmediatas a establecer.*

Lo anterior, considerando los recursos designados; el personal interno y externo en su organización y las fechas compromiso para la implementación de las medidas de seguridad nuevas o faltantes.

Por su parte, el artículo 32 de la Ley General, citado en la fracción V del artículo 60 de los Lineamientos Generales, dispone lo siguiente:

> ***Artículo 32.*** *Las medidas de seguridad adoptadas por el responsable deberán considerar:*
>
> *I. El riesgo inherente a los datos personales tratados;*
>
> *II. La sensibilidad de los datos personales tratados;*
> *III. El desarrollo tecnológico;*
> *IV. Las posibles consecuencias de una vulneración para los titulares;*
> *V. Las transferencias de datos personales que se realicen;*
> *VI. El número de titulares;*
> *VII. Las vulneraciones previas ocurridas en los sistemas de tratamiento, y*
> *VIII. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.*

A partir de lo dispuesto por los artículos antes citados, el análisis de riesgo se lleva a cabo a partir de cuatro fuentes de información:

1. Análisis de riesgos de la infraestructura tecnológica y recursos de software y hardware;
2. Análisis de riesgos de hábitos de seguridad del personal de la UACh;
3. Análisis de riesgos a partir de los inventarios de tratamientos de datos personales, y
4. Análisis de riesgos vinculado con el cumplimiento de obligaciones normativas en materia de datos personales.

Los dos primeros análisis se realizan de manera general y aplican transversalmente, ya que el primero refiere a los distintos sistemas o medios en los que se llevan a cabo los diversos tratamientos que realiza el Instituto, por lo que los riesgos y controles que se determinen aplican de manera directa a estos medios o sistemas; mientras que el segundo versa sobre los hábitos de seguridad del personal, de manera general y no asociados a un tratamiento en lo particular.

Por su parte, los análisis 3 y 4 se realizan, de manera específica, asociados a cada uno de los tratamientos, y tomando en cuenta sus particularidades.

Los elementos requeridos en los artículos 33, fracción IV, de la Ley General y 60 de los Lineamientos Generales se atienden de la siguiente forma:

Elemento requerido	Fundamento
Tomar en cuenta amenazas y vulnerabilidades existentes.	33, fracción IV, de la Ley General.
Tomar en cuenta los recursos involucrados.	33, fracción IV, de la Ley General.
Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico.	60, fracción I, de los Lineamientos Generales.
El valor de los datos personales de acuerdo a su clasificación previamente definida y su ciclo de vida.	60, fracción II, de los Lineamientos Generales.
El valor y exposición de los activos involucrados en el tratamiento de los datos personales	60, fracción III, de los Lineamientos Generales.
Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida.	60, fracción IV, de los Lineamientos Generales.
El riesgo inherente a los datos personales tratados.	32, fracción I, de la Ley General.
La sensibilidad de los datos personales tratados.	32, fracción II, de la Ley General.
El desarrollo tecnológico.	32, fracción III, de la Ley General.
Las posibles consecuencias de una vulneración para los titulares.	32, fracción IV, de la Ley General.
Las transferencias de datos personales que se realicen.	32, fracción V, de la Ley General.
El número de titulares.	32, fracción VI, de la Ley General.
Las vulneraciones previas ocurridas en los sistemas de tratamiento.	32, fracción VII, de la Ley General.
El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.	32, fracción VIII, de la Ley General.

El proceso del análisis de riesgos se encuentra definido en el **Documento de Seguridad como base para el Sistema de Gestión de Protección de Datos Personales (SGPDP) de la UACh"**, se encuentra en el **Anexo 6**.

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.

Como se señaló, de acuerdo con la fracción VI del artículo 35 de la Ley General, los mecanismos de monitoreo y revisión forman parte del documento de seguridad.

Así, respecto a los mecanismos de monitoreo y revisión de las medidas de seguridad, el artículo 63 de los Lineamientos Generales señala lo siguiente:

> ***Monitoreo y supervisión periódica de las medidas de seguridad implementadas***
> ***Artículo 63.*** *Con relación al artículo 33, fracción VII de la Ley General, el responsable deberá evaluar y medir los resultados de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales, a fin de verificar el cumplimiento de los objetivos propuestos y, en su caso, implementar mejoras de manera continua.*
>
> *Para cumplir con lo dispuesto en el párrafo anterior del presente artículo, el responsable deberá monitorear continuamente lo siguiente:*
>
> ***I.*** *Los nuevos activos que se incluyan en la gestión de riesgos;*
> ***II.*** *Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras;*
> ***III.*** *Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas;*
> ***IV.*** *La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;*

V. *Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;*

VI. *El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo, y*

VII. *Los incidentes y vulneraciones de seguridad ocurridas.*

Aunado a lo previsto en las fracciones anteriores del presente artículo, el responsable deberá contar con un programa de auditoría, interno y/o externo, para monitorear y revisar la eficacia y eficiencia del sistema de gestión.

De lo anterior es posible identificar que el monitoreo y revisión de las medidas de seguridad tiene el objetivo de fortalecer la protección de los datos personales que resguarda la UACh.

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

Mecanismos de Monitoreo

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

1) **Revisión de cumplimiento de las políticas internas de la UACh, relacionadas con el tratamiento de datos personales.** Tiene el objetivo de asegurar que las personas servidoras públicas realicen los tratamientos de datos personales en concordancia con lo dispuesto en la Ley General, los Lineamientos Generales, y demás normatividad que resulte aplicable.

   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 los accesos a la UACh, (II) control de acceso del personal académico, administrativo y alumnado con tarjeta de proximidad a sistemas de acceso, (III) control de acceso a través de bitácoras para visitantes, proveedores, vendedores, y toda persona ajena a la Institución (IV) control de asistencia a través de datos biométricos (huella digital, reconocimiento de rostro) y (V) circuito cerrado de cámaras de vigilancia.
b. **Monitoreo del entorno electrónico.** Para la detección continua de amenazas y vulnerabilidades, el Centro de Cómputo Universitario y las áreas de sistema de los departamentos generales y de enseñanza, implementarán herramientas automatizadas de monitoreo de activos, así como con bitácoras de los sistemas informáticos de la UACh.
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. Estos cambios se pondrán a consideración del área que apoya en el análisis de riesgos, Centro de Cómputo Universitario, áreas de sistemas y el Comité de Transparencia.
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, se hará una revisión de 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.
f. **Vulneraciones a la seguridad de los datos personales.** En caso de identificar un incidente de seguridad que involucre datos personales, el área que apoya en el análisis de riesgos, Centro de Cómputo Universitario, área de sistemas y el Comité de Transparencia se coordinarán para decidir sobre las acciones pertinentes para mitigar dicho incidente.

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 internas de la UACh, 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.	1. Revisión de cumplimiento de las políticas internas de la UACh, relacionadas con el tratamiento de datos personales.
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.	1. Revisión de cumplimiento de las políticas internas de la UACh, relacionadas con el tratamiento de datos personales. 2.a. Monitoreo del entorno físico. 2.b. Monitoreo del entorno electrónico.
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 internas de la UACh, relacionadas con el tratamiento de datos personales. 2.a. Monitoreo del entorno físico. 2.b. Monitoreo del entorno electrónico.
Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;	63, fracción V, de los Lineamientos Generales.	1. Revisión de cumplimiento de las políticas internas de la UACh, relacionadas con el tratamiento de datos personales. 2.a. Monitoreo del entorno físico. 2.b. Monitoreo del entorno electrónico.
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 internas de la UACh, relacionadas con el tratamiento de datos personales. 2.c. Actualización del plan de trabajo. 2.d. 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 políticas internas de la UACh, relacionadas con el tratamiento de datos personales. 2.f. Vulneraciones a la seguridad de los datos personales.

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 (desarrolladas por la UACh) o externas (solicitada al INAI o realizando una contratación o a través de un convenio con un tercero).

Hasta el momento no se han realizado auditorías en materia de protección de datos personales a los tratamientos de la UACh.

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 internamente por personal de la UACh, 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 de la UACh.

Los resultados de las auditorías se considerarán para realizar adecuaciones al análisis de riesgos de la UACh y, por lo tanto, al plan de trabajo.

VII. El programa general de capacitación

Con relación al programa de capacitación, la fracción VIII del artículo 33 de la Ley General señala que, para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.

Como se señaló, de acuerdo con la fracción VII del artículo 35 de la Ley General, el programa de capacitación forma parte del documento de seguridad.

Por su parte, el artículo 64 de los Lineamientos Generales señala lo siguiente:

> ***Capacitación***
> ***Artículo 64.*** *Para el cumplimiento de lo previsto en el artículo 33, fracción VIII de la Ley General, el responsable deberá diseñar e implementar programas a corto, mediano y largo plazo que tengan por objeto capacitar a los involucrados internos y externos en su organización, considerando sus roles y responsabilidades asignadas para el tratamiento y seguridad de los datos personales y el perfil de sus puestos.*
>
> *En el diseño e implementación de los programas de capacitación a que se refiere el párrafo anterior del presente artículo, el responsable deberá tomar en cuenta lo siguiente:*
>
> ***I.*** *Los requerimientos y actualizaciones del sistema de gestión;*
> ***II.*** *La legislación vigente en materia de protección de datos personales y las mejores prácticas relacionadas con el tratamiento de éstos;*
> ***III.*** *Las consecuencias del incumplimiento de los requerimientos legales o requisitos organizacionales, y*
> ***IV.*** *Las herramientas tecnológicas relacionadas o utilizadas para el tratamiento de los datos personales y para la implementación de las medidas de seguridad.*

A partir de lo anterior, la Universidad Autónoma Chapingo, se encuentra desarrollando su programa general de capacitación, mismo que integra en sus avances en el **Anexo 5** de este documento de seguridad.

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.

Km 38.5 carretera México – Texcoco.
Texcoco, Estado de México.
C.P. 56130