GOBIERNO DE MÉXICO | CONAHCYT CONSEJO NACIONAL DE HUMANIDADES CIENCIAS Y TECNOLOGÍAS | CIATEQ

CIATEQ, A.C. Centro de Tecnología Avanzada.

DOCUMENTO DE SEGURIDAD
Versión Pública

Índice

Introducción.

CIATEQ A.C., Centro de Tecnología Avanzada, en adelante "CIATEQ" es una Asociación constituida mediante escritura pública número 19,276 de fecha 9 de noviembre de 1978, cuenta con personalidad jurídica y patrimonio propio. Tiene su domicilio fiscal en Avenida del Retablo, número 150, Colonia Constituyentes FOVISSSTE, C.P. 76150, en la Ciudad de Santiago de Querétaro, Estado de Querétaro; y cuenta con sedes establecidas en los Estados de Aguascalientes, Estado de México, Hidalgo, Jalisco, Querétaro, San Luis Potosí y Tabasco.

Es un Centro Público de Investigación Humanística y Científica, Desarrollo Tecnológico e Innovación, perteneciente al Sistema Nacional de Centros Públicos del Consejo Nacional de Humanidades, Ciencias y Tecnologías (CONAHCYT), con autonomía técnica y de gestión, de conformidad con los artículos 4, fracción IV, 75, 81, 82, 84 y 91 de la Ley General en Materia de Humanidades, Ciencias, Tecnologías e Innovación. Además; reconocida como Entidad Paraestatal asimilada al régimen de las Empresas de Participación Estatal Mayoritaria a que se refieren la Ley Orgánica de la Administración Pública Federal y la Ley Federal de las Entidades Paraestatales.

Tiene por objeto entre otros, realizar actividades de investigación y desarrollo tecnológico en el área manufactura avanzada; sistemas mecánicos; procesos de manufactura, diseño y desarrollo de productos; ingeniería y construcción de plantas; plásticos y materiales avanzados; sistemas de medición; telecomunicaciones; tecnologías de la información, control y electrónica; ingeniería virtual, confiabilidad y disciplinas afines.

De acuerdo con lo estipulado en la Constitución Política de los Estados Unidos Mexicanos, en su artículo 6, Apartado A, fracciones I y II, la información en posesión del "CIATEQ" se regirá por el principio de máxima publicidad, mientras que los datos personales serán protegidos según lo establecido por las leyes aplicables. En cumplimiento con la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, que establece las bases, principios y procedimientos para garantizar el derecho de protección de los datos personales, el CIATEQ se compromete a los principios de accesibilidad, transparencia, objetividad e independencia.

En cuanto al deber de seguridad, el artículo 31 de la Ley General indica que el responsable del tratamiento de datos personales deberá 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.

En relación con lo anterior, el artículo 33 señala que, 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.

Asimismo, en el artículo 35 de la Ley General se establece la obligación de elaborar un documento de seguridad, que de acuerdo con lo dispuesto en el artículo 3, fracción XIV, se define como:

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.

Mismo que de conformidad con lo establecido en el artículo 35 de la Ley General, deberá contener 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.

En virtud de lo anterior, el "CIATEQ" elabora el presente documento de seguridad, atendiendo los requisitos previstos en el artículo 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

I. Inventario de datos personales y sistemas de tratamiento.

De acuerdo con lo previsto en los artículos 33, fracción III y 35 de la Ley General, el responsable debe elaborar un inventario de datos personales y de los sistemas de tratamiento, para implementar y mantener medidas de seguridad para la protección de los datos personales; mismo que forma parte del documento de seguridad.

Los artículos 58 y 59 de los Lineamientos, 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.

Tomando en cuenta lo establecido en los artículos referidos, el "CIATEQ" implementó un cuestionario de 13 preguntas, mismo que se transcribe a continuación:

Cuestionario		
Indicaciones: Previa identificación de los procesos que se llevan a cabo en su área, favor de contestar las siguientes preguntas:		
No.	**Interrogante**	**Indicación y/o aclaración**
1.	¿A qué datos personales da tratamiento?	(Identificar si son datos personales y/o datos personales sensibles)
2.	¿De qué forma se obtienen?	(Indicar si se obtienen de forma física o por medios electrónicos)
3.	¿En qué formatos se encuentran? Descripción general de su ubicación.	(Carpetas, estantes, discos, archiveros, equipos de cómputo, en la nube, etc.)
4.	Para llevar a cabo sus funciones, ¿solicitan algún documento a los titulares de datos personales?	
5.	¿Cuáles son las finalidades del tratamiento?	(Respecto de los datos personales en cada uno de los procesos)
6.	¿Cómo procesan la información?	(Desde que se obtiene hasta que ya no se utiliza)
7.	¿Qué personas tienen acceso a los datos personales o Sistema de tratamiento?	(Sistema de tratamiento: Conjunto de elementos mutuamente relacionados o que interactúan para realizar la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, transferencia o disposición de datos personales, en medios físicos o electrónicos)
8.	¿Quiénes dan tratamiento a los datos personales?	(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.)
9.	¿Se realizan transferencias de datos personales?	(Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado). En caso afirmativo, describir a quién se realizan y la finalidad de las mismas.
10.	¿Se realiza remisión de datos personales?	En caso afirmativo, describir a quién se realizan y la finalidad de las mismas.
11.	¿En qué momento deja de tener utilidad la información a que se da tratamiento? Una vez que deja de tener utilidad, ¿qué hacen con la información?, ¿es destruida (físico) o eliminada (electrónico)?	
12.	¿Cuentan con medidas de seguridad para resguardar los datos personales?	

A partir de la respuesta a dicho cuestionario por parte de las áreas, se realizaron los inventarios de los distintos tratamientos de datos personales que se realizan al interior del "CIATEQ"; a continuación, se muestra un resumen de los inventarios elaborados:

Dirección General			
No.	**Áreas**	**No. De procesos**	**Nombre del tratamiento**
1	Posgrados	5	1. Registro de aspirantes en proceso de admisión; 2. Integración del expediente académico del estudiante; 3. Otorgamiento de acceso a los sistemas del Centro; 4. Integración de expediente para instancias educativas; 5. Integración de informes dirigidos a instancias fiscalizadoras.

Dirección Administrativa.			
No.	**Áreas**	**No. De procesos**	**Nombre del tratamiento**
1	Subdirección de Recursos financieros	5	1. Verificación de identidad de clientes (Personas físicas); 2. Verificación de legal constitución (Personas morales); 3. Registro de clientes en padrón interno; 4. Integración de informes dirigidos a instancias fiscalizadoras. 5. Emisión de comprobantes fiscales. 6. Integración de expedientes de cobranza extrajudicial.
2	Subdirección de Recursos Humanos	4	1. Integración de expediente del personal con vínculo laboral; 2. Integración de expediente del personal sin vínculo laboral; 3. Registro del personal ante instancias fiscalizadoras; 4. Integración de expediente del personal para clientes; 5. Otorgamiento de credencial de acceso a instalaciones; 6. Integración de informes dirigidos a instancias fiscalizadoras.
3	Jefatura de Servicios Generales	3	1. Registro de control de accesos a las instalaciones; 2. Verificación de vigencias de derechos de prestadores de servicio social y practicas profesionales; 3. Verificación de vigencias de derechos del personal de proveedores o contratistas; 4. Integración de informes dirigidos a instancias fiscalizadoras.
4	Gerencia de Insumos a proyectos	3	1. Registro de licitantes, proveedores y prestadores de servicios en el padrón interno; 2. Revisión de expedientes de licitantes; 3. Formalización de pedidos o contratos derivados de los procedimientos de contratación;

Dirección de Gestión Institucional.			
No.	**Áreas**	**No. De procesos**	**Nombre del tratamiento**
1	Gerencia de Vinculación	6	III. Verificación de identidad de clientes (Personas físicas); IV. Verificación de legal constitución (Personas morales); V. Registro de clientes en padrón interno; VI. Integración de informes dirigidos a instancias fiscalizadoras; VII. Registro de asistentes a actividades de divulgación; VIII. Registro de autorizaciones para el uso de imagen personal en fotografías y videos usados en archivos promocionales.

Total	**26 PROCESOS IDENTIFICADOS.**

II. Funciones y obligaciones de las personas que traten datos personales

De acuerdo con lo previsto en el artículo 33, fracción II de la Ley General, el responsable debe definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales, para implementar y mantener medidas de seguridad para la protección de los datos personales; mismo que forma parte del documento de seguridad.

El artículo 57 de los Lineamientos, establece 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.

Tomando en cuenta lo establecido en el artículo referido, las funciones y obligaciones del personal del "CIATEQ"; que trata datos personales se han identificado en dos niveles:

I. De manera general, a través de la implementación del Programa de Protección de Datos Personales, en el cual se describirán todas las obligaciones que establece la Ley General y los Lineamientos Generales y éstas se asociaron con el área responsable de su cumplimiento, y

II. De forma específica, a través de los inventarios que se desarrollaron por cada uno de los tratamientos de datos personales por unidad administrativa, en los cuales se identificó el personal que, conforme a sus facultades y atribuciones realiza el tratamiento de datos personales, así como la finalidad de dicho tratamiento.

A continuación, se muestra un ejemplo de cómo se identifican las funciones y obligaciones a nivel macro en el Programa de Protección de Datos Personales, por cada una de las obligaciones que establecen la Ley General y los Lineamientos:

Obligaciones	Actividades para su cumplimiento	Unidades administrativas responsables del cumplimiento	Medios que facilitan la acreditación del cumplimiento
Sujetar el tratamiento de los datos personales a las atribuciones o facultades que la normatividad aplicable confiera al sujeto obligado, así como con estricto apego y cumplimiento de lo dispuesto en dicho ordenamiento, los Lineamientos Generales, la legislación mexicana que le resulte aplicable y, en su caso, el derecho internacional, respetando los derechos y libertades de los titulares	1. Identificar el marco normativo (leyes, tratados o acuerdos internacionales, reglamentos, lineamientos, entre otros, con sus respectivos artículos) que faculta a la unidad administrativa a tratar los datos personales para cada una de las finalidades, y aquél que regula el tratamiento respectivo.	Todas las unidades administrativas que realicen tratamiento de datos personales.	Marco normativo respectivo.

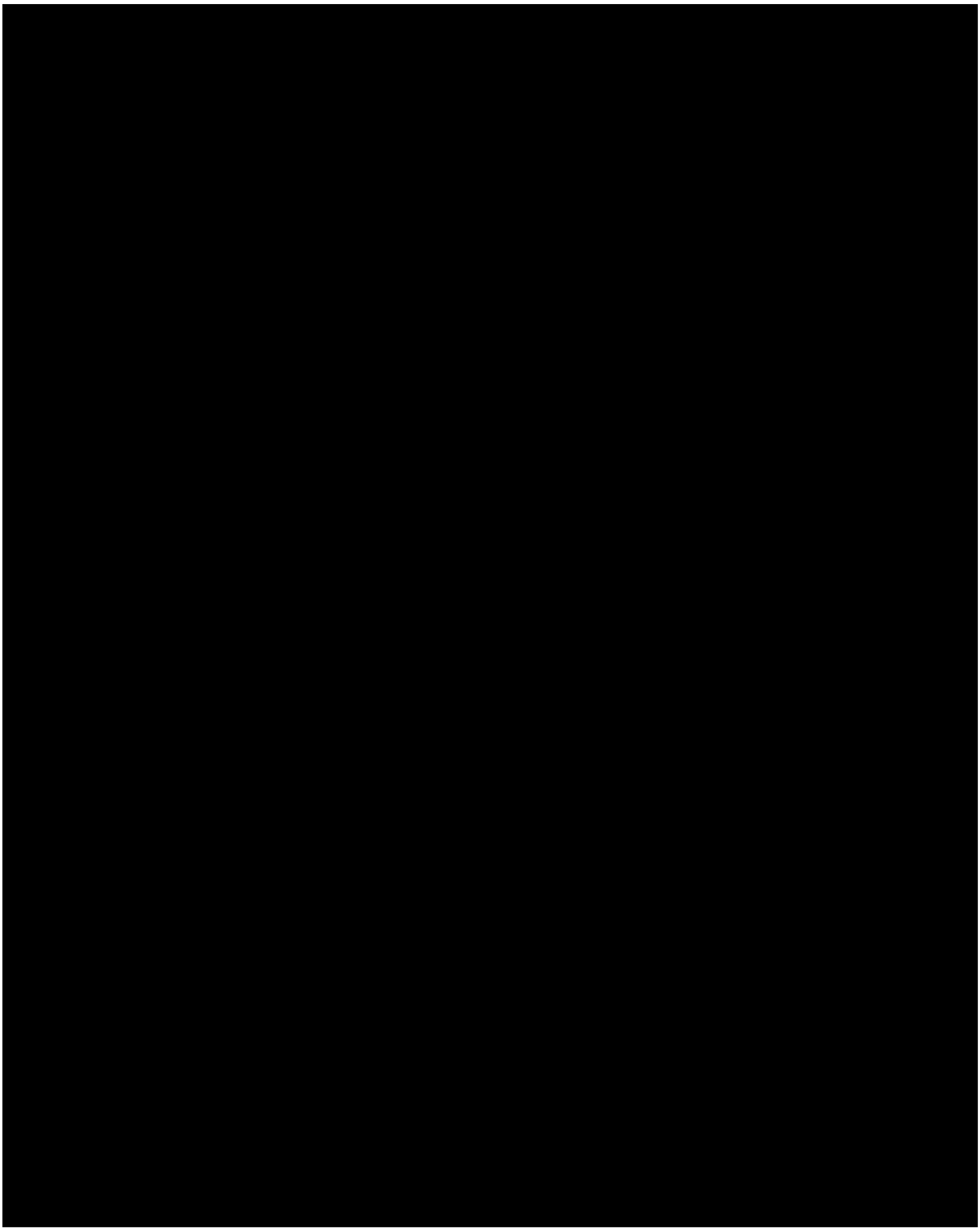
III. Análisis de riesgo.

[redacted]

IV. Análisis de brecha

[redacted]

V. Plan de trabajo.



[redacted]

Cronograma General

[redacted]

VI. Proceso General Para el Establecimiento, Actualización, Monitoreo y Revisión de Los Mecanismos y 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 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, a través de un ciclo de mejora continua, la protección de los datos personales que resguarda este Sujeto Obligado.

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

I. Mecanismos de Monitoreo**.**

Para los tratamientos de datos personales del **"CIATEQ"**, 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 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 las instalaciones del "CIATEQ", (II) control de acceso del personal con credencial laboral vigente, (III) control de acceso a través de bitácoras para visitantes y personal del "CIATEQ" que olvidó su credencial, (IV) control de asistencia a través listas, y (V) Control de acceso sólo a personal autorizado a Centros de Datos y Comunicaciones propios o arrendados.

   b. **Monitoreo del entorno electrónico**. Para la detección continua de amenazas y vulnerabilidades, la Gerencia de Cómputo y Comunicaciones, cuenta con herramientas automatizadas de monitoreo (activo y pasivo), así como con bitácoras de los sistemas informáticos, bases de datos y configuraciones de los componentes.

   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 de la Unidad de Transparencia, la Gerencia de Cómputo y Comunicaciones y el Comité de Transparencia.

d. **Revisión de avances del plan de trabajo**. A través de los mecanismos que determine la Unidad de Transparencia, la Gerencia de Cómputo y Comunicaciones y 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 de manera anual una actualización del análisis de riesgo, análisis de vulnerabilidades 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, la Unidad de Transparencia, la Gerencia de Cómputo y Comunicaciones y el Comité de Transparencia se coordinarán para decidir sobre las acciones pertinentes para mitigar dicho incidente.

II. Mecanismos de Supervisión y Revisión

Además del monitoreo continuo de las medidas de seguridad, se requiere realizar una supervisión periódica de las mismas, a través de auditorías las cuales pueden ser realizadas de manera interna; desarrolladas por el propio Centro o en su caso por el Órgano Interno de Control Específico del CONAHCYT; o bien de forma externa, a través de la contratación de proveeduría externa; o bien, a través de las Auditorias Voluntarias establecidas por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

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 cada año. Dicha auditoría se puede llevar a cabo por terceros según la disponibilidad presupuestal con al que cuente el **"CIATEQ"**; o bien, de forma interna conforme a 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 del **"CIATEQ"**.

VII. Programa de capacitación.

El Programa de Capacitación al personal que realiza tratamiento de datos personales en CIATEQ, A.C. Centro de Tecnología Avanzada está en primer término, integrado en el Programa de Capacitación en Transparencia, Acceso a la Información, Protección de Datos Personales y temas relacionados (PCTAIPDP) que el Centro compromete cada año con el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos.

La Unidad de Transparencia registra al personal en los cursos relacionados con la protección de datos, dependiendo de sus roles y responsabilidades respecto del tratamiento de datos personales. De manera interna, la Unidad de Transparencia ofrece un curso relacionado con la protección de datos personales, en el momento que es solicitado por algún área.

VIII. Actualización.

De conformidad con lo establecido en el artículo 36 de la LGPDPPSO, el Documento de Seguridad será actualizado cuando ocurra alguno de los siguientes eventos:

- Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el 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, y

- Cuando se efectúe la implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

Adicionalmente, podrá actualizarse el presente documento, en caso de cambios estructurales, de personal, de funciones, obligaciones o cualquier cambio que afecte la información contenida en éste.