BIRMEX
LABORATORIOS DE BIOLOGICOS Y REACTIVOS DE MÉXICO, S.A. DE C.V.

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

Programa de Protección de Datos Personales

2023

ÍNDICE

1. MARCO NORMATIVO

- Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados.
- Ley Federal de Transparencia y Acceso a la Información Pública.
- Lineamientos Generales de Protección de Datos Personales para el Sector Público.

2. OBJETIVO

El presente documento tiene como propósito establecer el marco de trabajo necesario para la protección de los datos personales en posesión de BIRMEX, a fin de cumplir con las obligaciones que establece la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y los Lineamientos Generales de Protección de Datos Personales para el Sector Público, así como la normatividad que derive de los mismos.

En el presente documento se establecen los elementos y actividades de dirección, operación y control de los procesos que impliquen el tratamiento de datos personales, a efecto de protegerlos de manera sistemática y continua.

3. RESPONSABLES Y FUNCIONES

COMITÉ DE TRANSPARENCIA

De conformidad con los artículos 83 y 84, fracción I de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados (LGPDPPSO), numerales 47 segundo párrafo y 48 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales) el Comité de Transparencia es la autoridad máxima en materia de protección de datos personales y 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 BIRMEX.

Funciones del Comité de Transparencia

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 de BIRMEX;
IV. Coordinar la implementación del Programa en las unidades administrativas de BIRMEX;
V. Asesorar a las unidades administrativas en la implementación de este Programa, con el apoyo de las áreas técnicas que estime pertinente;
VI. Presentar un informe anual al Director General de BIRMEX, 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,
IX. Las demás que de manera expresa señale el propio Programa.

UNIDADES ADMINISTRATIVAS

Las áreas que en el ejercicio de sus actividades o funciones recaben o resguarden datos personales, deberán observar los principios establecidos en el Título Segundo, Capítulo I "De los principios", de la LGPDPPSO, y tendrán las siguientes funciones:

I. Dar cumplimiento a las políticas internas establecidas por el Comité de Transparencia, para la gestión y tratamiento de los datos personales.
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. 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.

4. ALCANCE

Para que la implementación del Programa tenga como resultado el cumplimiento integral de las obligaciones que establece la LGPDPPSO y los Lineamientos Generales, será de observancia obligatoria para todos los servidores públicos de BIRMEX que en el ejercicio de sus funciones cuenten o puedan contar y dar tratamiento a datos personales.

El presente programa aplicará a todas las unidades administrativas que realicen tratamiento de datos personales en ejercicio de sus atribuciones, y a todos los tratamientos de datos personales que éstas efectúen en ejercicio de sus atribuciones.

Las unidades administrativas deberán realizar las acciones necesarias para cumplir con las obligaciones que establece este Programa, para lo cual deberán asignar los recursos materiales y humanos necesarios, y prever lo que se requiera en sus programas de trabajo.

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.

5. ACCIONES

5.1 Inventario de tratamientos de datos personales

Para el debido cumplimiento de las obligaciones que se establecen en este Programa, es necesario que cada una de las unidades administrativas responsables de datos realicen un diagnóstico de los tratamientos de datos personales que llevan a cabo.

El diagnóstico en mención se basa en la elaboración de un inventario con la información básica de cada tratamiento de datos personales que se realizan en BIRMEX.

Por "inventario de tratamientos de datos personales", se entenderá el control documentado que se llevará de los tratamientos que realizan las unidades administrativas de BIRMEX, realizado con orden y precisión.

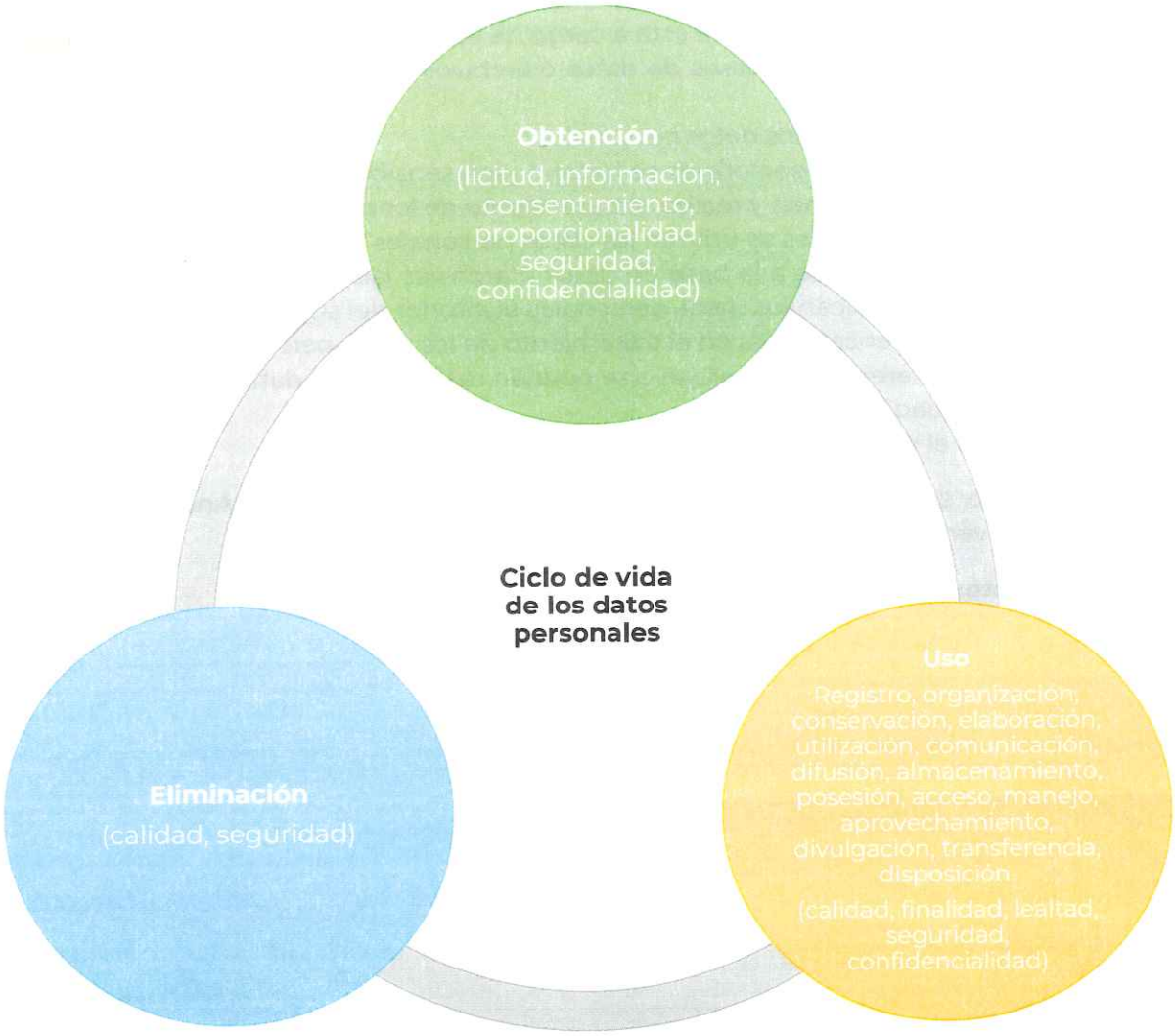
El inventario de datos personales al que hace referencia la LGPDPPSO en los artículos 33, fracción III, 35, fracción I, y 58 de los Lineamientos Generales, identificará los siguientes elementos relevantes:

1. ¿Qué tratamientos de datos personales realiza la unidad administrativa?
2. ¿Qué unidad administrativa está a cargo de estos procesos y que por tanto sea la administradora de las bases de datos o archivos que se generen con motivo de dichos tratamientos?
3. ¿Cómo se obtienen los datos personales?
4. ¿Qué tipo de datos personales se tratan? ¿son sensibles?
5. ¿Dónde se almacenan y realiza el tratamiento de los datos personales?
6. ¿Para qué finalidades se utilizan los datos personales?
7. ¿Quién tiene acceso a la base de datos o archivos (sistemas de tratamiento) y a quién se comunican los datos personales al interior del sujeto obligado?
8. ¿Intervienen encargados en el tratamiento de los datos personales?
9. ¿Qué transferencias se realizan o se podrían realizar de los datos personales y con qué finalidad?
10. ¿Cuál es el plazo de conservación de los datos personales?

El diagnóstico se deberá realizar en la matriz correspondiente al Anexo 1 de este programa (Inventario de Tratamientos), y se deberá realizar por proceso.

Cumplimiento: Primer trimestre de 2023

5.2 Cumplimiento de obligaciones



5.2.1 Valuación de las Medidas de Seguridad

En esta etapa se identifican las medidas de seguridad que establecen los responsables del manejo de datos para minimizar las vulneraciones a la seguridad de las bases de datos personales.

Actividad para su cumplimiento:

Análisis de Brecha

Las áreas responsables del manejo de datos realizarán un análisis de brecha, en el cual se determinará si cuentan con las siguientes medidas de seguridad:

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

Medidas administrativas: Se refieren a las 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: Medidas que se enfocan en prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información; proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización; entre otros.

Medidas de seguridad técnicas: Algunas medidas establecidas en la LGPDPPSO, son las de prevenir el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados; generar un esquema de privilegios; gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales, entre otras.

Las áreas responsables deberán enviar a la Unidad de Transparencia, el análisis de las medidas de seguridad implementadas a través del formato establecido en el **Anexo 2**.

5.2.2 Medidas de seguridad

El deber de seguridad consiste en la implementación de medidas de seguridad físicas, técnicas y administrativas necesarias para proteger los datos personales contra daño, pérdida, alteración, destrucción, o su uso, acceso o tratamiento no automatizado, así como para garantizar su confidencialidad, integridad y disponibilidad.

Las medidas de seguridad son el conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales.

Las **medidas de seguridad administrativas** refieren a las 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.

Por su parte, las **medidas de seguridad físicas** son el conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.

Actividad para su cumplimiento:

Documento de Seguridad

Las unidades administrativas que manejan datos personales en BIRMEX, deberán elaborar un documento de seguridad que describa y dé 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.

El documento de seguridad deberá integrar la siguiente información:

- Catálogo de sistemas de datos personales.
- Responsables (todos los servidores públicos del área que intervengan en los procesos de manejo de datos, es decir, responsables, encargados y usuarios).
- Mecanismos de monitoreo y revisión de las medidas de seguridad.
- Programa de Capacitación General (en apego al Programa establecido por la Unidad de Transparencia).

Cumplimiento: Segundo trimestre de 2023.

5.2.3 Confidencialidad

Las áreas administrativas responsables de datos personales establecerán controles o mecanismos para que todas las personas que intervengan en cualquier fase del tratamiento de los datos personales guarden confidencialidad, obligación que subsistirá aún después de finalizar sus relaciones con BIRMEX y sin menoscabo de lo establecido en las disposiciones de acceso a la información pública.

Actividades para su cumplimiento:

1. Las áreas deberán **emitir un acuerdo de confidencialidad** de datos personales signado por el personal involucrado en el tratamiento de datos personales con apego al formato establecido en el **Anexo 3**.
2. Elaborar un documento mediante el cual se establecen los **controles dirigidos a asegurar la confidencialidad** que deben guardar todas las personas que intervienen en cualquier fase del tratamiento de datos personales. Los controles deben identificarse con claridad de forma sencilla.
3. Elaborar un documento que contenga la relación de los **instrumentos jurídicos mediante los cuales se formaliza la contratación o adhesión a servicios, aplicaciones e infraestructura en el cómputo en la nube y otras materias**, en los cuales se establezcan las condiciones o cláusulas generales de contratación, incluidas aquéllas en las cuales el o los proveedores se obliguen a guardar confidencialidad respecto de los datos personales sobre los que se preste(n) el servicio (en caso de que no aplique, el responsable deberá notificar a la Unidad de Transparencia que a la fecha no se cuenta con proveedor(es) de servicios, aplicaciones e infraestructura en el cómputo en la nube y otras materias).
4. Elaborar un documento que contenga la **relación de los instrumentos jurídicos mediante los cuales se formalizan las transferencias de datos personales, y en**

los cuales el receptor de los datos personales se obliga a garantizar la confidencialidad de los datos personales a los que da tratamiento. El documento deberá contener la denominación e hipervínculo de la versión pública de cada instrumento jurídico, su finalidad, breve descripción de la forma en la que se obtuvo el consentimiento del titular, o bien, especificar alguna de las excepciones establecidas en los artículos 22 fracción II y/o 70 de la LGPDPPSO; medio o forma por el que el responsable comunicó al receptor de los datos personales, el aviso de privacidad conforme al cual se tratan los datos personales frente al titular; así como indicar si estos incluyen la cláusula general de confidencialidad (en caso de que no aplique, el responsable deberá notificar a la Unidad de Transparencia que a la fecha no se han realizado transferencias, o bien, que no aplica por actualizarse alguno de los supuestos que establece el artículo 66 fracciones I y II de la LGPDPPSO.

5. Informar a la Unidad de Transparencia si el área administrativa responsable realiza tratamientos de datos personales por medios automatizados o electrónicos.

5.2.4 Aviso de privacidad

Las áreas responsables del manejo de datos personales deberán elaborar el aviso de privacidad con todos los elementos informativos que establece la LGPDPPSO, y con información que corresponda a la realidad del tratamiento que se efectúan.

El documento se elabora de conformidad con la guía que se presenta en el **Anexo 4**.

Cumplimiento: Tercer trimestre de 2023

6. INFORMES

En cumplimiento a la fracción VI del apartado "Funciones del Comité de Transparencia" numeral 3 Responsables y funciones, del presente documento, el Comité de Transparencia deberá presentar al Director General, un informe anual en el que se describan las acciones realizadas para cumplir con lo dispuesto por este Programa.

Cumplimiento: Cuarto trimestre de 2023

7. CALENDARIO DE CUMPLIMIENTO Y CRONOGRAMA

Anexo 5

8. INTERPRETACIÓN

La aplicación e interpretación para efectos administrativos del presente documento, así como la solución de casos no previstos corresponderá al Comité de Transparencia a través de la Unidad de Transparencia de BIRMEX.

INTEGRANTES DEL COMITÉ DE TRANSPARENCIA

MTRA. NORMA ANGÉLICA CABRERA HERNÁNDEZ

RESPONSABLE DE LA UNIDAD DE TRANSPARENCIA

DESIGNADA MEDIANTE OFICIO DG/006/2023 DEL 09 DE ENERO DE 2023

LIC. RAMÓN GÓMEZ GAYTÁN

SUPLENTE DE LA RESPONSABLE DEL ÁREA COORDINADORA DE ARCHIVOS

C.P. LEOPOLDO GÓMEZ GEN

SUPLENTE DEL TITULAR DEL ÓRGANO INTERNO DE CONTROL

ELABORÓ

C. Nadya Reyes Leos
Soporte Administrativo C

VERIFICÓ

Lic. Jorge Soto Ruiz
Gerente de Área

ANEXO 1

INVENTARIO DE TRATAMIENTOS DE DATOS PERSONALES.

El presente formato es un documento que servirá de apoyo a las diferentes áreas administrativas que conforman al responsable y/o sujeto obligado, en el diagnóstico de los tratamientos de datos personales que llevan a cabo.

Este diagnóstico se basa en la elaboración de un inventario de tratamientos de datos personales, entendiéndose como el control documentado que se llevará de dichos procedimientos, realizado con orden y precisión.

Sujeto obligado	Laboratorios de Biológicos y Reactivos de México S.A. de C.V.
Área administrativa:	
Fecha de elaboración o última actualización:	
Nombre del tratamiento (proceso):	
Sistemas físicos o electrónicos que integran el tratamiento de datos personales.	
Fundamento jurídico que faculta el tratamiento.	
Atribuciones de la unidad administrativa para realizar el tratamiento.	
Medios a través de los cuales se obtienen los datos personales en este tratamiento (proceso).	1. Directamente del titular - De manera personal, con la presencia física del titular de los datos personales o su representante, en su caso. - Vía telefónica

	- Por correo electrónico - Por Internet o sistema informático - Por escrito presentado directamente en las oficinas del sujeto obligado - Por escrito enviado por mensajería 2. Mediante una transferencia - Quién transfiere los datos personales y para qué fines - Medios por los que se realiza la transferencia 3. De una fuente de acceso público
Tipo de datos personales que se tratan.	• Se podrá consultar el cuadro de las categorías de datos personales (apéndice a) • Especificar si son datos personales sensibles.
Almacenamiento de los datos personales	• Formato en que se encuentra la base de datos: físico y/o electrónico • Ubicación de la base de datos • Sección, serie y subserie de archivos
Finalidades para las que se tratan los datos personales.	
Indicar si la finalidad requiere o no el consentimiento del titular, para tratar sus datos personales.	
En caso de que la finalidad no requiera el consentimiento del titular, señalar el o los supuestos del artículo 15 de la Ley de Protección de Datos Personales en	

Posesión de Sujetos Obligados del Estado de Durango, que se actualizan.	
En caso de que la finalidad requiera el consentimiento del titular, señalar el tipo de consentimiento que se necesita.	
Servidores públicos que tienen acceso a las bases de datos personales, así como el área de adscripción.	
Finalidades del acceso de los servidores públicos antes identificados, a las bases de datos personales.	
Nombre de la o las personas físicas o morales que actúan como encargados en el tratamiento, en su caso.	De conformidad con la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados, se entiende por encargados a La 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;
Número de identificación del instrumento jurídico que regula la relación con el encargado.	
Se realizan o no transferencias en el marco del tratamiento.	
Nombre, razón o denominación social de los terceros a los que se transfieren los datos personales, en su caso.	

Finalidades para las cuales se transfieren los datos personales por cada uno de los terceros, en su caso.	
Señalar si la transferencia requiere o no consentimiento.	
En caso de que la transferencia no requiera consentimiento, señalar los supuestos que se actualizan.	
En caso de que la finalidad de la transferencia requiera el consentimiento del titular, señalar si se requiere el tácito o el expreso y por escrito.	
Señalar el plazo de conservación de los datos personales, según lo señalado en los instrumentos de clasificación archivística.	
Observaciones	

APÉNDICE A
CATEGORÍAS DE DATOS PERSONALES

Datos de identificación	Datos como nombre, domicilio, teléfono particular y/o celular, correo electrónico personal, estado civil, firma, firma electrónica, cartilla militar, lugar y fecha de nacimiento, nacionalidad, edad, fotografía, clave del Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP), nombres de familiares, dependientes y/o beneficiarios.
Datos Laborales	Pueden referirse a los contenidos en las solicitudes de empleo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales, referencias personales, recomendaciones, capacitaciones, documentos de selección, reclutamiento, nombramiento, incidencias, hojas de servicio y otras generadas derivadas de nuestra relación laboral.
Datos patrimoniales	Se refiere a los bienes muebles e inmuebles, ingresos y egresos, cuentas bancarias, seguros, fianzas, afores, historial crediticio, información fiscal, servicios contratados y afines.
Datos sobre procedimientos administrativos y jurisdiccionales	Es aquella información disponible en procedimientos administrativos o juicios en materia laboral, civil, penal, fiscal, mercantil o de cualquier otra rama del Derecho.
Datos académicos	Son los datos que permiten identificar nuestra trayectoria académica y formación profesional como son calificaciones, boletas, constancias, certificados, reconocimientos, títulos, cédulas profesionales.
Datos de tránsito y movimientos migratorios	Información necesaria para nuestro tránsito dentro y fuera de país.
Datos personales sensibles	Datos de salud Datos ideológicos Datos de vida sexual Datos de origen Datos biométricos Datos electrónicos (correos electrónicos particulares, nombres de usuarios, contraseñas, firma electrónica)

ANEXO 2

MEDIDAS DE SEGURIDAD PARA LOS TRATAMIENTOS DE DATOS PERSONALES

En el presente formato se identificarán las medidas de seguridad implementadas en las áreas que manejan datos personales para el tratamiento de los datos.

Instrucciones: Marque con una X las medidas de seguridad implementadas en el proceso en el cual se realiza el tratamiento de datos personales (en el apéndice A, se encuentra la descripción de cada una de las medidas).

Laboratorios de Biológicos y Reactivos de México, S.A. de C.V.	
Área administrativa:	
Fecha de elaboración o actualización:	
Nombre del tratamiento (proceso):	
Medidas de seguridad administrativas	
Declaración de confidencialidad	
Listado de personal	
Clasificación de los archivos físicos	
Clasificación de los archivos electrónicos	
Capacitación	
Bitácora de vulneraciones	
Depuración y borrado seguro del archivo físico	
Depuración y borrado seguro del archivo electrónico	
Bitácora de consulta	
Responsable de seguridad	
Transferencias	
Medidas de seguridad físicas	
Cuidado de los bienes informáticos	
Prevenir accesos no autorizados	
No instalar equipos ajenos	
Traslado de equipos de cómputo	
Archivero con candado	
Candados de seguridad para equipos de cómputo	
Zona de confidencialidad	
Medidas de seguridad técnicas	
Cuidado de la contraseña personal	
Actualización de contraseñas	
Reportar fallas	
No instalar softwares	
Contraseñas robustas	
Respaldo de información	

Análisis de riesgo y medidas de seguridad
(Uso exclusivo de la Unidad de Transparencia)

Nivel de riesgo	**Resultado de la encuesta**
Bajo	0 a 5
Medio	6 a 8
Alto	9 en adelante

Análisis de brecha

El análisis de brecha consiste en identificar la distancia que existe entre las medidas recomendadas y las medidas implementadas por cada uno de los tratamientos reportados.

APÉNDICE A

MEDIDAS DE SEGURIDAD

MEDIDAS DE SEGURIDAD ADMINISTRATIVAS	
Declaración de confidencialidad (acuerdo de confidencialidad)	Realizar una declaración que será puesta a disposición del personal que interviene en el tratamiento de datos personales para que estén informados de los deberes y medidas de seguridad que deben tomar en consideración en sus actividades relacionadas con dichos tratamientos.
Listado de personal	Elaborar un documento que contenga la relación del personal que interviene en el tratamiento de datos personales, en donde se incluya nombre, cargo, funciones en el tratamiento y obligaciones en materia de datos personales, por cada tratamiento.
Clasificación de los archivos físicos	Identificar o incluir la base de datos en soporte físico en el Catálogo de Disposición Documental para tener control del ciclo de vida a que deben estar sujetos los archivos administrativos.
Clasificación de los archivos electrónicos	Identificar o incluir la base de datos en soporte físico en el Catálogo de Disposición Documental para tener control del ciclo de vida a que deben estar sujetos los archivos administrativos.
Capacitación	El personal involucrado en el tratamiento de los datos personales deberá asistir a los cursos de capacitación implementados por el Comité de Transparencia en el Programa Anual de Capacitación.
Bitácora de vulneraciones	Implementar un control informativo en donde se reporten los tipos de vulneraciones[1] con los siguientes datos: fecha y lugar en donde se produjo, nombre y cargo de quien notifica la incidencia, nombre y cargo de la persona a la que se le comunica, y las medidas que se implementaron para subsanar la misma. Toda vulneración deberá notificarse, también, al Comité de Transparencia para que tome las acciones pertinentes.
Depuración y borrado seguro del archivo físico	Transferir y depurar el archivo físico de manera periódica, conforme a los plazos de conservación y parámetros dispuestos la normativa en materia.

[1] De conformidad con el artículo 38 de la LGPDPPSO, son: I) La pérdida o destrucción no autorizada; II) el robo, extravío o copia no autorizada; III) el uso, acceso o tratamiento no autorizado, o IV) el daño, alteración o modificación no autorizada

Depuración y borrado seguro del archivo electrónico	Borrar, de manera segura y permanente, las bases de datos o parte de ellas que se encuentren en archivo electrónico, en desuso o que hayan cumplido su finalidad o el tiempo de conservación dispuesta para el archivo administrativo. Solicitar a Dirección de Tecnologías de la Información que proporcione un programa para el borrado integral de la información, o en su defecto, reinicio de los equipos o medios de almacenamiento a los valores de origen.
Bitácora de consulta	Establecer una bitácora como control para registrar el nombre, cargo, fecha y hora de consulta de la base de datos.
Responsable de seguridad	Designar un responsable de seguridad para coordinar y verificar las medidas de seguridad establecidas en el Documento de Seguridad.
Transferencias	Realizar transferencias con las medidas de confidencialidad necesarias, enviar la información en sobre cerrado y con la leyenda de "confidencial" o en archivos electrónicos encriptados.
MEDIDAS DE SEGURIDAD FÍSICAS	
Cuidado de los bienes informáticos	Mantener en buen estado el bien informático que le haya sido asignado y no abrir los equipos o bien, introducir en ellos cualquier tipo de instrumento o software que no sean los apropiados para el trabajo y que no hayan sido validados por la Dirección de Tecnologías de la Información.
Prevenir accesos no autorizados	Prevenir que el acceso a las bases de datos o a la información, así como a los recursos que las contengan, se realice únicamente por usuarios identificados y autorizados por el área.
No instalar equipos ajenos	Abstenerse de instalar equipos de cómputo que no sean propiedad de la Birmex sin permiso de la Dirección de Tecnologías de la Información. Los usuarios que requieran hacer uso de la red interna de Birmex deben usar solamente las direcciones IP asignadas por la Dirección de Tecnologías de la Información. En caso de requerir conectar un dispositivo de almacenamiento de información (p. ej. USB, disco duro portátil, etcétera) al equipo del usuario, éste debe ser revisado previamente por el antivirus. En el caso de encontrarse infectado el dispositivo, el usuario debe extraer

	inmediatamente sin consultar, modificar o copiar información alguna.
Archivero con candado	Resguardar las bases de datos en archivo físico en un archivero con candado o con llave de seguridad, cuyo acceso sólo será permitido al personal autorizado.
Zona de confidencialidad	Definir una zona de confidencialidad en donde se resguardarán los archivos físicos o equipos de cómputo que contengan las bases de datos, cuya finalidad sea limitar el acceso al personal no autorizado, equipos o aparatos de copiado.
Medidas de seguridad técnicas	
Cuidado de la contraseña personal	Abstenerse de compartir contraseñas personales de la red institucional, las contraseñas, tokens, identificadores o cualquier mecanismo utilizado para la autenticación en un recurso informático.
Actualización de contraseñas	Cambiar las contraseñas cada tres meses por lo menos, a efecto de evitar robo de identidad. En caso de olvido o sospecha de divulgación de una contraseña o mecanismo de autenticación, los usuarios deberán realizar el cambio de estos en los sistemas informáticos.
Reportar fallas	Notificar al área correspondiente cualquier fallo, error, sospecha, violación o incumplimiento a las políticas de seguridad de la información.
No instalar softwares	Abstenerse de descargar en el equipo de cómputo institucional software y aplicaciones de lugares no seguros o dudosa procedencia.
Contraseñas robustas	Construir contraseñas con rol de administrador de forma robusta (longitud adecuada, uso de mayúsculas, minúsculas, caracteres especiales, evitar uso de palabras comunes, etcétera).
Respaldo de información	Realizar respaldos de la información que resida en el equipo de cómputo asignado. La Dirección Tecnologías de la Información, a solicitud del usuario, asesorará y apoyará a los usuarios en el procedimiento para considerando las necesidades propias del área.

UNIDAD DE TRANSPARENCIA

Ciudad de México, XX de XX de 20XX

PROGRAMA DE PROTECCIÓN DE DATOS PERSONALES
LABORATORIOS DE BIOLÓGICOS Y REACTIVOS DE MÉXICO S.A. DE C.V.
ACUERDO DE CONFIDENCIALIDAD

Con fundamento en los artículos 31 y 42 de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados publicada en el Diario Oficial de la Federación el 26 de enero de 2017, es un deber de los responsables del manejo de datos personales establecer controles o mecanismos que tengan por objeto que todas aquellas personas que intervengan en cualquier fase del tratamiento de los datos personales, guarden confidencialidad respecto de éstos, obligación que subsistirá aún después de finalizar sus relaciones con el mismo.

Por lo anterior, en virtud de que de acuerdo con mis actividades en _____ (nombre del área de adscripción), manifiesto expresamente que no utilizaré, en ningún caso la información recibida relacionada con los datos personales, para fines propios y asumo la obligación de no revelar, publicar, enseñar, transmitir o de alguna forma divulgar la información que recibo en cumplimiento a mis obligaciones.

Nombre, cargo y firma

ANEXO 4

GUÍA PARA LA ELABORACIÓN DEL AVISO DE PRIVACIDAD

INTRODUCCIÓN

¿Qué es el aviso de privacidad?

Es un documento físico, electrónico o en cualquier otro formato (por ejemplo, sonoro), a través del cual el responsable informa al titular sobre la existencia y características principales del tratamiento al que serán sometidos sus datos personales. A través del aviso de privacidad se cumple el principio de información que establece la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados.

¿Quién está obligado a generar y poner a disposición un aviso de privacidad?

Aquellos que traten datos personales, en su carácter de responsables, sin importar sus facultades y competencias están obligados a cumplir con el principio de información y poner a disposición del titular el aviso de privacidad de conformidad con lo dispuesto en la Ley General y los Lineamientos, con independencia de que no se requiera el consentimiento del titular para el tratamiento de sus datos personales. Cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos que traten datos personales están obligados a tener aviso de privacidad.

¿En qué momento se debe poner a disposición el aviso de privacidad?

El momento en que el responsable debe poner a disposición de los titulares el aviso de privacidad depende de la forma en que se obtengan los datos personales, es decir, si éstos se recaban directa o indirectamente del titular.

- De forma directa. El aviso de privacidad deberá ponerse a disposición de manera previa a la obtención de los datos personales, independientemente de los formatos o medios físicos y/o electrónicos utilizados para tal fin.
- De forma indirecta. El aviso de privacidad deberá ponerse a disposición en el primer contacto con el titular o previo al aprovechamiento de los datos personales. Como ejemplos de datos personales obtenidos de manera indirecta se pueden considerar los recabados a través de una fuente de acceso público o una transferencia.

CONTENIDO DEL AVISO DE PRIVACIDAD

1. Denominación del responsable y área administrativa – Laboratorios de Biológicos y Reactivos de México S.A. de C.V.
2. Domicilio del responsable - indicar domicilio sin omitir la calle, número, colonia, ciudad, municipio o delegación, código postal y entidad federativa.
3. Datos personales que serán sometidos a tratamiento - datos personales solicitados para el tratamiento que llevará a cabo, tanto los que recaba directamente del titular como aquéllos que obtiene indirectamente, distinguiendo expresamente los datos personales de carácter sensible.
4. Finalidades del tratamiento - El responsable deberá describir puntualmente cada una de las finalidades para las cuales se tratarán los datos personales.
5. Transferencias de datos personales que requieran consentimiento - El responsable deberá señalar las transferencias de datos personales que requieran para su realización del consentimiento del titular, precisando: a) Los destinatarios o terceros receptores, de carácter público o privado, nacional y/o internacional, de los datos personales, ya sea identificando cada uno de éstos por su nombre, denominación o razón social; o bien, clasificándolos por categorías según corresponda, y b) II. Las finalidades de las transferencias de los datos personales relacionadas por cada destinatario o tercero receptor.
6. Mecanismos y medios disponibles para que el titular pueda manifestar previamente su negativa para el tratamiento de sus datos personales - El responsable deberá incluir o informar sobre los mecanismos y medios que tiene habilitados para que el titular pueda manifestar su negativa para el tratamiento de sus datos personales para aquellas finalidades que requieran de su consentimiento.
7. Fundamento legal que faculta al responsable para llevar a cabo el tratamiento.
8. Mecanismos medios y procedimientos disponibles para ejercer los derechos ARCO (Unidad de Transparencia).
9. Domicilio de la Unidad de Transparencia.
10. Medios a través de los cuales el responsable comunicará a los titulares los cambios al aviso de privacidad - El responsable deberá señalar el o los medios disponibles y a través de los cuales hará del conocimiento del titular los cambios o actualizaciones efectuados al aviso de privacidad simplificado e integral.
11. Fecha de elaboración o última actualización

Podrá consultar el Formato de Autoevaluación de Avisos de Privacidad Sector Público, el cual es un cuestionario que tiene como objetivo que el responsable verifique que sus avisos de privacidad contengan los elementos informativos obligatorios y, en su caso, opcionales, este documento de facilitación podrá ser consultado en el siguiente hipervínculo: http://inicio.ifai.org.mx/AvisoPrivacidad/AutoevaluacionResponsableSectorPublico1.docx

Asimismo, se puede consultar el Generador de Avisos de Privacidad para el Sector Público, el cual consiste en una herramienta informática que ha sido desarrollada para facilitar la creación de avisos de privacidad que los responsables del tratamiento de datos personales, del sector público y privado, tienen la obligación de poner a disposición de los titulares de estos, conforme a la normativa que les resulta aplicable. El cual se encuentra disponible en el siguiente hipervínculo:
http://gapsectorpublico.inai.org.mx/

Modelo Aviso de privacidad

AVISO DE PRIVACIDAD

Laboratorios de Biológicos y Reactivos de México S.A. de C.V. a través de la _____ (área administrativa responsable) con domicilio en [indicar vialidad, número, colonia o localidad, ciudad, municipio o alcaldía, código postal y entidad federativa del domicilio del sujeto obligado], es el responsable del tratamiento de los datos personales que nos proporcione, los cuales serán protegidos conforme a los dispuesto por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y demás normatividad que resulte aplicable.

Los datos personales que recabamos, los utilizaremos para las siguientes finalidades que son necesarias para el servicio que solicita:

a) Finalidad A
b) Finalidad B
c) Finalidad C

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

[listado de datos personales o sus categorías del anexo].

Ejemplo:

Nombre

Dirección

Teléfono

Transferencias de datos personales

Opción 1 Se informa que no se realizarán transferencias de datos personales, salvo aquéllas que sean necesarias para atender requerimientos de información de una autoridad competente, que estén debidamente fundados y motivados.

Opción 2 Le informamos que sus datos personales son compartidos dentro y fuera del país con las siguientes personas, empresas, organizaciones y autoridades distintas a nosotros, para los siguientes fines:

Destinatario de los datos personales	Finalidad
Nombre del tercero receptor o sector al que pertenece	Descripción de la finalidad

Fundamento para el tratamiento de datos personales

Laboratorios de Biológicos y Reactivos de México S.A. de C.V. a través de la _____ (área administrativa responsable) tratará los datos personales antes señalados con fundamento en lo dispuesto en _____.

Derechos ARCO

Usted podrá presentar su solicitud para el ejercicio de los derechos de acceso, rectificación, cancelación u oposición de sus datos personales (derechos ARCO) directamente ante nuestra Unidad de Transparencia, cuyos datos de contacto son los siguientes:

Horario de Atención

8:00 a 17:00 horas

Teléfono y Extensión

55 55 27 52 66

Correo electrónico:

uenlace@birmex.gob.mx

Domicilio

Mariano Escobedo No. 20, Col. Popotla, Alcaldía Miguel Hidalgo, C.P. 11400

Asimismo, usted podrá presentar una solicitud de ejercicio de derechos ARCO a través de la Plataforma Nacional de Transparencia, disponible en http://www.plataformadetransparencia.org.mx y a través de los siguientes medios:

Para la atención de Derechos ARCO, presentar su solicitud a través de la Unidad de Transparencia o por correo electrónico uenlace@birmex.gob.mx

ANEXO
CATEGORÍAS DE DATOS PERSONALES

Datos de identificación	Datos como nombre, domicilio, teléfono particular y/o celular, correo electrónico personal, estado civil, firma, firma electrónica, cartilla militar, lugar y fecha de nacimiento, nacionalidad, edad, fotografía, clave del Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP), nombres de familiares, dependientes y/o beneficiarios.
Datos Laborales	Pueden referirse a los contenidos en las solicitudes de empleo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales, referencias personales, recomendaciones, capacitaciones, documentos de selección, reclutamiento, nombramiento, incidencias, hojas de servicio y otras generadas derivadas de nuestra relación laboral.
Datos patrimoniales	Se refiere a los bienes muebles e inmuebles, ingresos y egresos, cuentas bancarias, seguros, fianzas, afores, historial crediticio, información fiscal, servicios contratados y afines.
Datos sobre procedimientos administrativos y jurisdiccionales	Es aquella información disponible en procedimientos administrativos o juicios en materia laboral, civil, penal, fiscal, mercantil o de cualquier otra rama del Derecho.
Datos académicos	Son los datos que permiten identificar nuestra trayectoria académica y formación profesional como son calificaciones, boletas, constancias, certificados, reconocimientos, títulos, cédulas profesionales.
Datos de tránsito y movimientos migratorios	Información necesaria para nuestro tránsito dentro y fuera de país.
Datos personales sensibles	Datos de salud Datos ideológicos Datos de vida sexual Datos de origen Datos biométricos Datos electrónicos (correos electrónicos particulares, nombres de usuarios, contraseñas, firma electrónica)

SALUD | BIRMEX

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

PROGRAMA DE PROTECCIÓN DE DATOS PERSONALES 2023

2023 Actividades	ENERO	FEBRERO	MARZO	ABRIL	MAYO	JUNIO	JULIO	AGOSTO	SEPTIEMBRE	OCTUBRE	NOVIEMBRE	DICIEMBRE
Inventario de tratamientos de datos personales (5.1)												
Cumplimiento a las Obligaciones (5.2)												
Valuación de medidas de seguridad (5.2.1) Análisis de Brecha												
Medidas de Seguridad Documento de seguridad (5.2.2)												
Confidencialidad (5.2.3)												
Acuerdo de Confidencialidad												
Controles dirigidos a asegurar la confidencialidad que deben guardar todas las personas que intervienen en cualquier fase del tratamiento de datos personales												
Relación de los instrumentos jurídicos mediante los cuales se formaliza la contratación o adhesión a servicios, aplicaciones e infraestructura en el cómputo en la nube y otras materias												
Relación de los instrumentos jurídicos mediante los cuales se formalizan las transferencias de datos personales, y en los cuales el receptor de los datos personales se obliga a garantizar la confidencialidad												
Informar a la Unidad de Transparencia si el área administrativa responsable realiza tratamientos de datos personales por medios automatizados o electrónicos												
Elaborar el aviso de privacidad												
Informe de Actividades (6)												