DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES

UR 410- DIRECCIÓN GENERAL DE POLÍTICA EDUCATIVA, MEJORES PRÁCTICAS Y COOPERACIÓN.

CONTENIDO

I. INTRODUCCIÓN

La información, al ser un conjunto organizado de datos relevantes para uno o más sujetos y del que se extraen conocimientos, debe ser protegida mediante procesos y sistemas diseñados, administrados y mantenidos por una organización, por lo que es necesario establecer, implementar, operar, monitorear y mejorar los procesos y sistemas relativos a la gestión de la seguridad de dicha información obteniendo con esto la total confidencialidad, integridad y disponibilidad de la misma.

El presente Documento de Seguridad se elabora en cumplimiento a lo dispuesto por el artículo 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), señalando el control interno relacionado con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales que aplica la UR 410 – Dirección General de Política Educativa, Mejores Prácticas y Cooperación.

II. OBJETIVO

El principal objetivo de este documento es describir e informar de manera general las medidas de seguridad de carácter administrativo, físico y técnico para la protección de datos personales, adoptadas por la Dirección General de Política Educativa, Mejores Prácticas y Cooperación, con el fin de protegerlos contra el daño, pérdida, alteración, destrucción o uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad de la información en los sistemas manejados en la UR 410.

III. GLOSARIO

Para los efectos del presente Documento de Seguridad para la Protección de Datos Personales, además de las definiciones contenidas en el artículo 3° de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, se entenderá por:

I. **Áreas**: Instancias de los sujetos obligados previstas en los respectivos reglamentos interiores, estatutos orgánicos o instrumentos equivalentes, que cuentan o puedan contar, dar tratamiento, y ser responsables o encargadas de los datos personales. Para el presente documento, será la UR 410;

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

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

IV. **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;

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

VI. **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;

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

VIII. **Ley General**: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados;

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

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

XI. **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;

XII. **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;

XIII. **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;

XIV. **Responsable**: Los sujetos obligados a que se refiere el artículo 1 de la Ley General que deciden sobre el tratamiento de datos personales;

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

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

XVII. **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.

PARTE 1.- INVENTARIO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO

De acuerdo con los Artículos 58 y 59 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público (ACT -PUB/19/12/2017.10), se presenta en este apartado, el inventario de datos personales, así como los sistemas de tratamientos implementados por esta Dirección General de Política Educativa, Mejores Prácticas y Cooperación.

En relación con lo previsto en el artículo 33, fracción III de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, el responsable (SEP) 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;
V. 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.

En cuanto al ciclo de vida de los datos personales en el inventario, el Artículo 59 de los Lineamientos Generales, informa que, aunado a lo dispuesto en el artículo anterior, 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.

Por ello, la Dirección General de Política Educativa, Mejores Prácticas y Cooperación (UR 410), informa que se atienden los procedimientos establecidos en el artículo 31 del Reglamento Interior de la Secretaría de Educación Pública publicada en el Diario Oficial de la Federación el 15 de septiembre de 2020 y posteriores reformas, así como temas relacionados con otorgamiento de becas y con contratación del personal. Los datos personales tratados son los siguientes:

- Datos personales:

Nombre(s), apellidos, edad, domicilio, colonia, demarcación territorial, código postal, capital, estado o municipio, fecha de nacimiento, lugar de nacimiento y fecha de registro civil, nacionalidad, sexo, estado civil, nombre completo del cónyuge o concubina, hijos y abuelos, ocupación, códigos QR en actas de nacimiento, número telefónico (casa y celular), correo electrónico personal, tipo de régimen (separación de bienes o sociedad conyugal); clave de elector, año de registro, emisión y vigencia, Clave Única de Registro de Población, Registro Federal de Contribuyentes, cartilla del servicio, número de cédula profesional, nombre de la licenciatura, posgrado, maestría o doctorado, firma del titular, lugar y fecha donde se expidió; cursos de capacitación, conocimiento de otro idioma, información de su empleo actual y anteriores, referencias personales, hoja única de servicio y acuse de recibo de la Declaración de Situación Patrimonial (si el puesto que ocupara el empleado así lo requiere).

- Datos sensibles:

Constancia de examen médico expedida por Institución Oficial, huella digital, estado de salud, sexo y tipo sanguíneo.

✓ Catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales:

Medios electrónicos:

- Sistema de Administración de Becas Internacionales (SABI)
- [redacted]

Medios Físicos:

- Originales y/o copias de la documentación relacionada con la entrega en propia mano del signatario o servidor públicos en el momento de su contratación.
- Originales y/o copias de la documentación relacionada con el otorgamiento de becas.

✓ Finalidad de cada tratamiento de los datos personales:

Realizar el procedimiento de registro y dar cumplimiento a lo dispuesto en el artículo 31 del Reglamento Interior de la Secretaría de Educación Pública (DOF: 15/09/2020).

También los datos personales que el servidor público proporciona de forma directa a la Jefatura de Departamento de Enlace Administrativo de la UR 410, serán utilizados en el proceso de contratación a través del Sistema Integral de Administración de Personal (SIAPSEP); así como en el Sistema de Honorarios (SIHO); mismos que se utilizan en los procesos de ingreso, baja, modificación, consultas, capacitación y elaboración e integración de su expediente laboral en físico; así como para gestionar la documentación oficial que son: contrato de Honorarios, Constancia de Nombramiento, Fondo de Retiro para los afiliados de la Educación Pública, Seguro de Separación Individualizado, aviso de ingreso, baja o modificación ante el Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado (ISSSTE).

En el caso del otorgamiento de becas, se solicita información que acredite que las personas solicitantes cumplen con los requisitos enlistados en las convocatorias, además de que se gestionan los pagos correspondientes.

✓ Formatos de almacenamiento:

- Ubicación física: Al integrar el expediente en original y/o copia certificada se realiza el registro correspondiente y se resguarda en el archivo destinado para ello de la Subdirección de Relaciones Bilaterales y en la Jefatura de Departamento de Enlace Administrativo de la UR 410.

- Ubicación electrónica: a través de los correos electrónicos: [redacted]

✓ Lista de servidores públicos que tienen acceso a la información:

- [redacted]
- [redacted]
- [redacted]

✓ Nombre completo del encargado de Protección de Datos Personales:

Enlace de Transparencia de la DGPEMPC – [redacted].

✓ Destinatarios o terceros receptores de las transferencias que se efectúen:

Unidades administrativas y órganos desconcentrados de la SEP, autoridades administrativas y judiciales para el ejercicio de sus funciones y/o el enlace de Transparencia para la atención de solicitudes de acceso a la información y el enlace encargado de los temas relacionados con los Sistemas de Portales de Transparencia (SIPOT).

Transmisiones mediante el traslado de soportes físicos:

- La transmisión de datos personales mediante el traslado de soportes físicos se lleva a cabo por medio de mensajero oficial.
- El paquete con datos personales en soportes físicos viaja debidamente sellado, de forma tal que sea perceptible cualquier violación o apertura no autorizada del mismo.
- La entrega del paquete se realiza únicamente si el destinatario acredita su identidad. Para ello, el destinatario presenta una identificación oficial con fotografía y el mensajero recaba nombre, firma y un número de referencia que aparezca en tal identificación, además de la fecha de entrega.
- El mensajero no entrega el paquete si el destinatario no puede acreditar su identidad. En este caso, el mensajero devuelve el paquete al transmisor.
- El transmisor verifica que el mensajero haya entregado el paquete al destinatario. Si el transmisor detecta que dicho paquete fue entregado a otra persona, da inicio al proceso de atención de un incidente.

Transmisiones mediante el traslado en soportes electrónicos:

La transmisión de datos personales mediante el traslado de soportes electrónicos se realizan a los correos electrónicos autorizados por la UR 410: [redacted] así como el correo electrónico que el Titular de los datos haya destinado para tales efectos.

Resguardo de sistemas de datos personales con soportes físicos:

Medidas de seguridad que se han implementado para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.

El ciclo de vida de los datos personales es el siguiente:

1. Obtención de los datos: Los datos personales tratados obran inmersos en los actos de contratación de personal, procedimientos de otorgamiento de becas, y se obtienen ya sea al momento de capturar información en las bases de datos durante el registro en el SABI, o bien, al remitir documentación a la subdirección de Relaciones Bilaterales y/o a la jefatura de departamento de Enlace Administrativo, o por el enlace encargado de los temas relacionados con los Sistemas de Portales de Transparencia (SIPOT).

También, los datos personales tratados por este responsable se obtienen al momento de ingresar a laborar en la Unidad Administrativa, la persona entrega toda la documentación requerida en propia mano o a través de correo electrónico.

2. Almacenamiento: los datos personales son resguardados de la siguiente manera:

- Ubicación física: Expediente físico donde se resguarda el original y/o copia certificada al momento de ingresar a laborar en la Unidad Administrativa, temas relacionados con el derecho de acceso a la información y transparencia. El archivo se encuentra en el interior de las oficinas destinadas para el resguardo y custodia que cuenta con archiveros metálicos para el resguardo de los expedientes y es atendido por personal de apoyo operativo.
- Dichos expedientes físicos se encuentran ubicados en las oficinas ubicadas en Calle de Donceles número 100, Colonia Centro, Demarcación Territorial Cuauhtémoc, Ciudad de México, C.P. 06020. Se ha destinado distintas áreas estratégicas físicas para el resguardo y conservación de la información que trata esta UR 410.
  Al momento de integrar el expediente único de personal “activo” este se resguarda en el archivo de la jefatura del departamento de Enlace Administrativo, en caso de que el personal cause “baja” el expediente se resguarda en el archivo de trámite por 30 años del Enlace Administrativo.
  En el caso de los expedientes de becarios, se resguardan en la subdirección de Relaciones Bilaterales y se conservan durante 3 años en el archivo de trámite.
- Ubicación electrónica: a través de los cómputos destinados para el resguardo y aseguramiento de la información que llega a través de los siguientes correos electrónicos:
  [redacted]
- Uso de los datos: Algunos se utilizan para la integración de las bases de datos para el otorgamiento de becas y temas relacionados con SIPOT. También los datos personales son usados para elaborar Constancias de Nombramiento, Contratos de Prestación de Servicios Profesionales por Honorarios, elaboración e integración del expediente único de personal, así como los formatos de prestaciones laborales.
- Divulgación de los datos: No aplica.
- Bloqueo de los datos: De acuerdo con el artículo 3, fracción IV de la Ley General, donde se precisa que el bloqueo consiste en la identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se

procederá a su cancelación en la base de datos que corresponda. En este sentido, esta Dirección General realiza el proceso de bloqueo conforme lo estipulado en la Ley de la materia, así como lo establecido en los Lineamientos Generales. Una vez que el responsable de la información determine que el proceso de bloqueo puede darse, se asegura que la información cuente con dicha naturaleza para que se proceda realizar el bloqueo de la información.

- Cancelación, supresión o destrucción de los datos: La UR 410 realiza el proceso de cancelación, supresión o destrucción de los datos una vez que se logra identificar que el ciclo de vida de los datos personales se ha cumplido conforme a la normatividad aplicable, por lo que la baja archivística de los datos personales, que resulte en la eliminación, borrado o destrucción de los datos personales se realizará bajo las medidas de seguridad previamente establecidas por este responsable. En el caso de los expedientes únicos del personal, la coordinación Administrativa una vez que el trabajador causa baja, se resguardan en el archivo de trámite por 30 años y transcurrido ese tiempo, son remitidos al archivo de concentración de la SEP.

  En el caso de los expedientes de becarios, los expedientes se resguardan en el archivo de trámite 3 años, mientras que en el archivo de concentración se conservan durante 3 años más, para posteriormente solicitar su baja.

PARTE 2.- FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATAN DATOS PERSONALES

De acuerdo con las funciones y obligaciones establecidas en el artículo 33, fracción II de la Ley General, así como lo establecido en el artículo 57 de los Lineamientos Generales, 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. Bajo este tenor, se informa lo siguiente:

RESPONSABLE 1

- Cargo:

Subdirectora de Relaciones Bilaterales – [redacted].

- Funciones:

Según lo establecido en el artículo 31, fracción VI del Reglamento Interior de la Secretaría de Educación Pública (DOF: 15/09/2020), es la responsable de operar los programas de becas administrados por la DGPEMPC, por lo recaba información de personas interesadas a través del SABI, a fin de verificar que cumplan con los requisitos establecidas en las convocatorias, así como de las personas beneficiarias, con el objetivo de entregar los apoyos a los que son acreedores.
Además, en dicha área se requisitan los formatos correspondientes al SIPOT.

- Obligaciones:

Tiene la obligación de implementar las medias necesarias para asegurar la protección de los datos personales, así como el resguardo, confidencialidad, integridad y disponibilidad de estos.

RESPONSABLE 2

- Cargo:

Jefe de departamento de Enlace Administrativo – [redacted].

- Funciones:

Con fundamento en el artículo 31 del del Reglamento Interior de la Secretaría de Educación Pública (DOF: 15/09/2020), verifica la administración de los recursos humanos, financieros, materiales y servicios generales de la Dirección General Política Educativa, Mejores Prácticas y Cooperación, con el fin de contribuir al cumplimiento de los objetivos institucionales.
Gestiona el proceso de ingreso, contratos de honorarios, pago de remuneraciones, estímulos y recompensas de los servidores públicos, ayuda en los diferentes subsistemas del Servicio Profesional de Carrera, integrar y registrar la información en el Sistema de Administración y Desarrollo del Personal,

coordinar las acciones del sistema de desempeño basado en resultados del personal, gestionar la elaboración de la descripción, perfil y valuación de puestos, así como la identificación y descripción de capacidades técnicas y gestionar los pagos de los compromisos adquiridos por la UR 410 con beneficiarios de los programas de becas.

- Obligaciones:

Dirigir al personal del Enlace Administrativo y asegurar el buen desarrollo de la Unidad

RESPONSABLE 3

- Cargo:

Jefa de departamento de Cooperación para América – [redacted].

- Funciones:

Con fundamento en el artículo 31 del del Reglamento Interior de la Secretaría de Educación Pública (DOF: 15/09/2020), propone y desarrolla el programa de la difusión entre las instituciones involucradas en educación migrante de México, difunde las convocatorias de los programas en los que se requiera profesionales de la educación que atiendan a las comunidades mexicanas o de origen mexicano que radican en Estados Unidos y revisa los proyectos de convenios educativos de carácter bilateral con el propósito de que las partes lleguen a un acuerdo sobre el contenido del mismo, verificando que cuente con los requisitos mínimos vigentes.
Además, funge como Enlace de Transparencia de la Dirección General de Política Educativa, Mejores Prácticas y Cooperación.

- Obligaciones:

Además de cumplir con las funciones establecidas en su perfil de puesto, atiende los requerimientos turnados por la Dirección General de Actualización Normativa, Cultura de la Legalidad y Transparencia, recursos de revisión y solicitudes de información pública turnados por el Sistema de Atención a Solicitudes de Acceso a la Información Pública (SASAISEP), además de reportar en la Plataforma Nacional de Transparencia la información relacionada con el SIPOT.

ENCARGADOS:

- Cargo:

Personal bajo el mando de la Subdirección de Relaciones Bilaterales y de las Jefaturas de Departamento de Enlace Administrativo y de Cooperación para América.

- Funciones:

En el caso del personal adscrito a la Subdirección de Relaciones Bilaterales, se encargan de revisar expedientes, elaborar bases de datos y padrones de pago, además de realizar las actividades correspondientes para la conservación del archivo.
El personal de la Jefatura de departamento de Enlace Administrativo es el encargado de realizar contratos de prestación de servicios profesionales por

honorarios, justificaciones técnicas y funcionales correspondiente a través del Sistema de Honorarios (SIHO), resguardo de expedientes e informes mensuales del personal contratado bajo el régimen de honorarios, realizar los movimientos del personal de estructura (operativo de base, confianza y mando) así como del personal eventual; gestionando la captura de movimientos (alta, baja o reingreso del personal), cambio de datos personales, transferencia de plaza, promociones, licencias y prórroga de nombramientos y consultas a través del Sistema Integral de Administración de Personal SEP (SIAPSEP), operar la inscripción y baja al Fondo de Retiro de los trabajadores de la SEP, así como la modificación de beneficiarios y autorización al pago de liquidación, expedientes de cada trabajador, movimientos afiliatorios, corrección y modificación de datos personales ante el ISSSTE, ejecutar la captura de incidencias, inasistencias y días económicos; consulta del historial de pago, cálculo de tiempo extraordinario;, gestión del archivo de trámite, llevar el control de las metas individuales de los servidores públicos sujetos al Servicio Profesional de Carrera (personal de estructura mandos) así como realizar la validación del expediente (personal de base) del Desarrollo Profesional de Carrera, y elaboración de oficios.

- Obligaciones: Las contempladas en los artículos 58 al 60 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

CONSECUENCIAS DE NO CUMPLIR CON LAS OBLIGACIONES CONTRAIDAS PARA LA SEGURIDAD, RESGUARDO, CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD DE LOS DATOS PERSONALES.

1. Se informará al Órgano Interno de Control de la SEP, a efecto de que se lleven las acciones conducentes para la investigación y lo relacionado con el procedimiento sancionatorio a que haya lugar.
2. Se informará al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) sobre la vulneración ocasionada por algún tercero o por los responsables y encargados.
3. Se llevará a cabo lo establecido en los artículos 39, 40, 41, 152 al 162, 163 al 168 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

PARTE 3.- ANÁLISIS DE RIESGOS

TIPO DE SOPORTE Y CARACTERÍSTICAS DEL LUGAR DONDE SE RESGUARDAN

[redacted]

POLÍTICAS INTERNAS PARA LA GESTIÓN Y TRATAMIENTO DE LOS DATOS PERSONALES O BUENAS PRÁCTICAS

[redacted]

- [redacted]

VALORIZACIÓN RESPECTO DEL RIESGO

[redacted]

PARTE 4.- ANÁLISIS DE BRECHA

[redacted]

- **Medidas de seguridad administrativas**: [redacted]
- **Medidas de seguridad físicas**: [redacted]
- **Medidas de seguridad técnicas**: [redacted]

[redacted]

MEDIDAS DE SEGURIDAD EXISTENTES

MEDIDAS DE SEGURIDAD ADMINISTRATIVAS:

[redacted]

[redacted]

MEDIDAS DE SEGURIDAD FÍSICAS:

[redacted]

[redacted]

MEDIDAS DE SEGURIDAD TÉCNICAS:

[redacted]

[redacted]

MEDIDAS DE SEGURIDAD FALTANTES

[redacted]

[redacted]

PARTE 5.- PLAN DE TRABAJO

[redacted]

- [redacted]
- [redacted]

PARTE 6.- MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Los artículos 33, Fracción VII y 35 fracción VI, de la Ley General establece que el responsable deberá elaborar un documento de seguridad que contenga los mecanismos de monitoreo y revisión de las medidas de seguridad, así como las amenazas y vulneraciones a las que están sujetos los datos personales, y El artículo 63 de los Lineamientos Generales manifiesta que el responsable de los datos personales debe de realizar un constante monitoreo y supervisión periódica de las medidas de seguridad implementadas. De esta manera, 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.

Para cumplir con lo dispuesto en la Ley General, así como en los Lineamientos Generales, se está monitoreando continuamente lo siguiente:

MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD Artículo 63 de los Lineamientos Generales.		
MONITOREO CONSTANTE:	**DESCRIPCIÓN**	**PERIOCIDAD**
I. Los nuevos activos que se incluyan en la gestión de riesgos;	El Enlace de Transparencia revisa de forma periódica aquellos nuevos activos que se incluyen de forma significativa en la gestión de riesgos.	Cada tres meses

II. Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras;	El Enlace de Transparencia y el personal habilitado para ello, revisa de forma constante aquellas nuevas modificaciones que se implementan para los activos, como el cambio o migración tecnológica, riesgos inherentes, transmisión de datos de forma segura y borrado seguro.	Cada que se presenta un cambio sustancial o migración tecnológica de la información de los activos.
III. Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas;	Dentro del equipo del responsable se cuenta con un conjunto de técnicas y maniobras para definir e identificar posibles nuevas amenazas dentro y fuera de nuestra organización a efecto de realizar mejoras constantes para la protección de los datos personales o activos.	Una vez al mes.
IV. La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;	Dentro del equipo del responsable se cuenta con un conjunto de técnicas y maniobras para definir e identificar posibles nuevas vulneraciones que puedan afectar los intereses de los titulares de los datos personales.	Cada dos meses.
V. Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;	Se busca que las amenazas y vulneraciones que se han sufrido no se repitan de nuevo dentro de la organización del responsable.	Cada tres meses.
VI. El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y	Cuando el personal habilitado para el tratamiento de datos personales se percata de	Cada que se identifica el riesgo.

riesgos en conjunto, que resulten en un nivel inaceptable de riesgo,	alguna amenaza o riesgo inaceptable, se realizan las gestiones necesarias para mitigar las consecuencias probables y evitar vulneraciones futuras.	
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 acuerdo con la bitácora de vulneraciones, se determina cuáles han sido los mayores riesgos coincidentes y se ha empleado un monitoreo constante a efecto de que no se repita una vulneración constante.	Cada tres meses.

PARTE 7.- PROGRAMA GENERAL DE CAPACITACIÓN

De manera permanente, se realizarán convocatorias para que el personal conozca lo establecido en la Ley Federal de Transparencia y Acceso a la Información Pública y en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Para ello, se les invitará a inscribirse a los cursos en línea proporcionados por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), a través de su Centro Virtual de Capacitación (CEVINAI) en la siguiente página: https://snt.org.mx/?page_id=1072.

Entre los cuáles se encuentran:

- Gobierno Abierto y Transparencia Proactiva
- Introducción a la Ley General de Transparencia y Acceso a la Información Pública
- Introducción a la Ley Federal de Transparencia y Acceso a la Información Pública
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
- Ley General de Archivos.
- Ética Pública.

IV. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD:

Elaboró:

[redacted]
Jefa de Departamento de Cooperación para América y Enlace de Transparencia.

Aprobó:

[redacted]
Jefe de Departamento de Enlace Administrativo.

Autorizó:

[redacted]
Titular de la Dirección General de Política Educativa, Mejores Prácticas y Cooperación.

Fecha de la última actualización: 4 de junio de 2024.