PROGRAMA DE PROTECCIÓN DE DATOS PERSONALES.

BIRMEX

LABORATORIOS DE BIOLÓGICOS Y REACTIVOS DE MÉXICO, S.A. DE C.V.

ÍNDICE

I. Glosario de términos comunes 2
II. Presentación 6
III. Marco Normativo 7
1. Objetivos 7
2. Roles y Responsabilidades. 8
3. Alcance 9
4. Política de Gestión de Datos Personales. 10
4.1 Identificación del Flujo de los Datos Personales. 10
4.1.2 Identificación de datos personales. 10
4.1.3 Identificación de mecanismos de obtención de datos personales. 11
4.1.4 Identificación de medios de almacenamiento. 11
4.1.5 Identificación de permisos y tratamiento. 11
4.2 Valuación de las Medidas de Seguridad 12
4.2.1 Medidas de seguridad administrativas 12
4.2.2 Medidas de seguridad físicas 12
4.2.3 Medidas de seguridad técnicas 13
4.3 Plan de Trabajo. 13
4.3.1 Selección de acciones prioritarias 13
4.3.2 Periodo de cumplimiento de acciones 13
4.3.3 Recursos humanos y materiales 13
4.4 Mejora Continua. 14
4.4.1 Acciones preventivas: 14
4.4.2 Acciones correctivas 14
4.4.3 Implementación de las medidas de seguridad 15
4.4.4 Modelo de madurez 15
5. Revisiones y Auditorías a Realizar. 15
6. Sanciones 16
7. ANEXOS. 18

I. Glosario de términos comunes

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias y evaluarlas de manera objetiva para determinar el grado de cumplimiento de los criterios preestablecidos para la misma.

Aviso de privacidad: Documento de forma física, electrónica o en cualquier formato, que es generado por el responsable y puesto a disposición de los titulares de los datos personales, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de estos.

Bases de datos: Conjunto ordenado de datos personales bajo criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

Comité de Transparencia: Instancia a la que hace referencia el artículo 43 de la Ley General de Transparencia y Acceso a la Información Pública.

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.

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.

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

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.

Encargado: Persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o juntamente con otras trate datos personales a nombre y por cuenta del responsable.

Evaluación de impacto en la protección de datos personales: Evaluación mediante la 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.

Instituto o INAI: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

LGPDPPSO: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Lineamientos Generales: Lineamientos Generales de Protección de Datos Personales para el Sector Público.

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.

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.

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.

Portabilidad de datos personales: Prerrogativa del titular de obtener una copia de los datos que ha proporcionado al responsable del tratamiento en un formato estructurado que le permita seguir utilizándolos.

Programa: Programa de Protección de Datos Personales.

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

Responsable: Sujeto obligado de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados que decide sobre el tratamiento de los datos personales.

Revisión: Actividad estructurada, objetiva y documentada, llevada a cabo con la finalidad de constatar el cumplimiento continuo de los contenidos establecidos en este Programa.

Riesgo: Combinación de la probabilidad de un evento y su consecuencia desfavorable.

SNT: Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Sujeto obligado: Cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, del ámbito federal.

Titular: Persona física a quien corresponden los datos personales.

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

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.

Unidad Administrativa: Área a la que se le confieren atribuciones específicas en el reglamento interno, estatuto orgánico o instrumento normativo equivalente que sea superior a un manual de organización.

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

II. Presentación

En México, el derecho a la protección de datos personales en el sector público encuentra su antecedente en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental publicada en 2002, que en sólo un capítulo y seis artículos se reguló su tratamiento. Posteriormente, las reformas en materia de transparencia, acceso a la información y protección de datos personales contempladas en los artículos 6 y 16 de la Constitución Política de los Estados Unidos Mexicanos en 2009 y 2014, propiciaron la emisión de diversa normatividad con el propósito de garantizar el ejercicio de este derecho humano.

En 2009 se reformó el artículo 16 de nuestra Carta Magna para establecer que toda persona tenía derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como manifestar su oposición al uso de su información personal, en los términos que fijara la ley. Esta reforma propició la publicación de la Ley Federal de Protección de Datos Personales en Posesión de Particulares en 2010, no obstante, es hasta la reforma del artículo 6° Constitucional en 2014, cuando se fijan las bases para la emisión de una Ley General respecto de la información en posesión de entes públicos. El 26 de enero de 2017 se publicó la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), en la cual se establecen las bases, procedimientos, principios, deberes y obligaciones que rigen el tratamiento de información de carácter personal, así como los derechos que tienen los titulares a la protección de sus datos personales en posesión de los organismos de los poderes Ejecutivo, Legislativo y Judicial en los tres niveles de gobierno. Asimismo, el 26 de enero de 2018, se publicaron los Lineamientos Generales de Protección de Datos Personales para el Sector Publico, en los que se enuncian las obligaciones exigibles en el tratamiento de datos personales y el ejercicio de los derechos (ARCO), a partir de ambas publicaciones, todo aquel sujeto obligado obtiene la figura jurídica del "Responsable" que debe actuar de conformidad a los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad, además de adoptar medidas de seguridad (administrativas, físicas y técnicas) en el tratamiento de datos personales. El 28 de septiembre de 2018, se publicó en el Diario Oficial de la Federación el decreto por el que se promulgan el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal ("Convenio 108") y su Protocolo Adicional relativo a las Autoridades de Control y a los Flujos Transfronterizos de Datos. Dicho decreto entró en vigor el día primero de octubre de 2018, con lo cual el Convenio 108 y su Protocolo son vinculantes para México a partir de esa fecha, Asimismo, México ha suscrito diversas convenciones, tratados y acuerdos en la materia, y participa en diversas iniciativas, destacando la Red Iberoamericana de Protección de Datos (RIPD).

Bajo estas premisas Laboratorios de Biológicos y Reactivos de México S.A. de C.V. (BIRMEX) es un sujeto obligado reconocido por la LGPDPPSO y tiene la obligación de cumplir con lo dispuesto en el marco normativo aplicable.

III. Marco Normativo

El derecho a la protección de datos personales, materia de este documento, tiene su fundamento en el marco jurídico siguiente:

- Constitución Política de los Estados Unidos Mexicanos.
- Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108) y su Protocolo adicional.
- Ley General de Transparencia y Acceso a la Información Pública.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO).
- Ley General de Responsabilidades Administrativas de los Servidores Públicos.

Ley federal de protección de datos personales en posesión de los particulares.

- Ley Orgánica de la Administración Pública Federal.
- Ley General de Archivos.
- Lineamientos Generales de Protección de Datos Personales en Sector Público.

1. Objetivos

El presente programa tiene como objetivos:

1. Proveer el marco de trabajo necesario para la protección de los datos personales en posesión del sujeto obligado;
2. Cumplir con las obligaciones que establece la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y los Lineamientos Generales, así como la normatividad que derive de los mismos;
3. Establecer las directrices y herramientas necesarias, para garantizar la protección de los datos personales en posesión de las unidades administrativas, por medio de la sensibilización, capacitación, implementación, operación, revisión, mantenimiento y mejora de las

acciones diseñadas para el tratamiento y la seguridad de los datos personales.

4. Promover la adopción de mejores prácticas en materia de protección de datos personales, así como proporcionar a los trabajadores la certeza de que sus datos personales en posesión de los Laboratorios de Biológicos y Reactivos de México S.A. de C.V. están siendo tratados de conformidad con lo establecido en el marco normativo.

2. Roles y Responsabilidades.

Con fundamento en lo dispuesto por los artículos 83 y 84, fracción I de la LGPDPPSO y 47, segundo párrafo, y 48 de los Lineamientos Generales, que señalan que el Comité de Transparencia es la autoridad máxima en materia de protección de datos personales y que tiene entre sus funciones la de coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, dicho órgano tendrá las siguientes funciones con relación a este programa:

I. Elaborar, aprobar, coordinar y supervisar el Programa, en conjunto con las áreas técnicas que estime necesario involucrar o consultar;
II. Proponer cambios y mejoras al Programa, a partir de la experiencia de su implementación;
III. Dar a conocer el Programa al interior del sujeto obligado; el cual se dará a conocer en las primeras dos semanas del mes de marzo, y referirá al año inmediato anterior.
Pudiendo incluir:
- Estadística e información general sobre el cumplimiento de las obligaciones señaladas en el Programa de Protección de Datos Personales por parte de las unidades administrativas;
- Acciones realizadas por el Comité de Transparencia y la Unidad de Transparencia para cumplir con las obligaciones específicas que establece el Programa de Protección de Datos Personales, y
- Los resultados de las revisiones y auditorias.

IV. Coordinar la implementación del Programa en las unidades administrativas del sujeto obligado;
V. Asesorar a las unidades administrativas en la implementación de este Programa, con el apoyo del Comité de Transparencia.
VI. Presentar un informe anual al titular de la institución, en el que se describan las acciones realizadas para cumplir con lo dispuesto por este Programa;
VII. Supervisar la correcta implementación del Programa;
VIII. Elaborar, aprobar, coordinar y supervisar el programa anual de capacitación, en conjunto con las áreas técnicas que estime necesario involucrar o consultar, y
IX. Las demás que de manera expresa señale el propio Programa.

Para que los objetivos planteados en la primera sección se logren con éxito, el Programa requiere del apoyo e impulso directo del más alto nivel de la institución. En ese sentido, el Programa se deberá hacer del conocimiento de Director General, a fin de que tome las medidas necesarias para que el mismo se observe en los Laboratorios de Biológicos y Reactivos de México S.A. de C.V.

La intervención del Director General, tendrá la finalidad única de impulsar la debida implementación del Programa al interior de Los Laboratorios de Biológicos y Reactivos de México S.A. de C.V., pero no podrá suplir ni afectar las funciones que otorgan los artículos 83 y 84 de la LGPDPPSO al Comité de Transparencia, en su carácter de máxima autoridad de datos personales en la organización.

Para ello, resulta fundamental que el Programa se conozca al interior de Los Laboratorios de Biológicos y Reactivos de México S.A. de C.V., por lo que el Comité de Transparencia se encargará de difundirlo entre los servidores públicos.

Cuando los recursos humanos y presupuestales lo permitan, se sugiere que la organización cuente con el Oficial de Protección de Datos al que refiere el segundo párrafo del artículo 85 de la LGPDPPSO y que tendrá las funciones que señala ese artículo y el 121 y 122 de los Lineamientos Generales.

En caso que no se requiera el Oficial o no se cuente con los recursos para su designación, se sugiere valorar la posibilidad de designar a personal que asista al Comité de Transparencia y a la Unidad de Transparencia en el cumplimiento de sus obligaciones en materia de protección de datos personales, el cual deberá contar con conocimientos técnicos sobre el derecho de protección de datos personales.

3. Alcance

El presente Programa de Datos Personales, aplicará a la Dirección de Administración y Finanzas de los Laboratorios de Biológicos y Reactivos de México S.A. de C.V., al 7 de abril de 2022., que en el cumplimiento de sus atribuciones recaban y tratan datos personales. Por lo que, atendiendo al Reglamento Interior, se señalan las siguientes:

- Dirección de Administración y Finanzas.
  - Gerencia de Sueldos y Salarios.
  - Gerencia de Contabilidad.
  - Gerencia de Adquisiciones.

Es importante atender que también aplicará a todos los servidores públicos que por sus funciones realicen algún tipo de tratamiento de datos personales. En este caso, están obligados a conocer y aplicar las medidas de seguridad mínimas, en la LGPDPPSO y sus lineamientos Generales.

Se destaca que la responsabilidad de la tarea implica no sólo tratar los datos personales con responsabilidad, sino también, guardar la debida confidencialidad y garantizar seguridad sobre la información a la que tengan acceso.

Quedan exceptuados de la aplicación de este programa, los datos personales que correspondan al cumplimiento de las obligaciones de transparencia a las que refieren el artículo 120 de la Ley General de Transparencia y Acceso a la Información Pública y numeral 117 de la Ley Federal de Transparencia y Acceso a la Información Pública.

4. Política de Gestión de Datos Personales.

4.1 Identificación del Flujo de los Datos Personales.

La presente etapa busca identificar los datos personales que componen cada sistema de información, su clasificación, el personal que tiene acceso a los sistemas de tratamiento y los permisos otorgados, para poder identificar las bases de datos utilizadas.

El diagnóstico de la etapa es el inventario de datos personales y el tratamiento al que son sometidos los datos personales que se realizan en los Laboratorios de Biológicos y Reactivos de México S.A. de C.V., mediante la identificación de los siguientes elementos relevantes. **(Anexo 1).** para dar cumplimiento al artículo 33, fracciones II y III de la Ley de Datos.

Por "inventario de tratamientos de datos personales" se entenderá el control documentado que se llevará de los tratamientos que realizan las unidades administrativas de Los Laboratorios de Biológicos y Reactivos de México S.A. de C.V., realizado con orden y precisión. **(Anexo 2).**

Esta etapa permitirá identificar y documentar el ciclo de vida de los datos personales, en los términos establecidos en el artículo 59 de los Principios de Protección (Lineamientos Generales) y verificar el cumplimiento de los ocho principios para la protección de los datos personales.

Asimismo, será la base para determinar el nivel de protección necesario para la salvaguarda de los datos personales, debido al tipo de dato –y su riesgo inherente- y del tratamiento al que es sometido. **(Anexo 2).**

Se compone de cuatro fases:

4.1.2 Identificación de datos personales.

El responsable, con apoyo de las áreas custodias y de la Unidad de Transparencia, deberá identificar los datos personales que están siendo tratados en el sistema de datos personales que esté a su cargo y su categorización, es decir, si los datos personales son estándar, sensibles o especiales.

Lo anterior permitirá determinar si los datos personales recabados cumplen con los principios de licitud, finalidad, proporcionalidad, y en caso de no ser así, el responsable deberá prescindir de los mismos y no incluirlos en nuevos procesos de recolección. **(Anexo 3).**

4.1.3 Identificación de mecanismos de obtención de datos personales.

El responsable deberá identificar el flujo y la forma a través de la cual se recaban los datos personales, proporcionando elementos para verificar, posteriormente, el aviso de privacidad; si los datos se obtienen de una manera libre, especifica e informada, lo cual permitirá acreditar la observancia al principio de información, lealtad, consentimiento, que establece la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados.

Cabe señalar que la Unidad de Transparencia analizará las particularidades de los datos personales que son recabados, como es el caso de los datos de menores.

4.1.4 Identificación de medios de almacenamiento.

El responsable deberá identificar los sitios, medios y formatos utilizados para almacenar los datos, si se resguardan en un sitio específico o en un área común, y si son resguardados en medios de almacenamiento físicos o digitales. Incluye a encargados, destinatarios o terceros receptores de las transferencias que se efectúen.

4.1.5 Identificación de permisos y tratamiento.

El responsable procederá a identificar al personal y, en su caso, prestadores de servicios, incluyendo a los encargados, destinatarios o terceros que intervengan en el tratamiento de los datos.

La identificación contempla el rol y los permisos que son asignados al personal para llevar a cabo el tratamiento; esto, a través de un formato integrado al Manual de Seguridad en el cual deberán señalar el tipo de permisos que tiene cada una de las personas/roles en la base o bases de datos correspondientes.

Esta fase guarda relación con el tiempo de almacenamiento de los datos, que deberá corresponder al tiempo necesario para el cumplimiento de las finalidades que justifican su tratamiento, así como del principio de calidad (incluyendo la supresión de los datos personales) **(Anexo 6).**

4.2 Valuación de las Medidas de Seguridad.

La presente etapa tiene como finalidad la gestión del riesgo. Si bien, no es posible eliminar los riesgos, es necesario identificar e implementar medidas de seguridad con la finalidad de minimizar las vulneraciones a la seguridad de las bases de datos personales. **(Anexo 4).**

La obligación de establecer medidas de seguridad se encuentra contemplada en los artículos 31, 32 y 33 fracciones VI y VII de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados.

Las medidas de seguridad se analizarán en el siguiente orden:

1. De la cultura del personal: medidas administrativas.
2. Del entorno físico: medidas de seguridad físicas.
3. Del entorno de trabajo digital: medidas de seguridad técnicas.

Lo anterior se llevará a cabo mediante la elaboración de un Análisis de brecha para conocer las medidas de seguridad existentes e identificarán las medidas faltantes, o el reforzamiento de las actuales.

El artículo 33 fracción V de la Ley de Datos, señala la obligación de realizarlo, conforme a lo establecido en el artículo 61 de los Lineamientos Generales.
El análisis lo realizará el responsable, con apoyo de la Unidad de Transparencia y, en su caso, los órganos vinculados con seguridad de la información.
El entregable generado en esta etapa es el Análisis de Brecha.

4.2.1 Medidas de seguridad administrativas

El responsable de la base o bases de datos personales, con apoyo de la Unidad de Transparencia y, en su caso, de los órganos vinculados con seguridad de la información, identificará las medidas de seguridad administrativas implementadas, con el objetivo de detectar prácticas inadecuadas en el tratamiento de los datos a su interior, mismas que podrían suscitar una vulneración. **(Anexo 5).**

La verificación de las medidas de seguridad se realizará con base en los estándares y buenas prácticas en la materia.

4.2.2 Medidas de seguridad físicas

La seguridad del entorno de trabajo físico es un elemento básico para mitigar las vulneraciones a la seguridad de los datos personales, por lo que en la presente fase se identificarán las medidas de seguridad implementadas, así como las áreas involucradas para su implementación. La verificación de las medidas de

seguridad se realizará con base en los estándares y buenas prácticas en la materia.

4.2.3 Medidas de seguridad técnicas

En la presente fase se evaluarán las medidas utilizadas en el entorno digital que busquen proteger los equipos de cómputo y dispositivos de almacenamiento, contra el acceso lógico no autorizado y contra amenazas informáticas. La verificación de las medidas de seguridad se realizará con base en los estándares y buenas prácticas en la materia.

4.3 Plan de Trabajo.

El responsable de la base de datos, previo a elaborar el Plan de trabajo, deberá ejecutar un análisis de riesgos, con la finalidad de identificar el orden de prioridad de las acciones a realizar para la implementación de las medidas de seguridad faltantes –detectadas en el análisis de brecha- o la mejora de las ya existentes. Lo anterior atendiendo al artículo 33 fracción VI de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados.

Los entregables de esta etapa son el Plan de Trabajo y el Análisis de Riesgos.

Fases que componen esta etapa son:

4.3.1 Selección de acciones prioritarias

Una vez realizada la identificación de los datos personales y su valor, el responsable –con apoyo de la Unidad de Transparencia y, en su caso, de los órganos vinculados con seguridad de la información- realizará un Análisis de riesgos, de conformidad con lo establecido en artículo 33, fracción IV de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados

4.3.2 Periodo de cumplimiento de acciones

El responsable –de acuerdo con sus actividades generales y con relación a la prioridad de las acciones- elaborará y dará a conocer a la Unidad de Transparencia el Plan de trabajo para la implementación o adecuación de las medidas de seguridad.

La Unidad de Transparencia reportará lo conducente ante el Comité de Transparencia.

4.3.3 Recursos humanos y materiales

El responsable determinará los recursos necesarios para cumplir con las acciones en el periodo establecido, con la finalidad de solicitarlo al área correspondiente del Instituto.

4.4 Mejora Continua.

Con apoyo de la Unidad de Transparencia y, en su caso, de los órganos vinculados con seguridad de la información, iniciarán un proceso de mejora continua, que permitirá verificar la seguridad en el tratamiento de los datos personales, lo que generará una mejora periódica de sus controles,

Se deberá contemplar los siguientes acciones y puntos de mejora de la implementación del programa, los cuales serán:

4.4.1 Acciones preventivas:

Son aquéllas encaminadas a evitar cualquier "no conformidad" (no cumplimiento) con relación a lo establecido en este Programa.

En las acciones preventivas se deben llevar a cabo las siguientes actividades:

- El análisis y revisión de las posibles causas de no conformidad;
- Determinar las no conformidades que podría desencadenarse a partir de ciertas situaciones de riesgo para el tratamiento de datos personales;
- Evaluar las acciones necesarias para evitar que la no conformidad ocurra;
- Determinar e implementar estas acciones;
- Documentar los resultados de las acciones tomadas, y
- Revisar la eficacia de las acciones preventivas tomadas.

4.4.2 Acciones correctivas

Son aquéllas encaminadas a eliminar las causas de la "no conformidad" con relación a lo previsto en este Programa.

En las acciones correctivas se deben llevar a cabo, al menos, las siguientes actividades:

- Analizar y revisar la no conformidad;
- Determinar las causas que dieron origen a la no conformidad;
- Evaluar las acciones necesarias para evitar que la no conformidad vuelva a ocurrir;
- Implementar estas acciones;
- Documentar los resultados de las acciones tomadas, y
- Revisar la eficacia de las acciones correctivas tomadas.

El objetivo de las acciones correctivas es eliminar la causa de la no conformidad, o bien, reducir su grado de prevalencia.

4.4.3 Implementación de las medidas de seguridad

Con base en el Plan de trabajo, el área responsable deberá implementar las medidas de seguridad que son necesarias para lograr el cumplimiento de los Deberes de Seguridad y Confidencialidad.

La Unidad de Transparencia verificará que la implementación se realice conforme a lo establecido en el Plan de trabajo.

En caso de detectar desfases, la Unidad de Transparencia verificará el nivel de riesgo al que se expondrán los datos personales derivado de la falta de los controles y determinará las acciones correspondientes, mismas que deberán comunicar a los titulares de las áreas.

Para lo cual se empleará el modelo de madurez que, previo análisis, estime pertinente la Unidad de Transparencia.

4.4.4 Modelo de madurez

Esta etapa estará encargada de Monitorear y revisar de manera periódica (por parte de los sujetos externos responsables) el nivel de madurez de las áreas con respecto al cumplimiento de los deberes de Seguridad y Confidencialidad con lo establecido en el Sistema de Gestión para la Protección de Datos Personales.

Cabe mencionar que los tiempos de monitoreo y revisión serán pactados por las dependencias de las cuales provengan estos sujetos externos.

Lo anterior, atendiendo al artículo 33, fracción VII de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados. relacionado al monitoreo y revisiones periódicas de las medidas de seguridad.

5. Revisiones y Auditorías a Realizar.

Con objeto de monitorear y revisar la eficacia y eficiencia del sistema de gestión en que se basa este Programa, vinculante al interior de Los Laboratorios de Biológicos y reactivos de México S.A. de C.V., se deberán contar con un programa para llevar a cabo dos tipos de acciones: 1) auditorías y 2) revisiones administrativas.

Las auditorías las deberá realizar un actor externo al Comité de Transparencia; mientras que las revisiones administrativas las realizará el propio Comité con el apoyo de la Unidad de Transparencia, si así lo estima pertinente. **(Anexo 7)**.

Las auditorías podrán ser:

1. Internas;
2. Externas, cuando exista el presupuesto para ello y la importancia del caso lo amerite, o
3. Voluntarias, realizadas a través del INAI según el artículo 151 de la LGPDPPSO, cuando sea con relación a un tratamiento específico y no a todo el sistema de gestión de los datos personales.

6. Sanciones.

Cuando el Comité de Transparencia tenga conocimiento del incumplimiento de alguna obligación prevista en este Programa, deberá realizar un exhorto a la unidad administrativa correspondiente para que ésta lleve a cabo las acciones que resulten pertinentes con objeto de modificar dicha situación y evitar incumplimientos futuros o situaciones de riesgo que los pudieran ocasionar.

De manera adicional, es importante que las y los servidores públicos que están a cargo del tratamiento de datos personales tengan presente que de conformidad con el artículo 163 de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados serán causas de sanción por incumplimiento de las obligaciones establecidas en dicha ley, las siguientes:

I. Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCO;
II. Incumplir los plazos de atención previstos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados para responder las solicitudes para el ejercicio de los derechos ARCO o para hacer efectivo el derecho de que se trate;
III. Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión;
IV. Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos en la Ley General de Datos Personales;
V. No contar con el aviso de privacidad, o bien, omitir en el mismo alguno de los elementos a que refiere el artículo 27 de la Ley General de Datos Personales, según sea el caso, y demás disposiciones que resulten aplicables en la materia;
VI. Clasificar como confidencial, con dolo o negligencia, datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables. La sanción sólo procederá cuando exista una resolución previa, que haya quedado firme, respecto del criterio de clasificación de los datos personales;
VII. Incumplir el deber de confidencialidad establecido en el artículo 42 de la Ley General de Datos Personales;

VIII. No establecer las medidas de seguridad en los términos que establecen los artículos 31, 32 y 33 de la Ley General de Datos Personales;
IX. Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad según los artículos 31, 32 y 33 de la Ley General de Datos Personales;
X. Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en Ley General de Datos Personales;
XI. Obstruir los actos de verificación de la autoridad;
XII. Crear bases de datos personales en contravención a lo dispuesto por el artículo 5 de la Ley General de Datos Personales;
XIII. No acatar las resoluciones emitidas por el Instituto, y
XIV. Omitir la entrega del informe anual y demás informes a que se refiere el artículo 44, fracción VII de la Ley General de Transparencia, o bien, entregar el mismo de manera extemporánea.

Las causas de responsabilidad previstas en las fracciones I, II, IV, VI, X, XII, y XIV, así como la reincidencia en las conductas previstas en el resto de las fracciones, serán consideradas como graves.

Asimismo, de conformidad con el artículo 105 de los Lineamientos Generales, cuando alguna unidad administrativa se niegue a colaborar con la Unidad de Transparencia en la atención de las solicitudes para el ejercicio de los derechos ARCO, ésta dará aviso al superior jerárquico para que le ordene realizar sin demora las acciones conducentes.

Si persiste la negativa de colaboración, la Unidad de Transparencia lo hará del conocimiento del Comité de Transparencia para que, a su vez, dé vista al Órgano Interno de Control, contraloría o instancia equivalente y, en su caso, dé inicio el procedimiento de responsabilidad administrativo respectivo de conformidad con la Ley Federal de Responsabilidades Administrativas de los Servidores Públicos.

Cabe destacar que las sanciones de carácter económico no podrán ser cubiertas con recursos públicos

TITULAR DE LA UNIDAD DE TRANSPARENCIA	MTRA. BEATRIZ ROMERO VALDERRAMA
SUPLENTE DE LA TITULAR DE LA UNIDAD DE TRANSPARENCIA	Q.B.P. CLAUDIA ARIADNA URIBE GUTIÉRREZ
SUPLENTE DEL TITULAR DEL ÓRGANO INTERNO DE CONTROL	C.P. LEOPOLDO GÓMEZ GEN
SUPLENTE DEL RESPONSABLE DEL ÁREA COORDINADORA DE ARCHIVOS	LIC. RAMÓN GÓMEZ GAYTÁN
GERENTE DE SUELDOS Y SALARIOS **RESPONSABLE DE ADMINISTRACIÓN DE DATOS PERSONALES**	LIC. EDUARDO CÁRDENAS GARCÍA