DOCUMENTO DE SEGURIDAD DEL INSTITUTO NACIONAL DE ASTROFÍSICA, ÓPTICA Y ELECTRÓNICA

ÍNDICE

Introducción

El 26 de enero de 2017 se expidió la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (en lo sucesivo, la Ley General de Datos), la cual tiene como objetivo establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales que estén en posesión de los sujetos obligados.

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

El artículo 35 de la Ley General de Datos establece como una obligación la elaboración de un documento de seguridad, que se define -según la fracción XIV del artículo 3 de la Ley General- como el instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

De conformidad con el artículo 35 de la Ley General de Datos, el documento deberá contener, al menos, la siguiente información:

I. El inventario de datos personales y de los sistemas de tratamiento;
II. Las funciones y obligaciones de las personas que traten datos personales;
III. El análisis de riesgos;
IV. El análisis de brecha;
V. El plan de trabajo;
VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad, y
VII. El programa general de capacitación.

En ese sentido, en cumplimiento de las obligaciones antes descritas, a continuación, se presenta el documento de seguridad del Instituto Nacional de Astrofísica, Óptica y Electrónica.

I. Objetivo

Establecer los procedimientos implementados en materia de seguridad y protección en el tratamiento de datos personales que son recabados por los órganos administrativos que conforman la estructura de la Secretaría General de Gobierno en el marco de sus atribuciones conferidas en las disposiciones legales aplicables, y a efectos de dar cumplimiento a los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad, previstos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligado y Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Instituto Nacional de Astrofísica, Óptica y Electrónica.

II. Marco Normativo

- Constitución Política de los Estados Unidos Mexicanos.
- Ley Orgánica de la Administración Pública Federal.
- Ley General de Transparencia y Acceso a la Información Pública.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Ley Federal de Transparencia y Acceso a la Información Pública.
- Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares
- Reglamento de la Ley General de Población.
- Lineamientos generales de protección de datos personales para el sector público.
- Lineamientos que establecen los parámetros, modalidades y procedimiento para la portabilidad de datos personales.

III. Ámbito de Aplicación

De conformidad con el artículo 35 de la LGDPPSO, el responsable deberá elaborar un documento de seguridad que contenga: el inventario de datos personales y de los sistemas de tratamiento; las funciones y obligaciones de las personas que traten datos personales; el análisis de riesgos; el análisis de brecha; el plan de trabajo; los mecanismos de monitoreo y revisión de las medidas de seguridad y, el programa general de capacitación.

El presente documento es de carácter obligatorio para todas las áreas del Instituto que reciban, procesen, almacenen y organicen bases de datos en sistemas o expedientes (físicos y electrónicos) que contengan datos personales.

Todas las personas servidoras públicas con acceso a datos personales, deberán ser sensibilizados y capacitados obligatoriamente con el fin de que conozcan y apliquen las medidas de seguridad pertinentes que garanticen que cada una de las fases del tratamiento de los datos personales se cumplan a cabalidad. Todas las personas servidoras públicas tratarán los datos personales con responsabilidad y acatarán las medidas impuestas para ese fin.

Las obligaciones de las y los operadores de datos personales dentro de esta entidad, deberán guardar confidencialidad sobre la información a la que tengan acceso dentro del Instituto; deberán capacitarse en temas de datos personales; deberán dar aviso sobre cualquiera que sea el caso de vulneración de datos personales.

Además de las funciones y obligaciones de las personas servidoras públicas involucradas, establecidas de manera específica en el análisis de cada uno de los Sistemas, de manera general deberán observar lo siguiente:

Funciones genéricas:

- Establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

- Establecer y documentar los procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales que lleve a cabo, en los cuales se incluyan los periodos de conservación de estos.
- Cuando no sean necesarios, suprimir los datos de forma adecuada.

Obligaciones genéricas:

- Observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales.
- Guardar confidencialidad sobre la información que conozcan en el desarrollo de sus actividades.
- Tratar los datos personales de manera adecuada, pertinente y limitado a lo necesario.
- Contar con capacitación en materia de tratamiento de datos personales.
- Dar aviso a los superiores jerárquicos, ante cualquier acción que pueda poner en riesgo los datos personales y, en general, que puedan vulnerar la seguridad de los datos personales.

Las personas servidoras públicas responsables del tratamiento de datos personales en todo momento deberán observar los principios generales, así como adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos.

Es importante mencionar que la obligación de confidencialidad debe subsistir aún después de que las personas servidoras públicas hayan finalizado su participación en el tratamiento de los datos personales porque hayan cambiado de funciones y aun cuando la relación laboral con el Organismo haya concluido.

Niveles de Protección de los Datos Personales

Las medidas de seguridad que son aplicables a cada uno de los sistemas a cargo de la INAOE deberán considerar el tipo de datos personales que contiene, lo cual determinan el nivel de protección requerido, siendo básico, medio o alto, como a continuación se establece:

Nivel de Protección Básico:

a) Datos de identificación: Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, firma electrónica, RFC, CURP, cartilla militar, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y beneficiarios, fotografía, costumbres, idioma o lengua, entre otros.

b) Datos laborales: Documentos de reclutamiento y selección, de nombramiento, de incidencia, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales, referencias personales, entre otros.

Nivel de Protección Medio:

a) Datos patrimoniales: Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados, referencias personales, entre otros.

b) Datos sobre procedimientos administrativos seguidos en forma de juicio y/o procesos jurisdiccionales: Información relativa a una persona que se encuentre sujeta como parte o tercero en torno a un procedimiento administrativo seguido en forma de juicio o proceso jurisdiccional en materia laboral, civil, familiar, penal, de justicia para adolescentes, amparo o administrativa, con independencia de su etapa de trámite

c) Datos académicos: Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros.

d) Datos de tránsito y movimientos migratorios: Información relativa al tránsito de las personas dentro y fuera del país e información migratoria de las personas, entre otros.

Nivel de Protección Alto:
a) Datos ideológicos:

Creencia religiosa, ideología, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y asociaciones religiosas, entre otros.

b) Datos de salud: Estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias adictivas, uso de aparatos oftalmológicos, ortopédicos, auditivos y prótesis, entre otros.

c) Características personales: Tipo de sangre, ADN, huella dactilar u otros análogos.

d) Características físicas: Color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros.

e) Vida sexual: Preferencia sexual, hábitos sexuales, entre otros.

f) Origen: Étnico y racial. El Instituto Nacional de Astrofísica, Óptica y Electrónica, a través de las Unidades Administrativas, debe asegurar de acuerdo con la naturaleza de los datos contenidos en los sistemas de datos personales que custodia, los niveles de protección conforme a su grado de confidencialidad, disponibilidad e integridad.

IV.- Inventario de Sistemas de Tratamiento de Datos Personales

Conforme lo dispuesto en el artículo 33, fracción III, de la Ley General, los Sujetos Obligados deben elaborar un inventario de datos personales y acorde con lo previsto en los artículos 58 y 59 de los Lineamientos Generales, los cuales establecen lo siguiente:

Inventario de datos personales

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

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

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

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

I. *La obtención de los datos personales;*
II. *El almacenamiento de los datos personales;*
III. *El uso de los datos personales conforme a su acceso, manejo, aprovechamiento, monitoreo y procesamiento, incluyendo los sistemas físicos y/o electrónicos utilizados para tal fin;*

La divulgación de los datos personales considerando las remisiones y transferencias que, en su caso, se efectúen;

IV. El bloqueo de los datos personales, en su caso, y
V. 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.

Además, como se señala en la fracción I del artículo 35 de la Ley General, este inventario forma parte del Documento de Seguridad.

a) Funciones genéricas en cualquier nivel de tratamiento

• Tratar los datos personales con responsabilidad y las medidas de seguridad que se haya establecido para tal fin.

b) Obligaciones genéricas en cualquier nivel de tratamiento

• Guardar confidencialidad sobre la información que conozcan en el desarrollo de sus actividades.

• Estar capacitado en materia de tratamiento de datos personales.

• Avisar a los superiores jerárquicos, ante cualquier acción que pueda poner en riesgo los datos personales, y en general que puedan vulnerar la seguridad de los datos personales.

• Las siguientes direcciones son las áreas administrativas que recaban datos personales, los cuales se encuentran tanto en soportes electrónicos como físico.

Subdirección de Recursos Humanos.
Dirección de Formación Académica.
Dirección de Investigación y Desarrollo Tecnológico.
Subdirección de Finanzas y Control Presupuestal.
Subdirección de Recursos Materiales y Servicios Generales.

Las categorías con que cuenta el Instituto Nacional de Astrofísica, óptica y Electrónica son consistentes en:

• **Datos académicos**: Títulos, cédula profesional, certificados, reconocimientos.

• **Datos biométricos**: Huella dactilar.

• **Datos de identificación y contacto**: Nombre, estado civil, Registro Federal de Contribuyentes, Clave Única de Registro de Población, lugar de nacimiento, fecha de nacimiento, nacionalidad, domicilio, teléfono celular, correo electrónico, firma autógrafa, edad, fotografía y referencias personales.

• **Datos laborales:** Puesto o cargo que desempeña, domicilio de trabajo, correo electrónico institucional, teléfono institucional, referencias laborales, información que integra el expediente personal (reclutamiento, selección y contrataciones), constancias de capacitación.

• **Datos legales:** Juicios, amparos o procesos administrativos de los servidores públicos.

• **Datos patrimoniales:** Cuentas bancarias, ingresos.

Los datos descritos se obtienen de los documentos y formatos físicos que presentan las personas servidoras públicas que laboran en el Instituto Nacional de Astrofísica, Óptica y Electrónica, personas que prestan servicio social y/o prácticas profesionales, clientes y proveedores.

El nivel de seguridad de los expedientes físicos y electrónicos, así como de los sistemas que contienen datos personales es de un nivel medio; todas las áreas garantizarán la confidencialidad, integridad y disponibilidad de los datos personales descritos en el cuerpo normativo.

II. Medidas de Seguridad

De acuerdo con lo establecido en el artículo 3, fracción XX de la LGDPPSO, las medidas son el conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales.

Las medidas de seguridad administrativas son consistentes en 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 un 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.

Las medidas de seguridad técnicas se conforman por un 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.

El Instituto cuenta con medidas de seguridad:

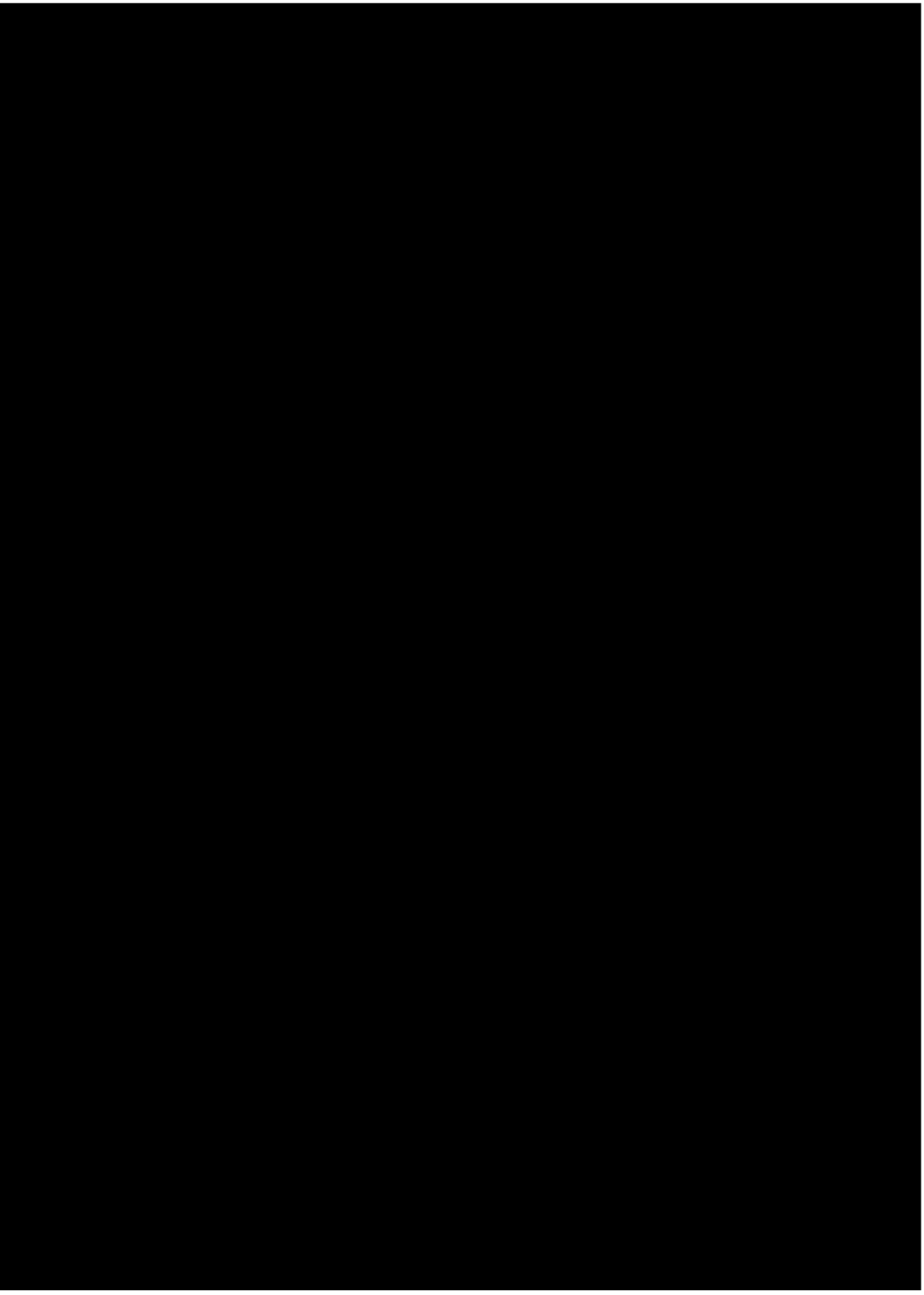
• **Administrativas**: Consistentes en identificación, clasificación y borrado seguro de información, sensibilización del personal, capacitación en materia de protección de datos personales y supervisión por parte del Comité de Transparencia del Instituto Nacional de Astrofísica, óptica y Electrónica.

• **Físicas:** La coordinación de archivos vigila que los archivos físicos sean consultados por el personal autorizado; las instalaciones del archivo de concentración, el archivo de trámite y los documentos generados en cada una de las áreas de la entidad cuentan con vigilancia permanente por parte del personal que genera la información y del personal de vigilancia. La entidad cuenta con un circuito cerrado que permite un mayor control de la documentación.

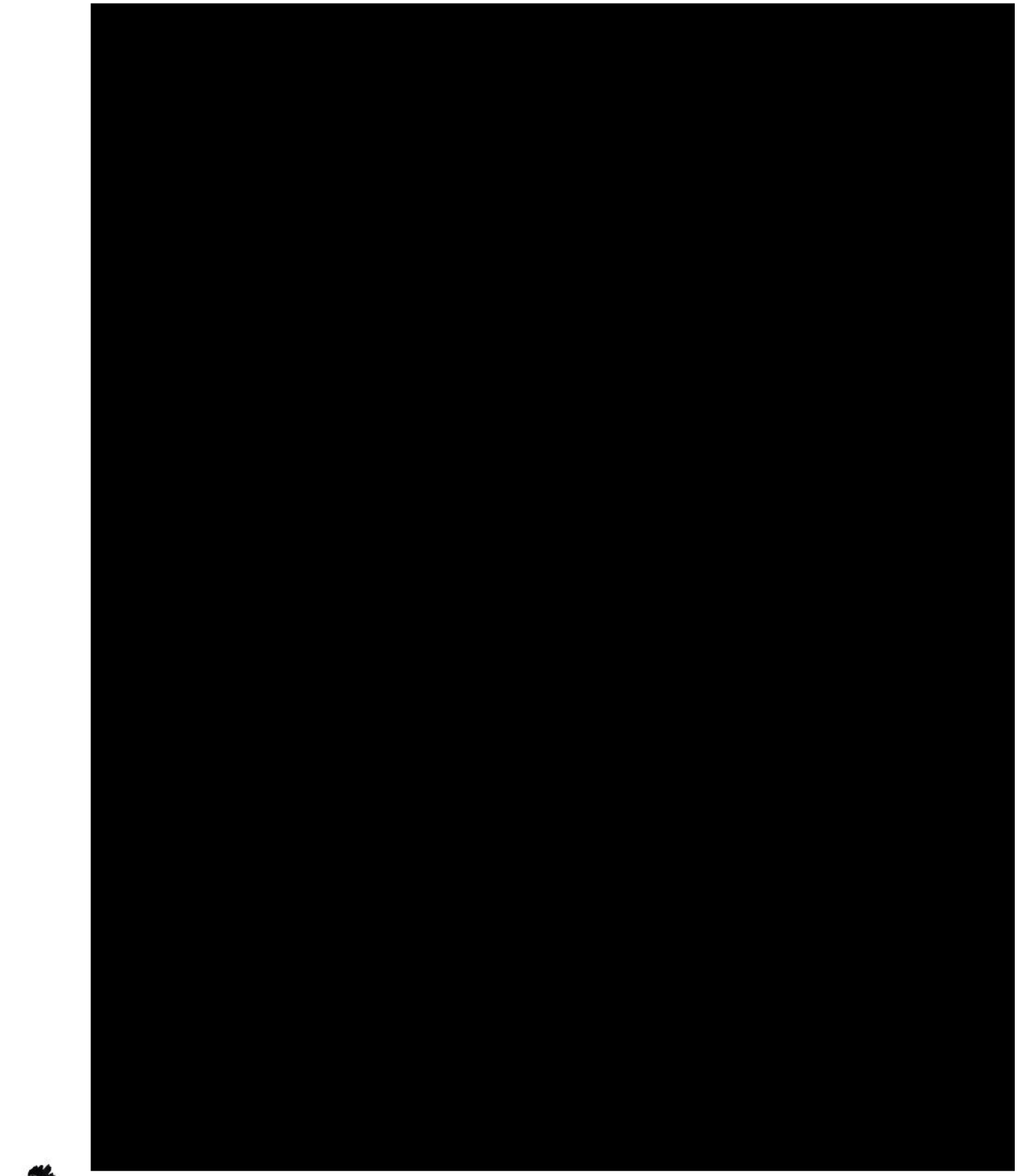
• **Técnicas**: Se consideran medidas de seguridad técnicas las aplicables a los sistemas de tratamiento de datos en soporte electrónico resguardados.

IV.- Análisis de riesgo

[redacted]

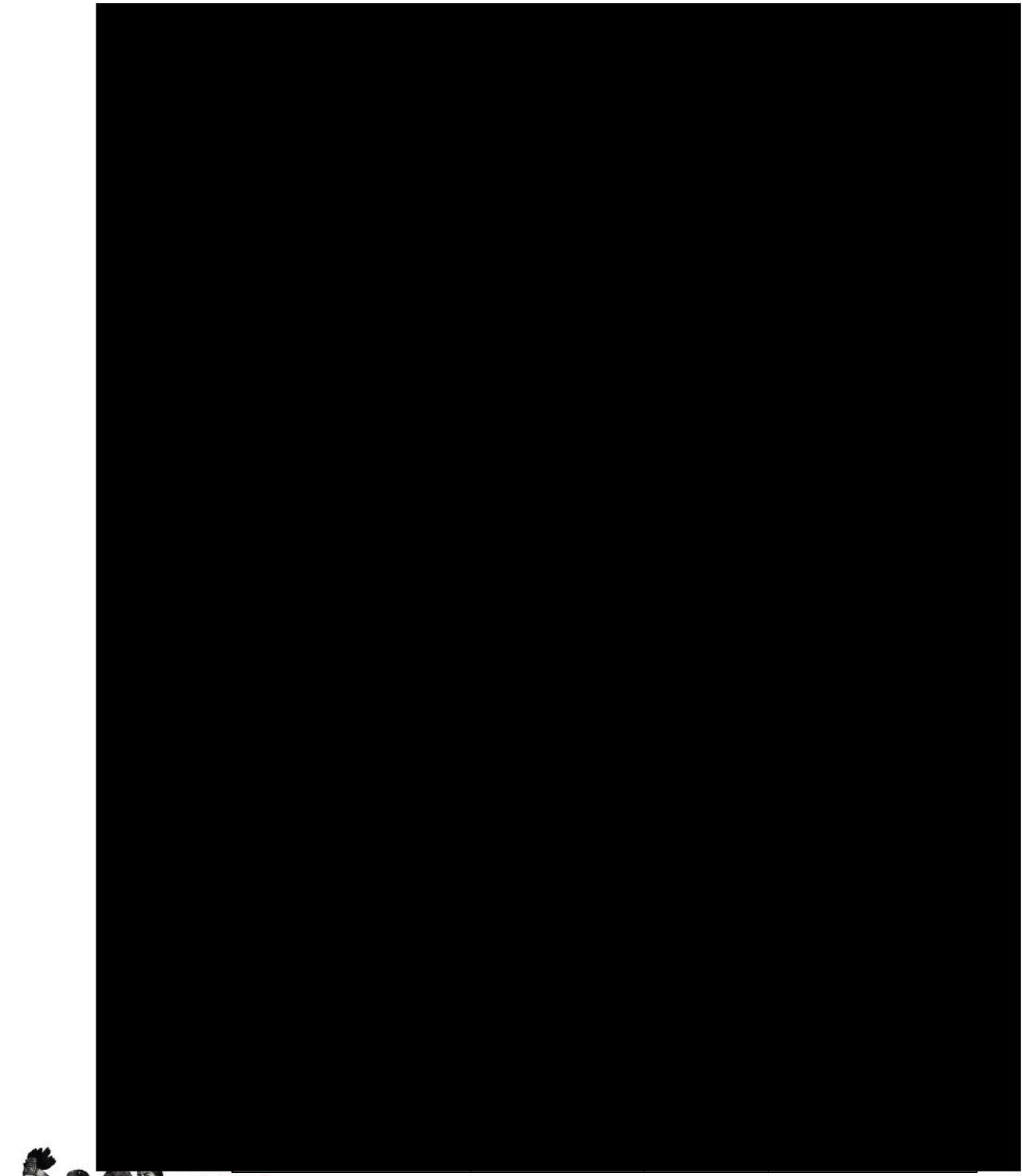


Luis Enrique Erro No. 1, CP. 72840, Tonantzintla, Pue., México. Tel: (222) 266 3100 ext. 3102 diradm@inaoep.mx www.inaoep.mx



[redacted]

Luis Enrique Erro No. 1, CP. 72840, Tonantzintla, Pue., México. Tel: (222) 266 3100 ext. 3102 diradm@inaoep.mx www.inaoep.mx

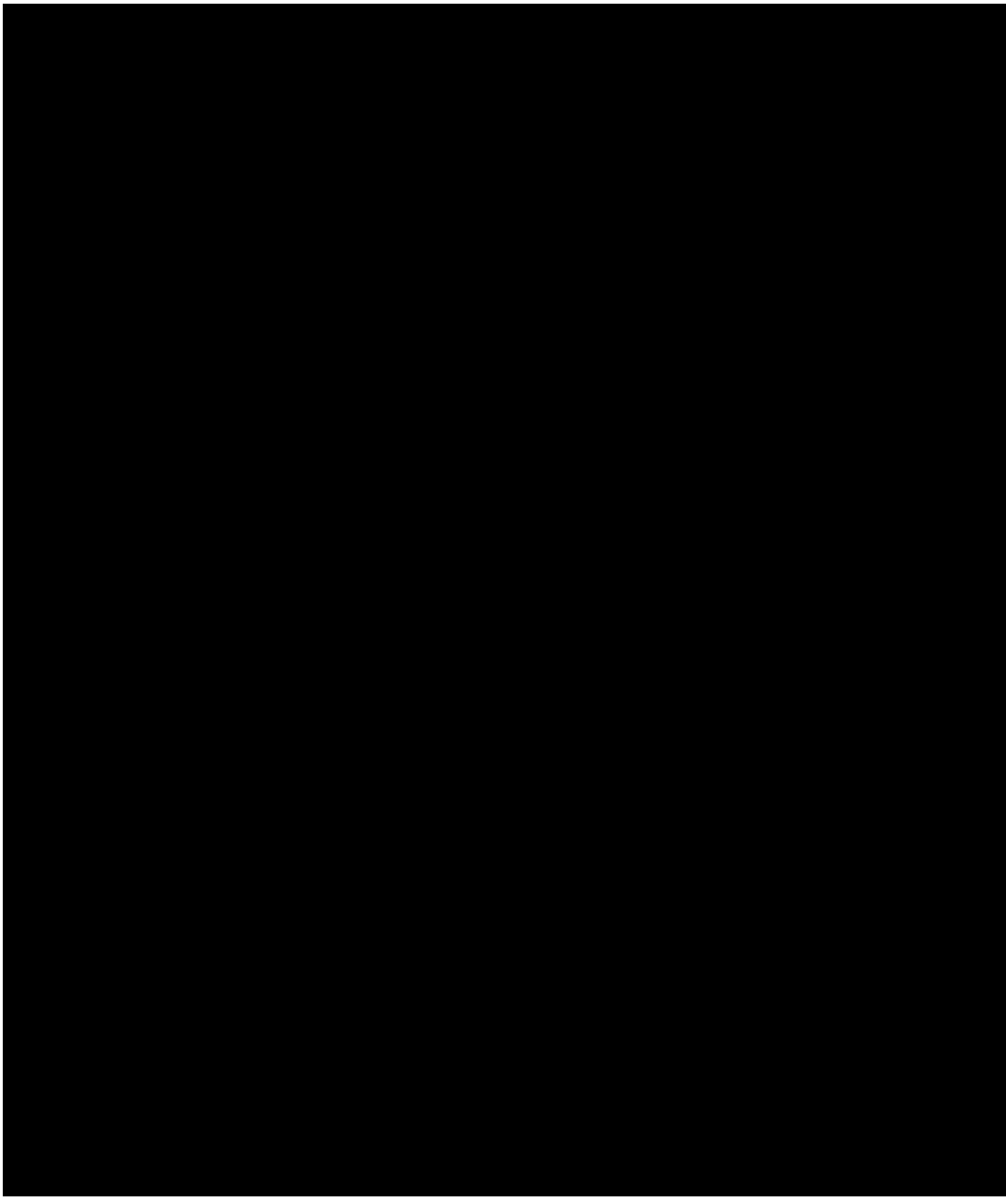


V.- Análisis de brecha

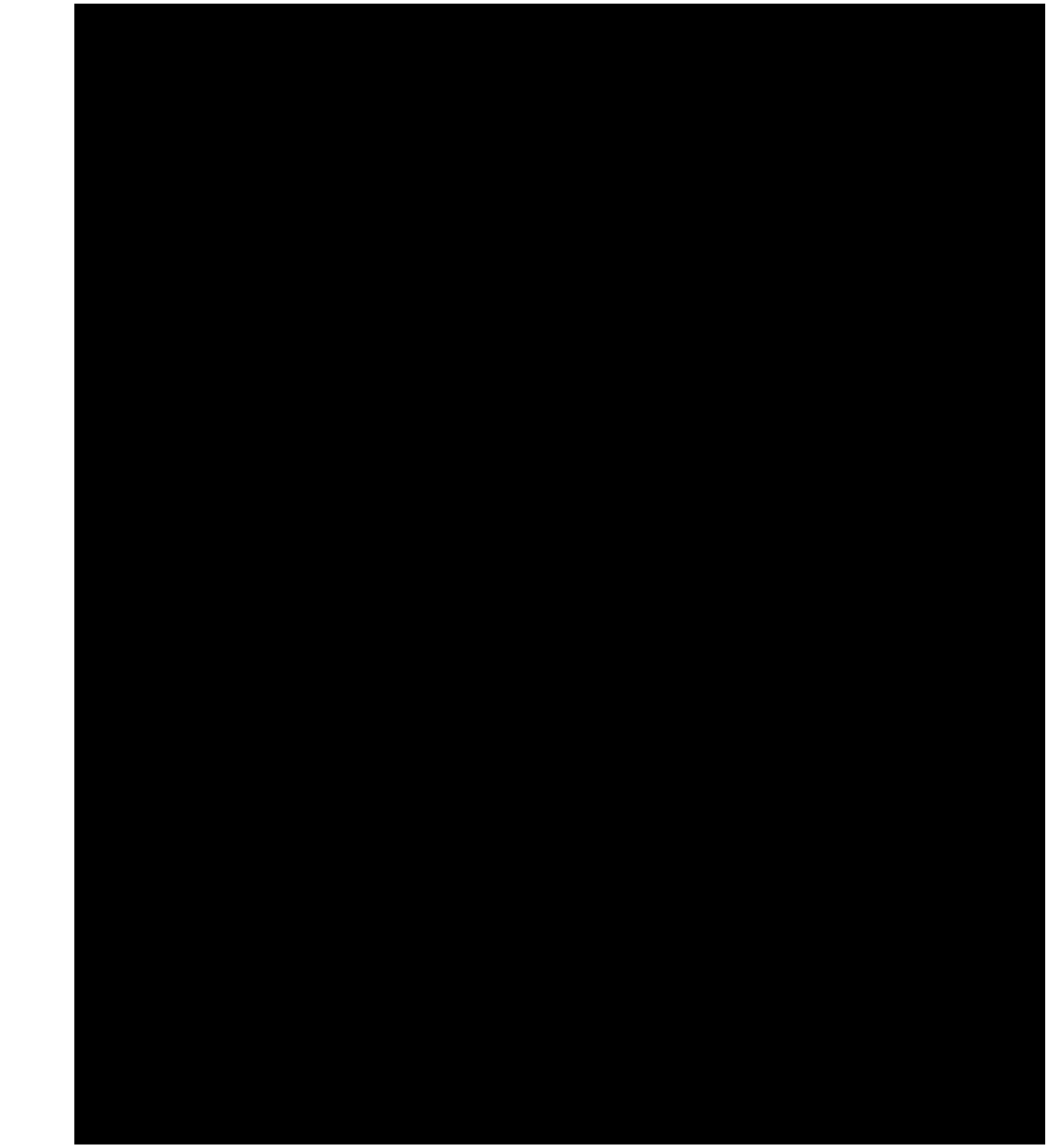
VI.- Plan de trabajo

Con los resultados obtenidos, en cumplimiento a lo dispuesto por los artículos 33, fracción VI y 35, fracción V de la Ley General de Protección de Dato Personales en Posesión de Sujetos Obligados, y 62 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, se determinó el 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 en el INAOE.

El personal del INAOE que maneja datos personales deberá participar en programas de c



Luis Enrique Erro No. 1, CP. 72840, Tonantzintla, Pue., México. Tel: (222) 266 3100 ext. 3102 diradm@inaoep.mx www.inaoep.mx



VII.- Mecanismos de monitoreo y revisión de las medidas de seguridad

Si usted desea ejercer alguno de los derechos de Acceso, Rectificación, Cancelación u Oposición al tratamiento de sus datos personales, conocidos como derechos ARCO, es importante que tome en cuenta que el derecho a la protección de datos personales es un derecho personalísimo, por lo que sólo usted, como titular de los datos personales o, en su caso, su representante legal podrán solicitarlo. A continuación, le explicamos el procedimiento a seguir para la presentación y atención de una solicitud de ejercicio de derechos ARCO:

A continuación, se hace mención de los requisitos para la presentación de una solicitud de ejercicio de derechos ARCO.

1. Usted puede registrarse en la Plataforma Nacional de Transparencia (PNT) para formular la solicitud por vía remota, para ello basta que ingrese a la página de internet www.plataformadetransparencia.org.mx y genere una cuenta personal con los siguientes datos: correo electrónico, nombre, contraseña y texto de verificación. Una vez generada la cuenta, podrá elegir la opción “Solicitud Datos Personales” y enseguida se mostrará el formulario para llenar los datos respectivos.

Toda solicitud de ejercicio de derechos ARCO deberá contener la siguiente información

• Nombre del titular de los datos personales.
• Documentos que acrediten la identidad del titular.
• En su caso, nombre del representante legal del titular y documentos para acreditar su identidad y personalidad.
• Especificar el domicilio o cualquier otro medio para recibir notificaciones.
• Descripción clara y precisa de los datos personales que se quieran rectificar, cancelar u oponerse a su tratamiento.
• Descripción del derecho que se quiere ejercer o de lo que solicita el titular.

• En su caso, documentos o información que faciliten la localización de los datos personales, entre ella, la unidad administrativa responsable que trata los datos.

Requisitos específicos. Además de la información general antes señalada, dependiendo del derecho que desee ejercer, deberá incluir la siguiente información en la solicitud:

- **Derecho de ACCESO:** la modalidad en la que prefiere que se reproduzcan los datos personales solicitados.
- **Derecho de RECTIFICACIÓN**: las modificaciones que solicita que se realicen a los datos personales, así como aportar los documentos que sustenten la solicitud.
- **Derecho de CANCELACIÓN**: las causas que motivan la petición de que se eliminen los datos de los archivos, registros o bases de datos del responsable del tratamiento.
- **Derecho de OPOSICIÓN**: las causas legítimas o la situación específica que lo llegan a solicitar que finalice el tratamiento de sus datos personales, así como el daño o perjuicio que le causaría que dicho tratamiento continúe; o bien, deberá indicar las finalidades específicas respecto de las cuales desea ejercer este derecho.

¿Cómo se puede acreditar la identidad en el trámite de las solicitudes de derechos ARCO?

La parte interesada, titular del derecho:

Identificación oficial, tales como:

- Credencial para votar;
- Pasaporte;
- Licencia para conducir; y,
- Documento migratorio.

Debiéndose presentar el original, para dejar la copia simple cotejada en los antecedentes.

Si se ejerce el derecho a través de representante:

Identificación de la parte interesada y del representante legal:

- Credencial para votar;
- Pasaporte;
- Licencia para conducir; y,
- Documento migratorio.

Debiéndose presentar los originales, para dejar las copias simples cotejadas en los antecedentes.

Documento con el que se justifique la personalidad:

Si el representante es persona física:

- Carta poder simple suscrita ante dos testigos, anexando copia simple de las identificaciones de quienes la firman (titular, representante y testigos);
- Instrumento público, pasado ante la fe de un notario público; o
- Acudiendo personalmente la parte interesada (titular del derecho) y el representante, ambos debidamente identificados, a la Unidad de Enlace de Información, a hacer constar el otorgamiento de la representación, mediante una comparecencia, en presencia del titular del área.
- Si el representante es de una persona moral, únicamente se podrá acreditar mediante instrumento público notariado.

Si se ejerce en representación de los menores, en estado de interdicción, y fallecidos:

Solicitud de derechos ARCO de **menores:**

Cuando los **padres** ejercen la patria potestad:

- Acta de nacimiento del menor.

- Identificación oficial del padre o la madre, según quien haya presentado la solicitud.
- Manifestación, bajo protesta de decir verdad, que actualmente no tiene impedimento o limitación legal alguna para ejercer la patria potestad y representación del menor.

Cuando **persona distinta** ejerce la patria potestad:

- Acta de nacimiento del menor.
- Documento legal que acredite la posesión de la patria potestad.
- Identificación oficial de quien presenta la solicitud y posee la patria potestad.
- Manifestación, bajo protesta de decir verdad, que ejerce la patria potestad del menor y no se encuentra dentro de alguno de los supuestos legales de impedimento o limitación.

Cuando un **tutor** es quien ejerce la patria potestad:

- Acta de nacimiento del menor.
- Documento legal que acredite la tutela.
- Identificación oficial del tutor.
- Manifestación, bajo protesta de decir verdad, que ejerce la tutela del menor y no se encuentra dentro de alguno de los supuestos legales de suspensión o limitación de la tutela.

Solicitudes de derechos ARCO de **interdicción o incapacidad** legal:

- Identificación oficial del titular de los datos personales.
- Documento legal de designación del tutor.
- Identificación oficial del tutor.
- Manifestación, bajo protesta de decir verdad, que ejerce la patria potestad del menor y no se encuentra dentro de alguno de los supuestos legales de impedimento o limitación.

Solicitudes de derechos ARCO de **personas fallecidas**:

- Acta de defunción.
- Documento que acredite algún interés de quien presenta la solicitud.

- En caso de ser familiar, podrá exhibir el instrumento con el que se justifique la filiación.
- En caso de no ser familiar, deberá exhibir el instrumento donde se justifique que la representación de los derechos recayó sobre esa persona.

➢ Identificación oficial de quien presenta la solicitud.
➢ Manifestación, bajo protesta de decir verdad, los motivos y fines para los cuales son solicitados.

Si la persona fallecida es un menor, podrá solicitarse por quien ejerza la patria potestad.

La Unidad de Enlace, cuenta con un plazo de 20 días hábiles, contados a partir del día hábil siguiente a la recepción de la solicitud, para notificar la repuesta recaída a la misma.

¿Cuáles son los plazos de atención de las solicitudes de derechos ARCO?

Si procedió el ejercicio del derecho, se le comunicarán las acciones necesarias para hacerlo efectivo, contando la Unidad de Enlace, con un plazo de 15 días hábiles, contados a partir del día hábil siguiente al que se le haya notificado la respuesta.

La Unidad de Enlace, podrá ampliar los términos citados, hasta por un periodo que no podrá exceder de 10 días hábiles adicionales, siempre y cuando existan causas justificables que así lo ameriten.

Si no procedió el ejercicio del derecho ARCO, la Unidad de Enlace, informará a la parte interesada la respuesta a la solicitud, exponiendo los motivos de la improcedencia. Para este supuesto, se deberá notificar la respuesta dentro del plazo de 20 días hábiles

VIII.- Programa de capacitación

Atendiendo a lo mencionado en el artículo 30, fracción III, de la Ley General, el Centro está comprometido en un programa de capacitación y que busque formar al personal en el tema de protección de Datos Personales. A su vez, el artículo 48 de los Lineamientos generales menciona que dicho plan de

capacitación deberá establecerse de forma anual, siendo aprobado, coordinado y supervisado por el Comité de Transparencia.

La Unidad de Transparencia se encargará, junto al Comité de Transparencia, de coordinar la capacitación continua y especializada del personal que integren el Instituto. Siendo el Comité de Transparencia que, entre sus atribuciones, incluye el establecer programas de capacitación y actualización para la debida formación de servidores públicos en materia de Transparencia y Protección de Datos Personales.

IX.- Actualización del documento de seguridad.

El artículo 36 de la LGPDPPSO establece la obligación de la actualización del documento de seguridad cuando ocurran los siguientes eventos:

I. Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;
II. Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;
III. Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida, y
IV. Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.
En ese sentido, el Comité de Transparencia deberá estar atento a la actualización de alguno de los supuestos antes citado, para, en su caso, actualizar el presente documento de seguridad.