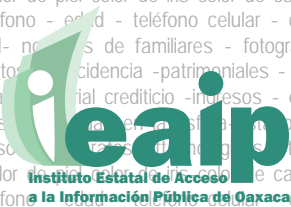




MANUAL

Protección de Datos Personales

OAXACA



Directorio

Genaro V. Vásquez Colmenares
Comisionado Presidente

Raúl Ávila Ortiz
Comisionado

Alicia Aguilar Castro
Comisionada

Luis Antonio Ortiz Vásquez
Secretario General

Adriana Vasseur Sánchez
Secretaria Técnica

Jorge Zárate Medina
Director Administrativo

Melina Reyes Escamilla
Directora Jurídica

Ma. Elisa Ruíz Hernández
Directora de Promoción,
Comunicación y Capacitación

Créditos

Coordinación
Genaro V. Vásquez Colmenares
Comisionado Presidente

Elaboración
Rosario Ponce de León Cortés
Titular de la Unidad del Registro Estatal
de Protección de Datos Personales

Formación y Diseño:
Mayra Victoria Hernández Luis

Primera edición, Agosto 2009
Instituto Estatal de Acceso a la Información Pública de Oaxaca
Amapolas N. 510, colonia Reforma, C.P. 68050, Oaxaca de Juárez, Oax.
Ejemplar de distribución gratuita, prohibida su venta.

1
uno
PÁGINA
09

Presentación.....	Pág. 7
Objetivos.....	Pág. 8
Principios generales	Pág. 9
Protección de datos de carácter personal.....	Pág. 11
Datos de carácter personal.....	Pág. 13
Sistemas de Datos Personales.....	Pág. 16
Tratamiento de Datos Personales.....	Pág. 17
Procedencia de los Datos Personales.....	Pág. 19
Cesión de los Datos Personales.....	Pág. 21
Acceso a Datos Personales por cuenta de terceros.....	Pág. 22

2
dos
PÁGINA
23

Principios que deben observar los Sujetos Obligados en el tratamiento de los Sistemas de Datos Personales	Pág. 25
Licitud de los Datos Personales.....	Pág. 27
Información a los interesados.....	Pág. 27
Consentimiento del interesado en la transmisión de Datos Personales.....	Pág. 29
Calidad de los Datos Personales.....	Pág. 32
Confidencialidad de los Datos Personales.....	Pág. 33
Seguridad de los Datos Personales.....	Pág. 35

3
tres
PÁGINA
35

Recomendaciones sobre medidas de seguridad aplicables a los Sistemas de Datos Personales	Pág. 37
Seguridad de los Sistemas de Datos Personales.....	Pág. 39
Recomendaciones a los Sistemas de Datos Personales en soportes físicos y automatizados.....	Pág. 45

4
cuatro
PÁGINA
55

Derechos en materia de Datos Personales	Pág. 57
Los derechos de los interesados.....	Pág. 59
La tutela de los derechos.....	Pág. 61
Del procedimiento personal de una solicitud de Acceso a la Información.....	Pág. 62

5
cinco
PÁGINA
61

Del Registro Estatal de Protección de Datos Personales y las responsabilidades y sanciones de los Sujetos Obligados	Pág. 71
El Registro Estatal de Protección de Datos Personales.....	Pág. 73
Inscripción de los Sistemas.....	Pág. 74
Modificación de los Sistemas.....	Pág. 75
Cancelación de los Sistemas.....	Pág. 76
La protestad sancionadora.....	Pág. 77
Anexos.....	Pág. 79
Vínculos de interés / Referencias documentales.....	Pág. 99

Presentación

El derecho a la intimidad personal y familiar es una garantía fundamental consagrada en los artículos 16 de la Constitución Política de los Estados Unidos Mexicanos y 14 de la Constitución Política del Estado Libre y Soberano de Oaxaca.

La intimidad, entendida como la esfera dentro de la cual el individuo desarrolla las facetas más reservadas de su vida, ha sido objeto de una amplia protección jurídica, que paradójicamente con la expansión de los medios informativos corre el riesgo de ser vulnerada.

De ahí la necesidad de diseñar nuevas técnicas legales e informativas que aseguren la privacidad de la persona y la inviolabilidad de sus referentes personales de toda índole; Por lo que hace falta precisar las características de la protección integral de esas garantías frente a la intervención de cualquier autoridad o corporación - y en algunos casos de la propia familia - para delimitar el ámbito privado, y garantizar plenamente la libertad personal.

No obstante el progresivo desarrollo de las técnicas de recolección, almacenamiento de datos y acceso a los mismos, es evidente que constituyen una amenaza real para la privacidad personal, la cual aun considerada aisladamente, tiene una trascendente significación intrínseca por su enlace recíproco con la sociedad. La confidencialidad de esos datos debe permanecer reservada.

Considerando que la Ley de Protección de Datos Personales, publicada el 23 de Agosto de 2008, tiene como objeto garantizar la Protección de Datos Personales, así como regular su registro, almacenamiento, distribución, transmisión, modificación, eliminación, duración, y en general, su tratamiento, siempre que estos estén asentados en archivos, registros, base de datos, u otros medios similares en soporte manual o automatizado que estén en poder de los Sujetos Obligados.

En consecuencia, el presente Manual de Protección de Datos Personales, responde a la necesidad de crear una herramienta dinámica y de fácil consulta, que apoye al desarrollo de sistemas protectores de los Datos Personales en poder de los Sujetos Obligados.

Las disposiciones de la Ley de la materia, los lineamientos emitidos por el Consejo General del Instituto Estatal de Acceso a la Información Pública de Oaxaca y las normas establecidas por la Ley de Transparencia y Acceso a la Información Pública para el Estado de Oaxaca en su Título Segundo, constituyen la base del presente documento.

Objetivo General:

Dar a conocer las políticas y procedimientos de los Sistemas de Datos Personales desarrollados por el IEAIP, los cuales deberán ser respetados por los Sujetos Obligados a través de los responsables, encargados y usuarios del tratamiento de los sistemas establecidos. En esta forma quedan garantizados el manejo, la seguridad, la protección, la confidencialidad y el destino de todo dato personal que haya llegado al poder de los Sujetos Obligados ya sea de forma física o automatizada.

La sujeción a las normas relativas permitirá evitar la pérdida, alteración, transmisión no autorizada y mal uso, asegurando su integridad y conservación. De lo anterior se desprenden los siguientes:

Objetivos Específicos:

Salvaguardar los principios y establecer los procedimientos que deban seguir los Sujetos Obligados en el tratamiento de los Sistemas de Datos Personales contra cualquier intento de acceso no autorizado.

Facilitar y agilizar el ejercicio de los derechos de carácter personal, así como adoptar un marco de publicidad necesaria apegado a la normatividad implementada.

Las políticas y procedimientos establecidos anteriormente son ineludibles y su violación implica la aplicación de las sanciones a que haya lugar.

1

Principios Generales

Protección de datos de carácter personal

¿Qué es la protección de datos de carácter personal?

Es un derecho fundamental de las personas físicas, que busca proteger su intimidad y su privacidad frente al riesgo de resultar de algún modo vulnerado en el momento de proceder a recoger y almacenar los Datos Personales en los sistemas desarrollados por los Sujetos Obligados.

Al referirnos al derecho a la protección de datos y del uso de los sistemas en sí, es importante encontrar, un punto de equilibrio, entre la protección y el progreso tecnológico cuya compaginación es indispensable para la protección de la persona.



¿Dónde se regula?



Artículo 16, segundo párrafo de la Constitución Política de los Estados Unidos Mexicanos:

“Toda persona tiene derecho a la protección de sus Datos Personales, al Acceso, Rectificación y Cancelación de los mismos, así como a manifestar su Oposición, en los términos que fije la Ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.



Artículo 6, Fracc.II de la Constitución Política de los Estados Unidos Mexicanos:

“La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes”



Artículo 14 de la Constitución Política del Estado Libre y Soberano de Oaxaca.

“Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente que funde y motive la causa legal del procedimiento...”



Título Segundo de la Ley de Transparencia y Acceso a la información Pública de Oaxaca.



Ley de Protección de Datos Personales del Estado de Oaxaca.



Lineamientos sobre Protección de Datos Personales expedidos por IEAIP.

Los Ordenamientos enumerados contienen los elementos necesarios para establecer una salvaguarda eficaz del derecho a la protección de esos datos. Nos referimos en **primer lugar** a principios cuyo objetivo es proteger al dato en sí, como elemento físico portador de información. En **segundo lugar**, a los derechos que los ya mencionados ordenamientos reconocen a los titulares, con el fin de hacer efectiva la defensa de aquellos mediante el ejercicio de los derechos de Acceso, de Rectificación, de Cancelación y de Oposición.

10

Por último, como Órgano Garante de los derechos de los ciudadanos, el Instituto Estatal de Acceso a la Información Pública de Oaxaca conforme el Registro Estatal de Protección de Datos Personales, el cual controlará la existencia y finalidad de los Sistemas de Datos Personales en poder de los Sujetos Obligados.

El Instituto procura difundir las disposiciones legales de la materia entre la ciudadanía, tomando en cuenta las características regionales para no obstruir el ejercicio del derecho a la Protección de los Datos Personales.

El objetivo perseguido por el Instituto es acercar más estas legislaciones a los ciudadanos y a la sociedad de cada Región, para difundir de manera sencilla su cumplimiento.



Datos de carácter personal

Me llamo Sandra,
vivo en..., 
mi teléfono es... 



¿Qué son los Datos Personales?

El artículo 6, fracc. I de la Ley de Protección de Datos Personales del Estado de Oaxaca expresa: “Toda la información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a una persona física, identificada o identificable, entre otra, la relativa a su origen étnico o racial, o que esté referida a las características físicas, morales o emocionales, a su vida afectiva y familiar, domicilio, número telefónico, patrimonio, ideología y opiniones políticas, creencias o convicciones religiosas o filosóficas, los estados de salud físico o mental y las preferencias sexuales”.

¿Qué son los Datos Públicos?

El artículo 6, fracc. II de la Ley de Protección de Datos del Estado de Oaxaca, expresa: “Se refiere a los datos calificados como tales según los mandatos de la Ley o de la Constitución Política y todos aquellos que no sean sensibles. Son públicos, entre

otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no tengan la clasificación de información reservada y los relativos al estado civil de las personas”.

¿Qué son los Datos Sensibles?

Son aquellos que por su particular sensibilidad y por contener la esfera más delicada de la intimidad de las personas, merece una protección legal más intensa.

Si los Sujetos Obligados tienen este tipo de Datos Personales registrados y almacenados, deben de adoptar especiales medidas para su tratamiento.

Estos datos son los relativos a la ideología, afiliación sindical, convicciones religiosas, filosóficas o morales, origen racial y étnico, estados de salud físico o mental y preferencias sexuales. (Art. 6, Ley de Protección de Datos Personales del Estado de Oaxaca).

¿Qué son los Datos Disociados?

Son aquellos resultantes de un tratamiento de Datos Personales que no deben relacionarse, con una persona identificada o identificable, por ejemplo; los datos estadísticos relativos a grupos de personas sin identificar. Este procedimiento se denomina disociación de los datos. (Art. 6, Ley de Protección de Datos Personales del Estado de Oaxaca).



Categorías de los Datos Personales.

Son los Datos Personales que se clasifican de acuerdo a las medidas de seguridad que deben adoptarse en los siguientes niveles:

12



A. NIVEL BÁSICO.

Las medidas de seguridad marcadas con el nivel básico serán aplicables a todos los Sistemas de Datos Personales.

A los Sistemas de Datos Personales que contienen alguno de los datos que se enlistan en el punto 1 de la Ilustración 1.



B. NIVEL MEDIO.

Son los que contienen alguna de las características que se enlistan en el punto 2 de la Ilustración 1, deberán aplicar las medidas de seguridad del nivel básico y el nivel medio.



C. NIVEL ALTO.

Son los que además de cumplir con las medidas de seguridad de nivel básico y nivel medio, requieren medidas más severas. Se enlistan en el punto 3 de la Ilustración 1.

Ilustración



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

Laborales: Documentos de reclutamiento y selección, documentos de nombramiento, documentos de incidencia, documentos de capacitación, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales, referencias personales (cartas de recomendación, etc.), trabajo actual, trabajos anteriores, otros.



Patrimoniales: Afores, fianzas, servicios contratados, referencias personales crediticias o matrimoniales, bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros.

Jurisdiccionales: Datos sobre procedimientos administrativos seguidos en forma de juicios y/o jurisdiccionales, información derivada de resoluciones judiciales o administrativas que incidan en la esfera jurídica de una persona física.

Académicos: Trayectoria educativa, títulos, cédula profesional, certificados, reconocimientos, otros.

Transitorios y de Movimientos: Información relativa al tránsito de las personas dentro y fuera del país, información migratoria de las personas, otros.



Estado de Salud Físico o Mental: Discapacidades, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos, entre otros (anteojos, aparatos de oído, prótesis, etc.), otros, estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas.

Características Físicas: Color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión.

Datos ideológicos y religiosos: Creencias religiosas, ideologías, afiliación, política, afiliación sindical, pertenencia a organizaciones de la sociedad civil, pertenencia a organizaciones religiosas.

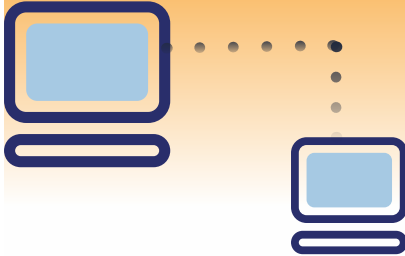
Características Personales: Tipo de sangre, ADN, huella digital, otros

Vida sexual: preferencias sexuales, hábitos sexuales, otros

Origen: Origen étnico, origen racial.

Sistemas de Datos Personales

¿Qué es el Sistema de Datos Personales?



Es el conjunto organizado de Datos Personales que están en posesión de los Sujetos Obligados, contenidos en archivos, registros, ficheros, bases o bancos de datos, cualquiera que fuere la modalidad de su creación, almacenamiento, organización o acceso. (Art. 6, Ley de Protección de Datos Personales del Estado de Oaxaca).

Esto significa que la Ley se aplica tanto a los datos tratados electrónicamente (bases de datos informáticas), como a los almacenados en papel (archivadores con fichas de datos ordenadas). En ambos casos los datos deberán formar un conjunto organizado.

¿Qué tipo de Sistemas pueden tener los Sujetos Obligados?

Por ejemplo los siguientes:



Sistema de Datos Personales de Servidores Públicos de los Sujetos Obligados



Sistema de Datos Personales de Proveedores y Contratistas



Sistema de Datos Personales para Servicios de Educación



Sistema de Datos Personales para Servicios de Salud

¿Puedo como Sujeto Obligado crear y mantener Sistemas de Datos Personales?

Sí. La Ley de Protección de Datos Personales en su artículo 8, contempla como una actividad lícita la creación y conservación de sistemas de titularidad pública de datos personales, siempre que ello resulte necesario para el logro de la actividad y atribuciones del Sujeto Obligado, y este cumpla con las obligaciones que la Ley le impone.

Esto se denomina pertinencia de los sistemas. Cuando la finalidad para la que fueron creados se vea cumplida.

¿Qué obligaciones asume el Sujeto Obligado por crear y mantener sistemas?

-Inscribir los sistemas en el Registro Estatal de Protección de Datos Personales del IEAIP. (Art. 42, Ley de Protección de Datos Personales del Estado de Oaxaca).

-Constar, cuando sea preciso, con el consentimiento de los titulares. (Art. 16, Ley de Protección de Datos Personales del Estado de Oaxaca).

-Informar a los titulares de la creación y finalidad del sistema. (Art. 13, Ley de Protección de Datos Personales del Estado de Oaxaca).

-Guardar secreto y mantener la confidencialidad de los datos recogidos. (Art. 14, Ley de Protección de Datos Personales del Estado de Oaxaca).

-Adoptar las medidas de seguridad exigidas por la Ley.

(Art. 26, Fracc. VIII. Ley de Protección de Datos Personales del Estado de Oaxaca).

-Dar curso al ejercicio de los derechos a los titulares de los datos. (Art.20, Ley de Protección de Datos Personales del Estado de Oaxaca)

Tratamiento de Datos Personales

¿Qué es el Tratamiento de Datos Personales?

La Ley define el tratamiento de datos de carácter personal como cualquier operación y procedimiento sistemáticos, electrónicos o no, que permiten recolectar, conservar, ordenar, almacenar, modificar, evaluar, bloquear, destruir, administrar, así como la cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias. (Art. 6, Ley de Protección de Datos Personales del Estado de Oaxaca).

15

Las operaciones de tratamiento más habituales son:

- El almacenamiento y registro organizado de datos.
- La conservación y mantenimiento actualizado y exacto de los datos.
- La transmisión de los datos a otros Sujetos Obligados.

¿Qué personas intervienen en el tratamiento?



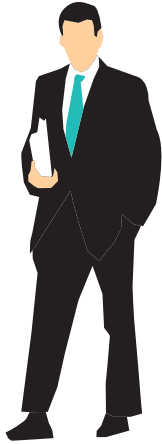
El responsable del sistema o tratamiento.



El interesado o titular de los datos.



El encargado del tratamiento.



¿Quién es el responsable del tratamiento de los Datos Personales?

Es responsable del sistema o tratamiento la persona física o jurídica u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

El responsable del tratamiento será el obligado a cumplir con los deberes de inscripción del sistema, informar a los interesados, recabar el consentimiento, permitir el ejercicio de derechos a los titulares, asegurar el secreto y confidencialidad de los datos, y garantizar su seguridad.

¿Quién es el interesado o titular de los datos?

La Ley considera interesado a la persona física titular de los datos que sean objeto de tratamiento. No pueden serlo personas jurídicas (sociedades, entidades, instituciones, etc...).

La Ley reconoce al interesado los siguientes derechos:

- Consultar los sistemas inscritos en el Registro Estatal de Protección de Datos.
- Tener acceso a sus datos.
- Pedir la rectificación de sus datos erróneos.
- Solicitar la cancelación total o parcial de sus datos.



¿Quién es el encargado del tratamiento de los Datos Personales?

Es la persona física o jurídica, autoridades públicas, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate Datos Personales por cuenta del responsable del tratamiento.

En definitiva, trata los datos, pero no decide cómo ni para qué, sino que lo hace siguiendo las indicaciones e instrucciones del responsable, de quien puede ser un empleado, un subordinado o un proveedor de servicios.

Procedencia de los Datos Personales

¿Qué es la procedencia de datos?



La procedencia es el origen y la manera de recoger u obtener los datos almacenados en los sistemas de los Sujetos Obligados. Básicamente los datos pueden obtenerse:

- Del propio interesado o su representante legal.
- De otros Sujetos Obligados distinto del interesado.
- De fuentes accesibles al público.

¿Cuándo obtengo los datos directamente del interesado?



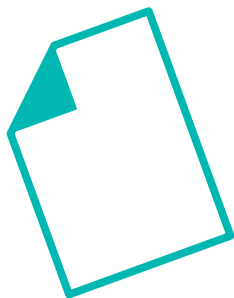
Al pedirlos de forma directa al interesado por cualquier medio o procedimiento y en cuantas ocasiones este los facilite por si mismo al Sujeto Obligado.

¿Por qué procedimientos puedo recabar los datos de los titulares?



A través de los siguientes medios:

- Encuestas o entrevistas.
- Formularios o cupones en soporte papel.
- Transmisión electrónica de datos.
- Formularios telemáticos a través de Internet.
- Por teléfono o por fax.



¿Cuáles son los deberes de los Sujetos Obligados cuando piden los datos al titular o interesado?

1.-Proporcionar la información previa sobre la recopilación y almacenamiento de sus datos.

2.-Facilitar al interesado la información que la Ley establece sobre las excepciones para el tratamiento de los Datos Personales. (Art. 16 Ley de Protección de Datos Personales del Estado de Oaxaca).

¿Qué son las fuentes accesibles al público?

Son las fuentes de información a disposición del público en general, cuya consulta puede ser realizada por cualquier persona, siempre que no lo impida una norma.

Si las fuentes accesibles al público se editan en forma de libro o en otro soporte físico pierden su accesibilidad y se recuperan al producirse una nueva edición.

¿Cuáles son las fuentes accesibles al público?

- El censo promocional.
- Los directorios telefónicos, en los términos previstos por su normativa específica.
- Las listas de personas pertenecientes a grupos profesionales (listado de colegiados).
- Los diarios y boletines oficiales.
- Los medios de comunicación en general.

¿Cómo debe proceder el Sujeto Obligado cuando obtiene datos de fuentes accesibles?

Debe informar al destinatario lo siguiente:

- El origen de los datos.
- La identidad del responsable del tratamiento.
- Los derechos que asisten al titular.

Cesión de los Datos Personales



¿Qué es la cesión de datos?

Es la comunicación o transmisión autorizada de Datos Personales hacia una persona distinta del titular.

(Art. 6, Ley de Protección de Datos Personales del Estado de Oaxaca).

¿Cuáles son los requisitos para poder ceder datos?

Si el Sujeto Obligado quiere ceder a un tercero los Datos Personales almacenados en sus sistemas, debe cumplir dos requisitos como regla general:

1 uno

Informar plenamente al titular de los datos del tipo de actividad a la que se dedica el tercero o la finalidad para que este tercero vaya a tratar sus datos.

2 dos

Obtener el consentimiento previo del interesado.

¿Qué son las cesiones legales?

Son las comunicaciones o transmisiones de los Datos Personales hacia una persona distinta del titular, amparadas por una Ley que autorice la cesión. En este caso el Sujeto Obligado no tiene la obligación de informar ni de obtener el consentimiento previo del titular de los datos.

Son ejemplos de cesiones legales:

- La comunicación o transmisión de los Datos Personales de los trabajadores del Sujeto Obligado a las instituciones de seguridad social,
- Los solicitados oficialmente por las autoridades investigadoras o jurisdiccionales.

Acceso a Datos Personales por cuenta de terceros

Es permitir y facilitar a un tercero, ajeno al Sujeto Obligado, el acceso y el tratamiento de Datos Personales incluidos en sistemas de los que sea responsable, con la finalidad exclusiva de prestar un servicio por este tercero al Sujeto Obligado.

Por ejemplo, cuando se facilitan los Datos Personales de los trabajadores del Sujeto Obligado a una gestoría contratada para prestar el servicio de pago de nóminas.

Los terceros no podrán utilizar los Datos Personales para propósitos distintos a aquellos para los cuales se les hubieren transmitido. (Art. 16, fracc. VII, Ley de Protección de Datos Personales del Estado de Oaxaca).

¿Qué necesita el Sujeto Obligado para permitir el acceso a terceros?

Un contrato debidamente formalizado en el que deberán constar los siguientes puntos:

- El encargado del tratamiento sólo tratará los datos según las instrucciones del responsable.
- No los aplicará con fines distintos, ni los comunicará a terceros.
- Las medidas de seguridad por adoptar.
- Obligaciones del encargado del tratamiento

⇒ (Ver obligaciones contractuales del encargado del tratamiento de Datos Personales).

¿Cuáles son las obligaciones del encargado del tratamiento?

-Tratar los datos conforme a las instrucciones emitidas por el responsable del sistema.

-Aplicarlos solamente a las especificadas finalidades, no comunicarlos a terceros, ni variar el contenido.

-Adoptar las medidas de seguridad necesarias. (Cap. IV, Ley de Protección de Datos Personales del Estado de Oaxaca).

-Devolver al Sujeto Obligado los documentos o soportes en que figuren los datos, y proceder a destruir los mismos finalizada la prestación del servicio.

Obligaciones contractuales del encargado de Tratamiento de Datos Personales

En todo contrato sobre tratamiento de Datos Personales, deben incluirse cláusulas que contengan las siguientes obligaciones del encargado del tratamiento:

1 El encargado del tratamiento se compromete y obliga a que los datos de carácter personal pertenecientes al sistema de datos propiedad del responsable del sistema, a los que pueda acceder en virtud del presente contrato, serán tratados de acuerdo con las disposiciones del artículo 16, fracc.VII y el Capítulo Sexto de la Ley de Protección de Datos Personales del Estado de Oaxaca.

2 El encargado del tratamiento se compromete y obliga también a lo siguiente:

- I.** Los datos de carácter personal se utilizarán exclusivamente para la realización de las actividades objeto del presente contrato conforme a las instrucciones indicadas por el responsable del sistema.
- II.** Sin utilizarlos o aplicarlos a fines distintos de los previstos en el presente contrato. Por lo tanto no podrá comunicarlos, transmitirlos, cederlos, ni siquiera para su conservación, a otras personas, físicas o jurídicas.

3 El encargado del tratamiento de acuerdo con lo dispuesto en el capítulo V de los Lineamientos para la Protección de Datos Personales expedidos por el Consejo General del IEAIP, deberá implementar y adoptar las medidas de seguridad de índole técnica y organizativa adecuadas y necesarias, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural. Dichas medi-

das garantizaran la seguridad de los datos de carácter personal materia del contrato.

4 Una vez cumplido lo estipulado en el presente contrato, el encargado del tratamiento procederá a la destrucción de los datos a los que tuvo acceso según las instrucciones recibidas o en su caso a devolverlos con los soportes o documentos en que consten aquellos provenientes del sistema propiedad del responsable del sistema, sin conservar copia alguna y sin que persona alguna física o jurídica tenga conocimiento de tales datos.

5 En caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado responsable del tratamiento indebido y se hará acreedor a las sanciones correspondientes, eximiendo expresamente al responsable del sistema acerca de cualquier responsabilidad relativa al incumplimiento, en las actividades objeto del presente contrato conforme lo establecido por la Ley de Protección de Datos Personales y sus Lineamientos.

6 De acuerdo con lo dispuesto en el artículo 29 de la Ley de Protección de Datos Personales del Estado de Oaxaca el encargado del tratamiento se compromete y obliga a guardar en secreto todos los datos de carácter personal que conozca y a los que tenga acceso en virtud del presente contrato. Igualmente, deberá custodiar e impedir el acceso a los datos de carácter personal a cualquier persona ajena al encargado del tratamiento.

2

Principios que deben observar los Sujetos Obligados en el tratamiento de los Sistemas de Datos Personales

2 Principios que deben observar los Sujetos Obligados en el tratamiento de los Sistemas de Datos Personales

Licitud de los Datos Personales

¿Qué es la licitud de los datos?



Es la obtención y tratamiento con apego a las diversas disposiciones legales aplicables. El Sujeto Obligado debe ajustarse a la Ley de Protección de Datos Personales del Estado de Oaxaca. (Artículo 8).

Información a los interesados

Es un derecho que tiene el titular de los datos y una obligación correlativa del Sujeto Obligado, como responsable de los sistemas que almacenan información relativa al titular de los datos.

Los Lineamientos sobre la Protección de Datos Personales expedidos por el Consejo del IEAIP, regula y establece el contenido de la información mínima que debe proporcionar el Sujeto Obligado a los titulares que sean objeto de tratamiento por los sistemas. (Art. Decimo Séptimo).

⇒ (Ver requerimientos de la nota informativa relativa al Sistema de Datos Personales).

En el momento que se configura como un deber básico del responsable de los Sistemas de Datos Personales.

-En caso de utilizar un cuestionario impreso o un formulario informático apropiado que incluyan una nota informativa legible.

-Si los datos proceden de fuentes accesibles al público y se utilizan con fines publicitarios, deben incluirse en cada documento publicitario una nota informativa. En este caso el origen de los datos, la identidad del responsable y sus derechos.

¿En qué consiste?

¿Cuándo procede proporcionar la información previa?

¿Qué se debe hacer para proporcionar la información previa?

Requerimientos de la nota informativa relativa al Sistema de Datos Personales

Los Datos Personales recabados serán protegidos, incorporados y tratados en el Sistema de Datos Personales **1**, con fundamento en **2** y cuya finalidad es **3**, el cual fue registrado en el Listado de Sistemas de Datos Personales ante el Instituto Estatal de Acceso a la Información Pública (www.ieaip.org.mx), y podrán ser transmitidos a **4**, con la finalidad de **5**, además de otras transmisiones previstas en la Ley. La Unidad Administrativa responsable del Sistema de Datos Personales es **6**, y la dirección donde el interesado podrá ejercer los derechos de Acceso, Rectificación, Cancelación y Oposición ante la misma es **7**. Lo anterior se informa en cumplimiento del Décimo sexto de los Lineamientos de Protección de Datos Personales, publicados en la página electrónica www.ieaip.org.mx **8**. (Art. Décimo Séptimo, Lineamientos de Protección de Datos Personales)

- 1** Indicar el nombre de Datos Personales.
- 2** Indicar el fundamento legal que faculta a los sujetos obligados para recabar los Datos Personales en el sistema.
- 3** Describir la finalidad del Sistema de Datos Personales.
- 4** Indicar las personas u organismos a las que podrán transmitirse los Datos Personales en el sistema.
- 5** Describir la finalidad de la transmisión.
- 6** Indicar el nombre de la Unidad Administrativa responsable del Sistema de Datos Personales.
- 7** Indicar la dirección de la Unidad de Enlace del Sujeto Obligado que posee el sistema.
- 8** Anotar la fecha de publicación de entrada en vigor.

Consentimiento del Interesado en la Transmisión de Datos Personales



¿Qué es el consentimiento del interesado?

Es la manifestación de voluntad, libre, inequívoca, específica e informada, mediante la cual el interesado permite al Sujeto Obligado el tratamiento de sus Datos Personales.

El consentimiento puede ser, en general, tácito; pero debe ser expreso en los casos del tratamiento de los datos especialmente protegidos como son la ideología, afiliación sindical, religión o creencias, etc.

27

¿Cuándo es necesario el consentimiento?

Siempre que se requiera manifestar la libre voluntad de permitir su tratamiento, salvo las excepciones señaladas en el artículo 16 de la Ley de Protección de Datos Personales del Estado de Oaxaca, que al mismo tiempo obliga al responsable de los sistemas a obtener el consentimiento inequívoco de los titulares de los datos almacenados y tratados por él.

¿Cuándo no es necesario el consentimiento?

En los casos previstos en el artículo 16 de la Ley de Protección de Datos Personales del Estado de Oaxaca, o sea:

I

Cuando se trate de la realización de las funciones propias de la administración pública en su ámbito de competencia.

II

Cuando se transmitan entre Sujetos Obligados, siempre y cuando los Datos Personales se utilicen para el ejercicio de sus facultades.

III

Cuando exista una solicitud u orden de autoridad en materia de procuración o administración de justicia.

IV

Cuando se trate de los Datos Personales de las partes en contratos civiles, laborales, comerciales o administrativos;

V

Cuando sean necesarios para el tratamiento médico del titular;

VI

Cuando se trate de razones estadísticas, científicas o de interés general previstas en la Ley, siempre que no puedan asociarse los Datos Personales con el individuo a quien se refieren;

VII

A terceros, cuando se contrate la prestación de un servicio que requiera el tratamiento de Datos Personales. Dichos terceros no podrán utilizar los Datos Personales para propósitos distintos a aquellos para los cuales se les hubiesen transmitidos; y

VIII

En los demás casos que establezcan las leyes.

Modelo de cláusula de consentimiento expreso

“He sido informado de que los datos que facilitó serán incluidos en el Sistema denominado _____ del Sujeto Obligado(responsable) _____, con la finalidad de _____ y manifiesto mi consentimiento expreso. También se me ha informado de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición, indicándome por escrito la ubicación de la Unidad de Enlace _____ y la posibilidad de transferir mis datos con los siguientes Sujetos Obligados _____”.

Estoy enterado y autorizo a que procedan al tratamiento de mis datos.

firma

firma

*Sujeto Obligado
responsable*

Interesado



Calidad de los Datos Personales

¿Qué es la **calidad** de los datos?

Es el conjunto de obligaciones a cargo del Sujeto Obligado, como responsable de los sistemas, diseñados para el correcto tratamiento de los datos durante su vigencia. Básicamente las principales obligaciones mencionadas son las siguientes:

- Pertinencia de los datos.
- Adecuación del tratamiento.
- Actualización de los datos.

¿Qué es la **adecuación** del tratamiento?

Es la conservación, seguridad y protección de los datos almacenados por los Sujetos Obligados. Que solo pueden ser tratados para las finalidades específicamente establecidas al recabarlos con el conocimiento por el titular de los datos.

¿Qué es la **pertinencia** de los datos?

Es el conjunto de datos adecuados y necesarios al cumplimiento de las finalidades para las que han sido recogidos y que el Sujeto Obligado tiene la obligación de almacenar y cancelar cuando dejen de serlo.

Por ejemplo, en un sistema de Proveedores, el Sujeto Obligado puede tener datos de identificación del proveedor, de los productos o servicios que suministra, pero no serían pertinentes en ese sistema incluir, datos relativos a sus creencias o ideología.

¿Qué es la **actualización** de los datos?

Según la Ley de Protección de Datos Personales del Estado de Oaxaca los datos de carácter personal deben ser exactos, completos, actualizados, comprensibles y adecuados, de tal forma que respondan con veracidad a la situación actual del interesado. (Artículo 9).

En cuanto tenga conocimiento el Sujeto Obligado del cambio de un dato como el apellido de un titular o el cambio de dirección de un proveedor debe rectificar o actualizar ese dato. (Art. 26, fracc.VI, Ley de Protección de Datos Personales del Estado de Oaxaca)



Confidencialidad de los Datos Personales

¿Qué es el deber de secreto y confidencialidad?

Es la responsabilidad de quienes intervienen como responsables, encargados y usuarios en cualquier fase del tratamiento de los Datos Personales de guardar secreto. Dicha responsabilidad subsiste aún después de cancelados o anulados los datos y sistemas utilizados, prolongándose aún después de finalizada la relación entre el titular de los datos y el responsable del sistema.

31

¿Cómo garantizar el cumplimiento de la confidencialidad?

Mediante la adopción por el Sujeto Obligado de una adecuada política de confidencialidad de los Datos Personales, en los contratos de trabajo que celebre el Sujeto Obligado con personal a su servicio deberá incluirse una cláusula obligatoria sobre guarda del secreto profesional. (Ver modelo de cláusula obligatoria sobre confidencialidad en los contratos de trabajo).

Esta política de confidencialidad debe ser conocida por todos los involucrados en el tratamiento y operación de los sistemas relativos. Los Sujetos Obligados, por su parte, deben promover y realizar jornadas de capacitación dirigidas a quienes estén obligados a tratar Sistemas de Datos Personales.

Modelo de cláusula obligatoria sobre confidencialidad en los contratos de trabajo.

“El trabajador tiene y asume la obligación de guardar el secreto y la confidencialidad de toda la información utilizada en el desempeño de sus labores, durante la vigencia del presente contrato, especialmente la relativa a datos de personas físicas o jurídicas contenidos en los Sistemas de Datos Personales. Esta obligación subsistirá aun después de finalizada la relación laboral. (Art. 14, Ley de Protección de Datos Personales del Estado de Oaxaca).

El trabajador será responsable de todos los daños y perjuicios que se causen al empleador como Sujeto Obligado, derivados del incumplimiento doloso o culposo de la mencionada obligación. Lo anterior será causal de terminación de la relación de trabajo, sin responsabilidad para la parte patronal en su calidad de Sujeto Obligado”.



Seguridad de los Datos Personales

¿Qué es la seguridad de los Datos Personales?

Consiste en el deber que tiene el responsable de los sistemas de adoptar las medidas de índole técnica, administrativas y organizativas necesarias para garantizar la seguridad de los Datos Personales y evitar su alteración, pérdida, tratamiento o acceso no autorizado. (Art. 6, Ley de Protección de Datos Personales del Estado de Oaxaca).

Para el Sujeto Obligado el cumplimiento de este deber es en su beneficio, en cuanto la adopción de estas medidas de seguridad evitará perjuicios derivados de una seguridad deficiente.

¿Qué es un documento de seguridad?

Es un protocolo interno que operan los Sujetos Obligados, para mantener siempre actualizadas las medidas de protección, conservación y almacenamiento de los Datos Personales bajo su cuidado, comprendiendo los que intervienen en el tratamiento de los sistemas de datos que utilicen sus dependencias.

33

¿Cuáles son los rubros mínimos que debe incluir el documento de seguridad?

En el ámbito de aplicación:

- Especificación detallada de los recursos protegidos.
- Medidas, normas, procedimientos, reglas y estándares de seguridad.
- Funciones y obligaciones del personal.
- Estructura y descripción de los sistemas y sistemas de información.
- Procedimiento de notificación, gestión y respuesta de incidencias.
- Procedimientos de copias de respaldo y recuperación de datos.
- Medidas adoptadas en el transporte, destrucción y/o reutilización de soportes y documentos.
- Identificación del responsable de seguridad.
- Control periódico del cumplimiento del documento.
- Procedimientos de revisión.
- Consecuencias del incumplimiento del Documento de Seguridad.

3

Recomendaciones sobre medidas de seguridad aplicables a los Sistemas de Datos Personales

3

Recomendaciones sobre medidas de seguridad aplicables a los Sistemas de Datos Personales

Seguridad de los Sistemas de Datos Personales

¿Qué es la obligación de dar seguridad a los sistemas de Datos Personales?

Consiste en aplicar medidas técnicas adecuadas por ejemplo en la:



37

¿Cuántos niveles de seguridad existen?

Los Lineamientos de Políticas Generales emitidos por el IEAIP, sobre la Protección de Datos Personales clasifican las medidas de seguridad que deben adoptarse en tres niveles:

- Nivel básico, aplicable a todos los Sistemas de Datos Personales.
- Nivel medio, aplicable a los Sistemas con datos relativos a la comisión de infracciones administrativas o penales, entre otros.
- Nivel alto, aplicable a los Sistemas que contengan datos especialmente protegidos.

¿Qué medidas de seguridad exigibles debe tener el nivel básico?

Nivel Básico

- Documento de seguridad.
- Funciones y obligaciones del personal con acceso a datos y sistemas de información.
- Adopción de medidas para que el personal conozca la normativa y consecuencias de incumplimiento.
- Procedimiento de notificación y gestión de incidencias.
- Relación de usuarios con acceso y procedimientos de identificación y autenticación.
- Control de acceso.
- Gestión de soportes.
- Copias de respaldo y recuperación.

¿Qué medidas de seguridad exigibles debe tener el nivel medio?

Nivel Medio

- Controles para verificar que se cumple el documento de seguridad.
- Responsable de seguridad.
- Auditoría.
- Identificación y autenticación.
- Control de acceso físico.
- Gestión de soportes (registro de entrada y salida de soportes).
- Registro de incidencias.
- Pruebas con datos reales.

¿Qué medidas de seguridad exigibles debe tener el nivel alto?

Nivel Alto

- ↗ Distribución de soportes.
- ↗ Registro de accesos.
- ↗ Copias de respaldo y recuperación.
- ↗ Telecomunicaciones.



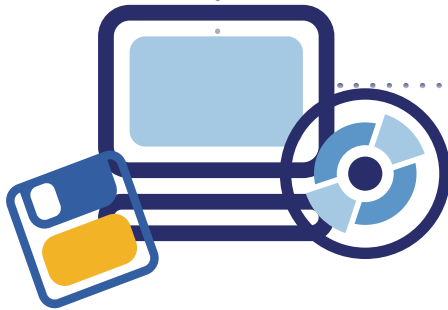
¿Cuáles son los elementos fundamentales a proteger en un sistema automatizado?

El software.
El hardware.
Los datos.



¿Qué es un software?

Es el programa o los programas de computadora en contraste con el equipo físico en que se ejecutan éstos (hardware).



¿Qué es hardware?

Es el conjunto formado por todos los elementos físicos de un sistema informático, como CPUs, terminales, cableado, medios de almacenamiento secundario (cintas, CD – ROMs, diskettes, etc.).

¿Qué son los Datos?

Son el conjunto de información lógica que maneja el software y el hardware, como ejemplo paquetes que circulan por un cable de red o entradas de una base de datos.

Visión global de la seguridad informática

Seguridad



Fiabilidad



Aspectos

Elementos

Amenazas

Mecanismos

Confidencialidad

Integridad

Disponibilidad

Tipos

Interrupción

Intercepción

Modificación

Fabricación

Origen

Personas

Amenazas Lógicas

Catástrofes

Prevención

Detección

Recuperación

Hardware

Software

Datos

Recomendaciones a los Sistemas de Datos Personales en soportes físicos y automatizados

SISTEMA DE DATOS PERSONALES EN SOPORTES FÍSICOS Y AUTOMATIZADOS			
Recepción de Datos Personales	Nivel Básico	Nivel Medio*	Nivel Alto**
		<p>1. Existe señalización visible sobre las restricciones de acceso, y las prohibiciones que se apliquen.</p> <p>2. El personal autorizado que labora en el área ostenta una identificación con fotografía (credencial o gafete) emitida por el Sujeto Obligado.</p> <p>3. Existe la infraestructura apropiada para mantener en forma organizada y segura los Datos Personales.</p> <p>4. El responsable deberá supervisar que el directorio de la entrada de los edificios del Sujeto Obligado cuente con su nombre como responsable del sistema, del encargado y del usuario, así como la ubicación de cada uno de ellos.</p> <p>5. El encargado de los sistemas de Datos Personales supervisa y verifica que la computadora de escritorio cumpla con los requerimientos y configuraciones de seguridad definidas. [Sistema en soporte electrónico]</p> <p>6. El equipo de cómputo instalado debe pasar por un proceso de preparación inicial a fin de instalarse solamente el software autorizado, que deberá registrarse en un formulario el cual será archivado por el área de sistemas o el personal de vigilancia. [Sistema en soporte electrónico]</p>	<p>Además de aplicar las medidas de seguridad del nivel básico, se aplican las siguientes:</p> <p>1. Se exhibirán en un lugar visible dentro y fuera del área el personal autorizado que labora en el área de recepción, donde el encargado de los sistemas actualiza los nombres completos y fotografías que se exhiben.</p> <p>2. No está permitido el libre acceso y el uso de aquellos dispositivos de almacenamiento externo excepto si se logra contar con la autorización correspondiente.</p> <p>3. El equipo de cómputo está provisto de la tecnología necesaria y suficiente para verificar la identidad del personal autorizado que labora en el área. [Sistema en soporte electrónico]</p>

SISTEMA DE DATOS PERSONALES EN SOPORTES FÍSICOS Y AUTOMATIZADOS

Resguardo de Datos Personales

Nivel Básico

1. Existe la infraestructura apropiada en donde al interior del área, existen las condiciones ambientales idóneas para preservar en buen estado los Datos Personales durante el tiempo de conservación.
2. La puerta de acceso del área de resguardo cuenta con cerradura, dispositivo electrónico o cualquier otra tecnología que impida su libre apertura. Este mecanismo queda cerrado en horas no hábiles.
3. El mobiliario utilizado protege los Datos Personales de la humedad, temperatura, iluminación solar, consumo de alimentos y presencia de plagas.
4. El personal autorizado que labora en el área ostenta una identificación con fotografía (credencial o gafete) emitida por el Sujeto Obligado.
5. Existe señalización visible sobre las restricciones de acceso, y las prohibiciones que se apliquen.
6. El equipó de computo instalado debe pasar por un proceso de preparación inicial a fin de instalarse solamente el software autorizado, que deberá registrarse en un formulario el cual será archivado por el área de sistemas o el personal de vigilancia. **[Sistema en soporte electrónico]**
7. La creación y asignación de claves de acceso deberá otorgarlo el responsable del Sistema de Datos Personales, para que el personal autorizado acceda al equipo a fin de realizar el tratamiento que corresponda al Sistema, estas contraseñas deberán de estarse actualizando mínimo cada año. **[Sistema en soporte electrónico]**

Nivel Medio*

Además de aplicar las medidas de seguridad del nivel básico, se aplican las siguientes:

1. De existir ventanas o muros divisorios transparentes en el área la visión esta obstruida mediante una película traslucida (papel albanene), por ejemplo.
2. Se exhibirán en un lugar visible dentro y fuera del área el personal autorizado que labora en el área de recepción, donde el encargado de los sistemas actualiza los nombres completos y fotografías que se exhiben.
3. No esta permitido el libre acceso y el uso de aquellos dispositivos de almacenamiento externo excepto si se logra contar con la autorización correspondiente.
4. El mobiliario utilizado para almacenar los Datos Personales cuenta con cerraduras, dispositivos electrónicos o cualquier otra tecnología que impida la libre apertura de sus puertas, cajones o compartimientos. Tales mecanismos quedan cerrados en horas no hábiles. **[Sistema en soporte físico]**
5. El equipo de cómputo esta provisto de la tecnología necesaria y suficiente para verificar la identidad del personal autorizado que labora en el área. **[Sistema en soporte electrónico]**

Nivel Alto**

Se aplican las medidas de seguridad del nivel básico y medio.

SISTEMA DE DATOS PERSONALES EN SOPORTES FÍSICOS Y AUTOMATIZADOS

Acceso y Consulta de Datos Personales

Nivel Básico

Además de las características mencionadas en la recepción y en el reguardo se observaran las siguientes:

1. Deberán de existir puntos de revisión al interior de las instalaciones del Sujeto Obligado, donde el personal de vigilancia controla el acceso y verifican la seguridad de una zona de acceso restringido ya que en dicha área se requiere invariablemente la autorización del responsable de los sistemas.

2. Existe la infraestructura apropiada de tal manera que es posible vigilar y supervisar los Datos Personales en soportes físicos o electrónicos que consultan los usuarios de los Datos dentro del área.

3. Existe señalización visible sobre: horarios de atención, restricciones de acceso, prohibiciones que apliquen y procedimiento para dar aviso al personal de vigilancia en caso de sospecha de presencia de personas no autorizadas.

4. El encargado de los Sistemas de Datos Personales al autorizar la salida de estos en soportes físicos o electrónicos hace el registro de actividades correspondientes.

5. Cada acceso y consulta realizada por personas NO autorizadas se considera como un incidente de intrusión que se denuncia a las autoridades competentes para su investigación.

6. El personal autorizado que labora en la zona de acceso restringido de los sistemas de Datos Personales verifica durante el desempeño de sus funciones que en dichas áreas no haya personas no autorizadas.

Nivel Medio*

Además de aplicar las medidas de seguridad del nivel básico, se aplican las siguientes:

Además de las características mencionadas en la recepción y en el reguardo se observaran las siguientes:

1. El personal que tiene la intención de ingresar a una zona de acceso restringido deberá entregar una identificación oficial con fotografía (credencial de elector, pasaporte, etc.), al personal que atiende dicha área.

2. El usuario consulta los Datos Personales exclusivamente en el área de consulta.

Nivel Alto**

Además de aplicar las medidas de seguridad del nivel básico y medio, se aplican las siguientes:

1. Las zonas de acceso restringido cuentan con un sistema de video-vigilancia remota que permite vigilar la puerta de acceso y al interior de dichas áreas. Dicho sistema cuenta con cámaras para visión nocturna, un sistema de grabación que opera la 24 hrs., en los 365 días del año y un archivo que acumula grabaciones de los dos meses anteriores, en caso de ocurrir un incidente de intrusión, la grabación realizada por este sistema de video-vigilancia remota se transmite a un soporte electrónico, para que pueda ser utilizado por la autoridad competente como prueba.

SISTEMA DE DATOS PERSONALES EN SOPORTES FÍSICOS Y AUTOMATIZADOS

Registro de Actividades

Nivel Básico	Nivel Medio*	Nivel Alto**
<p>El encargado de los sistemas de Datos Personales mantiene estricto control y registro de:</p> <ol style="list-style-type: none"> 1. Las autorizaciones dirigidas a destinatarios que han solicitado que los Datos Personales en soportes físicos o electrónicos en un formato que permita manipularlos o procesarlos 2. Todas las transmisiones efectuadas, para ello, anota todos los datos necesarios para emitir informes sobre la transmisión observando las disposiciones que marca el Capítulo IV de los Lineamientos sobre Políticas Generales de Protección de Datos Personales, emitidos el 14 de Enero de 2009 por el IEAIP. 3. De la asignación, actualización y reemplazo de llaves, tarjetas, contraseñas de acceso y demás elementos que entrega a los usuarios para que estos puedan abrir los mecanismos de apertura de puertas y mobiliario en las zonas de acceso restringido. 4. Las autorizaciones emitidas a los usuarios que solicitan acceso a las áreas de recepción o resguardo. 5. Las autorizaciones emitidas a los usuarios que solicitan permisos para extraer Datos Personales en soportes físicos o electrónicos del área de consulta. 6. Las autorizaciones emitidas a los usuarios que solicitan permiso para introducir a las zonas de acceso restringido aparatos no autorizados. 	<p>Además de aplicar las medidas de seguridad del nivel básico, se aplican las siguientes:</p> <p>El encargado de los sistemas de Datos Personales mantiene estricto control y registro de:</p> <ol style="list-style-type: none"> 1. Los que solicitan permiso para extraer Datos Personales en soportes físicos o electrónicos del área de consulta, deberán especificar por que necesita llevarse. 2. Los que solicitan permiso para introducir a las zonas de acceso restringido aparatos no autorizados, deberán indicar las razones por las que necesita introducirlo. 	<p>Además de aplicar las medidas de seguridad del nivel básico y medio, se aplican las siguientes:</p> <ol style="list-style-type: none"> 1. El sistema de videovigilancia remota registra las actividades diarias así como los incidentes en la zona de acceso restringido.

SISTEMA DE DATOS PERSONALES EN SOPORTES FÍSICOS Y AUTOMATIZADOS

Incidentes

Nivel Básico	Nivel Medio*	Nivel Alto**
<p>1.En caso de presentarse un incidente, se sigue el procedimiento que el Sujeto Obligado tenga definido en el cual le hará de conocimiento del incidente al órgano interno de control, al área jurídica y/o al servidor público que tenga facultades de presentar denuncia o querellas de cada Sujeto Obligado.</p> <p>2.El responsable del personal de vigilancia emite un informe al Responsable del los Sistemas de Datos Personales a no mas de tres días naturales de haber ocurrido el incidente.</p> <p>3.En caso de robo o extravío de Datos Personales, se alerta a los titulares de los Datos afectados para que tomen precauciones ante el posible uso ilegal de su identidad. Para tal efecto, el responsable de los Sistemas de Datos Personales da aviso por escrito a dichos titulares, a más tardar 5 días naturales de haber ocurrido el incidente, recabando el acuse de recibo de esta notificación.</p>	<p>Además de aplicar las medidas de seguridad del nivel básico, se aplican las siguientes:</p> <p>1. A no más de tres días de haber ocurrido el incidente, el responsable de los Sistemas de los Datos Personales da aviso al público mediante un desplegado de prensa que difunde el hecho por diversos medios según la gravedad del caso, a escala local, regional o nacional.</p> <p>2. Se deberán de aplicar los procedimientos de recuperación, personal que lo ejecuta, datos restaurados, y en su caso datos grabados manualmente.</p> <p>3. Deberá contar con la autorización del responsable del sistema para la recuperación de los datos.</p>	<p>Se aplican las medidas de seguridad del nivel básico y medio.</p>

SISTEMA DE DATOS PERSONALES EN SOPORTES FÍSICOS Y AUTOMATIZADOS

Baja

Nivel Básico

Para proceder a la baja documental de soportes físicos o electrónicos que contienen Datos Personales, deberán observarse las disposiciones establecidas por el Capítulo III de la Ley de Archivos del Estado de Oaxaca y además:

1. Todo soporte físico o electrónico que será dado de baja (ya sea por obsolescencia, sustitución o cualquier otra causa) deberá pasar por un proceso de preparación final antes de ser desechado. Dicho proceso incluye la transferencia del contenido que sea preciso conservar hacia otro soporte físico o electrónico y la destrucción, inhabilitación o daño que deje inservible dicho soporte.

2. Las únicas personas para realizar dicho proceso son los Responsables y Encargados de los sistemas los cuales vigilarán que se sigan los procedimientos y se sigan los mecanismos para realizar la destrucción de éstos. Estos llevarán una bitácora donde registran la baja de dichos soportes anotando:

- Nombre y firma de la persona que realiza esta acción.
- Fecha y hora en la que se realiza.
- El destino que se le dará al soporte electrónico desechado.
- Nombre y firma (Vo. Bo.) del Responsable de los Sistemas de Datos Personales.

Nivel Medio*

Además de aplicar las medidas de seguridad del nivel básico, se aplican las siguientes:

1. Si el Sujeto Obligado realiza la separación de materiales para su reciclaje (como podría suceder, con el papel, el cartón, el metal y el plástico), los Datos Personales contenidos en materiales reciclables son triturados y la viruta resultante se entrega directamente a una empresa que los recibe para procesarlos de inmediato garantizando por escrito que no serán examinados para su eventual reconstrucción. **[Sistema en soporte físico]**

Nivel Alto**

Se aplican las medidas de seguridad del nivel básico y medio.

SISTEMA DE DATOS PERSONALES EN SOPORTES FÍSICOS Y AUTOMATIZADOS

Transmisión de Datos Personales	Nivel Básico	Nivel Medio*	Nivel Alto**
	<p>Los Datos Personales que son enviados a un destinatario autorizado para manipularlos o procesarlos son sometidos a un proceso de preparación previa en la transmisión y:</p> <ol style="list-style-type: none"> 1. Los Datos Personales que son enviados a un destinatario autorizado para manipularlos o procesarlos no son reintegrados a los sistemas de Datos Personales de donde fueron extraídos, a menos que el destinatario haya efectuado una corrección solicitada por el titular de los datos. 2. La transmisión de Datos Personales al interior del Sujeto Obligado se realiza mediante la vía elegida, de común acuerdo, entre las partes: mensajero interno, asistente secretaria, visita personal, etc. 3. El paquete con Datos Personales viaja perfectamente sellado de forma tal que sea perceptible cualquier violación o apertura no autorizada del mismo. 4. Genera archivos electrónicos que contenga los Datos Personales solicitados en un formato que permita al destinatario efectuar las operaciones que requiera. [Sistema en soporte electrónico] 	<p>Los Datos Personales que son enviados a un destinatario autorizado para manipularlos o procesarlos son sometidos a un proceso de preparación previa en la transmisión y:</p> <ol style="list-style-type: none"> 1. La transmisión al exterior se realiza mediante un servicio de mensajería externo. Se define un destinatario primario y otro secundario por si el mensajero no encuentra al primero. 2. La entrega del paquete se realiza solo si el destinatario acredita su identidad. El cual deberá presentar una identificación oficial con fotografía (Credencial de elector, pasaporte, etc.) y el mensajero recaba el nombre, firma y un número de referencia que aparezca en tal identificación además de la fecha de entrega. 3. El mensajero no entrega el paquete si el destinatario no puede acreditar su identidad. El mensajero tiene la obligación de regresar el paquete al transmisor. 4. El responsable de los Sistemas de Datos Personales verifica que el mensajero entregue 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. 5. Somete Dichos archivos a un proceso de encriptación ALTO, no menor a 1024 bits. [Sistema en soporte electrónico] 6. Los Datos Personales que son enviados a un destinatario NO autorizado para manipularlos o procesarlos son sometidos a un proceso distinto de transmisión. En este caso, es el encargado que realiza dicho proceso el que debe de : Generar archivos electrónicos que contengan los Datos Personales en un formato protegido, de manera que el destinatario pueda examinar su contenido pero no pueda editarlo, copiarlo ni imprimirlo. [Sistema en soporte electrónico] 7. Somete los archivos resultantes a un proceso de encriptación que proteja los archivos durante su trayecto aplicando un nivel de encriptación MEDIO, no menor a 512 bits. [Sistema en soporte electrónico] 	<p>Se aplican las medidas de seguridad del nivel básico y medio.</p>

SISTEMA DE DATOS PERSONALES EN SOPORTES FÍSICOS Y AUTOMATIZADOS

Transmisión mediante redes de comunicación electrónica

Nivel Básico	Nivel Medio*	Nivel Alto**
<p>1.La transmisión de Datos Personales en archivos electrónicos, previamente preparados para su transmisión se realiza mediante redes de comunicación electrónica. [Sistema en soporte electrónico]</p>	<p>Además de aplicar las medidas de seguridad del nivel básico, se aplican las siguientes:</p> <p>1.El Transmisor recaba por escrito acuse de recibo del destinatario ya sea por correo electrónico o por oficio enviado por fax. [Sistema en soporte electrónico]</p> <p>2.Se aplican las medidas necesarias y suficientes para que los puntos de acceso inalámbrico a la red de comunicación electrónica del Sujeto Obligado, sean seguros y no existan huecos que puedan ser aprovechados por intrusos. [Sistema en soporte electrónico]</p> <p>3.El personal de sistemas mantiene actualizada la memoria técnica de la red de comunicación electrónica con el fin de identificar los equipos inicialmente configurados y puestos a disposición del personal autorizados para interactuar los Sistemas de Datos Personales. [Sistema en soporte electrónico]</p> <p>4.El responsable o encargado de los Sistemas de Datos Personales, en coordinación con el área de sistemas, realiza de manera periódica y en forma programada análisis de vulnerabilidades y pruebas de intrusión controladas en la infraestructura de cómputo, almacenamiento y comunicaciones. [Sistema en soporte electrónico]</p>	<p>Además de aplicar las medidas de seguridad del nivel básico y medio, se aplican las siguientes:</p> <p>1.La transmisión de datos se hace a través de redes de transmisión cifradas. [Sistema en soporte electrónico]</p> <p>2.Existen dispositivos de alta seguridad instalados en caso de que la red de comunicación electrónica (que conecta a los servidores que contengan los Datos Personales con las computadoras que se utilizan para acceder a ellos) este conectada a internet. [Sistema en soporte electrónico]</p> <p>3.Los dispositivos instalados incluyen sistemas de protección perimetral (cortafuegos) de detección de intrusos, filtros de contenido, de prevención de intrusiones y de análisis de protocolos. [Sistema en soporte electrónico]</p>

SISTEMA DE DATOS PERSONALES EN SOPORTES FÍSICOS Y AUTOMATIZADOS

	Nivel Básico	Nivel Medio*	Nivel Alto**
Gestión de Soportes	<p>1. Deberá llevar a cabo el inventario de soportes deberá ser independiente del que lleva en el área administrativa correspondiente, el cual deberá incluir todos los activos de computo, separados por tipo: es decir computadoras personales, servidores, impresoras, y equipos periféricos autorizados.</p> <p>2. Se dará un acceso restringido al lugar de almacenamiento.</p> <p>3. El responsable de los sistemas deberá dar la autorización de la salida de los Datos Personales en soportes físicos o electrónicos (incluidos a través de e-mail), y adoptará las medidas para el seguro transporte y desecho de los mismos.</p>	<p>Además de aplicar las medidas de seguridad del nivel básico, se aplican las siguientes:</p> <p>1. Se llevará a cabo el registro de entradas y salidas de soportes: documento o soporte, fecha, emisor/destinatario, número, tipo de información, forma de envío, responsable autorizado para la recepción/entrega.</p>	<p>Además de aplicar las medidas de seguridad del nivel básico y medio, se aplican las siguientes:</p> <p>Se contará con lo siguiente:</p> <p>1. Un sistema de etiquetado confidencial.</p> <p>2. Cifrado de datos en la distribución de soportes. [Sistema en soporte electrónico]</p> <p>3. Cifrado de información en dispositivos portátiles fuera de las instalaciones (evitar el uso de dispositivos que no permitan cifrado o adoptar medidas alternativas). [Sistema en soporte electrónico]</p>
Copias de respaldo	<p>Deberá ejecutar lo siguiente:</p> <p>1. Copia de respaldo semanal. [Sistema en soporte electrónico]</p> <p>2. Procedimientos de generación de copias de respaldo y recuperación de Datos. [Sistema en soporte electrónico]</p> <p>3. Verificación semestral de los procedimientos. [Sistema en soporte electrónico]</p> <p>4. Reconstrucción de los Datos a partir de la última copia, grabación manual en su caso, si existe documentación que lo permita. [Sistema en soporte electrónico]</p> <p>5. Pruebas con datos reales. [Sistema en soporte electrónico]</p> <p>6. Copias de seguridad y aplicación del nivel de seguridad correspondiente. [Sistema en soporte electrónico]</p>	<p>Se aplican las medidas de seguridad del nivel básico.</p>	<p>Además de aplicar las medidas de seguridad del nivel básico y medio, se aplican las siguientes:</p> <p>1. Se deberá ejecutar copia de respaldo y procedimientos de recuperación en lugar diferente del que se encuentren los equipos, las cuales serán depositadas en la bóveda de seguridad del Sujeto Obligado para su debida protección. [Sistema en soporte electrónico]</p>

SISTEMA DE DATOS PERSONALES EN SOPORTES FÍSICOS Y AUTOMATIZADOS

	Nivel Básico	Nivel Medio*	Nivel Alto**
Auditoría		<p>Deberá realizarse al menos cada dos años, ya sea de manera interna o externa.</p> <ol style="list-style-type: none"> 1. Debe realizarse ante modificaciones sustanciales en los Sistemas de información con repercusiones en seguridad. 2. Se verificará y controlará de la adecuación de las medidas. 3. Se realizará un informe de detección de deficiencias y propuestas correctoras. 4. Se hará un análisis del responsable de seguridad y conclusiones elevadas al responsable del fichero. 	Se aplican las medidas de seguridad del nivel medio.
Supervisión	<p>1. El comité de información del Sujeto Obligado propone la realización de una supervisión a las unidades administrativas que mantienen y operan sistemas de Datos Personales así como a los terceros contratados.</p>	Se aplican las medidas de seguridad del nivel básico.	Se aplican las medidas de seguridad del nivel básico.

SISTEMA DE DATOS PERSONALES EN SOPORTES FÍSICOS Y AUTOMATIZADOS

Documentación en medidas de seguridad en procesos y políticas de los Sistemas de Datos Personales	Nivel Básico	Nivel Medio*	Nivel Alto**
	<p>1. Existe un manual de operaciones donde están documentados los procesos y procedimientos que los servidores públicos llevan dentro de cada Sujeto Obligado.</p> <p>2. Deberán tomar un curso de sensibilización sobre Protección de Datos Personales los Responsables, los Encargados y los Usuarios que interactúan con los sistemas de Datos Personales, el cual se deberá impartir al menos una vez al año al personal.</p> <p>3. Deberá otorgarse un curso de sensibilización similar al curso anterior, que persigue el mismo fin pero que esta orientado a proveedores externos que interactúan con uno o mas sistemas de Datos Personales y a quienes también se exige se asegure la protección de Datos Personales.</p> <p>4. Los Sujetos Obligados deberán contar con un contrato de confidencialidad que ha firmado con cada proveedor o prestador de servicios que llama para la realización de servicios que impliquen interactuar con los sistemas de Datos Personales.</p>	<p>Además de aplicar las medidas de seguridad del nivel básico, se aplican las siguientes: 1. Al menos cada dos años el responsable de los Sistemas de Datos Personales (y archiva) una carta compromiso de parte de cada uno de los miembros del personal autorizado que interactúa con uno o mas Sistemas de Datos Personales.</p> <p>2. En dicha carta el servidor público manifiesta con su firma autógrafa, su compromiso para realizar su trabajo al mismo tiempo manifiesta conocer los Lineamientos y la Ley de la materia sobre la seguridad y protección que deben observar los Sistemas de Datos Personales a fin de garantizar al ciudadano la custodia de sus Datos Personales.</p>	<p>Se aplican las medidas de seguridad del nivel básico y medio.</p>

Algunas de las recomendaciones sugeridas en el cuadro anterior, se tomarón del: IFAI, "Recomendaciones sobre Medidas de Seguridad Aplicables a los Sistemas de Datos Personales", Ed. IFAI, México, D.F.

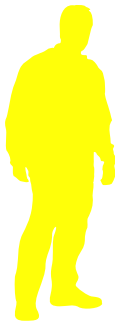
nota: De acuerdo con su disponibilidad presupuestal deberá contar con espacios seguros y adecuados para la operación de los Sistemas de Datos Personales Automatizados como expresa el Artículo Trigésimo de los Lineamientos de Políticas Generales de Protección de Datos Personales.

4 cuatro

Derechos en materia de Datos Personales.

4 Derechos en materia de Datos Personales

Los Derechos de los Interesados ¿Cuáles son los derechos de los interesados?



- 1 Consultar al Registro Estatal de Protección de Datos Personales.
- 2 Acceder a sus datos.
- 3 Rectificar sus datos.
- 4 Cancelar sus datos.
- 5 Oponerse al tratamiento de sus datos.

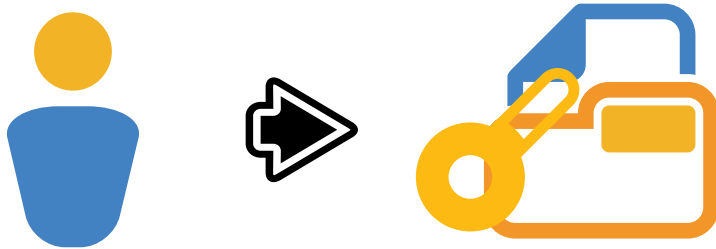
57

¿En qué consiste el derecho a consultar al Registro Estatal de Protección de Datos Personales?

En inquirir la facultad de cualquier persona a consultar al Registro Estatal de Protección de Datos Personales información sobre la existencia y finalidad de los sistemas de datos que manejan los Sujetos Obligados. El Registro Estatal de Protección de Datos Personales es de consulta pública y gratuita.

¿Qué es el derecho de Acceso?

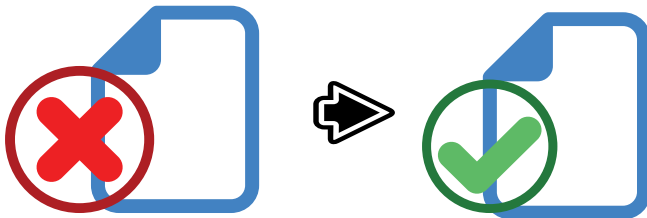
Es la facultad del titular de los datos a solicitar al Sujeto Obligado, como responsable del sistema a informarle como se encuentran almacenados, tratados y si han sido cedidos a terceras personas.



58

¿Qué es el derecho de Rectificación?

Es la facultad del interesado a solicitar al Sujeto Obligado, la corrección, complementación de uno o varios de sus datos. Por ejemplo: Cambio de nombre, de domicilio, etc.



¿Qué es el derecho de Cancelación?

Es la facultad del interesado para solicitar la cancelación de sus datos por causa justificada en el sistema correspondiente al Sujeto Obligado.

¿Qué es el derecho de Oposición?

Es el derecho que tienen los titulares a oponerse al tratamiento de sus datos, cuando éstos se hayan registrado sin su consentimiento. La oposición deberá fundarse y motivarse, ésta puede ser total o parcial.

La Tutela de los Derechos

¿Qué es la Tutela de los Derechos?

Es la guarda y custodia a cargo de los Sujetos Obligados de los sistemas de Datos Personales existentes en sus registros.

¿Qué puede hacer el interesado cuando se le niegue el Derecho de Acceso, Rectificación, Cancelación y Oposición a sus Datos Personales?

Promover ante el IEAIP el Recurso de Revisión.

¿Qué es el Recurso de Revisión?

Es un medio de defensa jurídica que tiene por objeto garantizar que en los actos y resoluciones de los Sujetos Obligados se respeten las garantías de legalidad y seguridad jurídica.

Del procedimiento de acceso a la información personal

¿Cuál es la denominación técnica de los Derechos de Acceso, Rectificación, Cancelación y Oposición?

Es la denominación que se conoce técnicamente como Derecho ARCO y comprende los mencionados derechos:

¿Quién puede interponer una solicitud del Derecho ARCO de los Datos Personales?

Solo los titulares de la información personal o sus representantes legales podrán solicitar y obtener, previa acreditación ante la Unidad de Enlace correspondiente del Sujeto Obligado el Acceso, Rectificación, Cancelación y Oposición de la información personal, registrada en los Sistemas de Datos Personales de los Sujetos Obligados. Esta solicitud generalmente gratuita puede requerir el pago de derechos según las leyes correspondientes.

60

¿Cómo puede ejercerse el Derecho ARCO por el titular de los Datos Personales?

- 1 Acreditando su identidad.
- 2 Cuando el titular se encuentre en situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal de estos derechos, podrán ejercitarse por su representante legal en cuyo caso será necesario que acredite tal condición.
- 3 Estos derechos también podrán ejercitarse a través de representante autorizado expresamente designado para el ejercicio del derecho. En ese caso, deberá constar claramente acreditada la identidad del representado, mediante la presentación de copia de CURP, credencial para votar, pasaporte, etc., y la representación conferida por aquel, por carta poder o poder notarial, según el caso, dejando constancia fidedigna del mismo o mediante declaración en comparecencia personal del titular.
- 4 Para el caso de personas fallecidas el ejercicio de estos derechos corresponderá a la sucesión, cuyo albacea podrá dirigirse a los Sujetos Obligados con la finalidad de notificar el fallecimiento aportando acreditación suficiente del mismo y ejercer en su caso el procedimiento correspondiente.

¿En dónde puede presentarse la solicitud del Derecho ARCO?

- a) En la Unidad de Enlace del Sujeto Obligado correspondiente, o bien
- b) Ante el Instituto Estatal de Acceso a la Información Pública de Oaxaca, directamente o por medio de la siguiente dirección electrónica:

http://www.ieaip.org.mx/datos_personales/formato.pdf



¿Cómo puede presentarse la solicitud del Derecho ARCO?



¿En qué tiempo deberá ser resuelta una solicitud del Derecho ARCO?

En un plazo no mayor a **15 días** hábiles contados desde la presentación de la solicitud.

Este plazo podrá ser ampliado una sola vez por un periodo igual, siempre que exista causa justificada. (Art. 31, Ley de Protección de Datos Personales del Estado de Oaxaca).

¿A quién corresponde atender las solicitudes que se reciben?

Corresponde a la Unidad de Enlace y personal habilitado de cada Sujeto Obligado atender las solicitudes del Derecho ARCO de Datos Personales.

62

¿Qué hacer una vez que se ha recibido una solicitud del Derecho ARCO?

Al recibir una solicitud de Acceso, Rectificación, Cancelación y Oposición de Datos Personales, la Unidad de Enlace deberá verificar que cumpla con los requisitos de procedibilidad, registrar la recepción, procesar y dar trámite a todas las solicitudes del Derecho ARCO de los Datos Personales.

Requisitos de Procedibilidad de la Solicitud

Para que una solicitud del Derecho ARCO de Datos Personales pueda ser atendida debidamente por la Unidad de Enlace, ésta debe verificar que cumpla con los siguientes requisitos de Procedibilidad:

- ① *El nombre y nacionalidad del solicitante, domicilio u otro medio para recibir notificaciones, correo electrónico; así como los datos generales de su representante legal, en su caso;*
- ② *La descripción clara y precisa de lo solicitado;*
- ③ *Cualquier otro dato que propicie su localización con objeto de facilitar su búsqueda;*
- ④ *Forma en que desea le sea entregada la notificación de procedencia o improcedencia y constancia de rectificación o cancelación de Datos Personales, ya sea personalmente en el domicilio de la Unidad de Enlace o por correo certificado con notificación, y*
- ⑤ *La modalidad en que desea le sea entregada la información. La información no se entregará por el medio electrónico y para recogerla deberá acudir a la Unidad de Enlace o al lugar que la misma designe.*
- ⑥ *Documentación que motive su solicitud.*

Si los detalles proporcionados por el solicitante no bastan para localizar los documentos o son erróneos, la Unidad de Enlace lo requerirá, por una sola vez para que dentro de los cinco días hábiles siguientes a la presentación de la solicitud, indique otros elementos o corrija los datos para que en un termino igual la complementé o la aclare. Este requerimiento interrumpirá el plazo establecido para la entrega de la información al interesado (15 días hábiles). (Art. 34 , Ley de Protección de Datos Personales del Estado de Oaxaca).

¿Qué tipo de documentación está obligada a entregar la Unidad de Enlace, al recibir una solicitud del Derecho ARCO?

1

Acuse de recibo de la solicitud.

2

La Notificación de procedencia o improcedencia resuelta por el Comité de Información a propuesta de la Unidad Administrativa, que consiste en informar al particular si la solicitud del Derecho ARCO de sus Datos Personales procede o bien, en caso contrario se informa de manera fundada y motivada las razones de su improcedencia.

3

Constancia de rectificación o cancelación parcial o total, que consiste en elaborar un documento a cargo de la Unidad Administrativa mediante el cual se hace constar que se realizó la rectificación o cancelación total o parcial de los Datos Personales en caso de que proceda.

4

Corresponderá al Comité de Información, analizar la solicitud del Derecho ARCO de los Datos Personales a propuesta de la Unidad Administrativa, la procedencia o improcedencia correspondiente y permitirle al solicitante ejercer los derechos. Dicha notificación la remitirá a la Unidad de Enlace correspondiente para que sea entregada al Solicitante.

1

Acuse de recibo
de la Solicitud

2

Notificación
de procedencia
o improcedencia

3

Constancia de
rectificación o
cancelación par-
cial o total

¿Qué hacer una vez que se recibe y que sí procede?

1

Recibida la solicitud del Derecho ARCO de Datos Personales, la Unidad de Enlace deberá turnarla a la (s) Unidad (es) Administrativa (s) que tengan la información correspondiente;



2

Cuando se trate de una Solicitud de Acceso a Datos Personales, y la Unidad Administrativa cuente con dicha información, lo hará del conocimiento para su visto bueno al Comité de Información, el cual remitirá la respuesta en un formato comprensible a la Unidad de Enlace para que ésta le sea entregada al solicitante en un lapso no mayor a 15 días, verificando su identidad.



3



De tratarse de una Solicitud de Rectificación o Cancelación la Unidad Administrativa correspondiente remitirá la notificación de procedencia o improcedencia al Comité de Información para su validación, la cual se enviará a la Unidad de Enlace correspondiente para que sea entregada al solicitante. De ser procedente la Rectificación o Cancelación, la Unidad Administrativa correspondiente realizará las modificaciones o cancelaciones pertinentes y elaborará una constancia donde se acrediten los cambios, la cual remitirá a la Unidad de Enlace del Sujeto Obligado correspondiente, para que le sea entregada al solicitante.





4

Si se tratase de una solicitud de Oposición, el Comité de Información del Sujeto Obligado resolverá la procedencia de dicha solicitud, tomando en consideración los motivos fundados y motivados, así como los documentos probatorios que juzgue necesarios para el titular de los datos. Si procede el Sujeto Obligado excluirá del tratamiento de sus sistemas los datos relativos al titular.

5

En caso de que la Unidad Administrativa determine que la información solicitada no figura en su Sistema de Datos Personales, deberá ponerlo del conocimiento del Comité de Información. Éste analizará el caso y tomará las medidas pertinentes para localizar la información solicitada. Si ésta no fuese localizada, expedirá una Resolución que comunique al solicitante la inexistencia de sus Datos Personales en el Sistema de que se trate.

6

En caso de contar con la información sobre los Datos Personales del solicitante, la Unidad Administrativa deberá remitirla en formato comprensible a la Unidad de Enlace, precisando en su caso la gratuidad de la reproducción respectiva y el costo del envío de la información, siempre y cuando la información requerida no se haya solicitado en intervalos no inferiores a doce meses.

(Ver anexo 2).

5 Cinco

Del Registro Estatal de Protección de Datos Personales y las responsabilidades y sanciones de los Sujetos Obligados

5 Del Registro Estatal de Protección de Datos Personales y las responsabilidades y sanciones de los Sujetos Obligados

El Registro Estatal de Protección de Datos Personales

¿Qué es el Registro Estatal de Protección de Datos Personales?

Es un órgano dependiente del Instituto Estatal de Acceso a la Información Pública de Oaxaca, cuyo objeto es llevar el control sobre la existencia y finalidad de los Sistemas de Datos Personales en poder de los Sujetos Obligados.

¿Para qué sirve?

Para velar por el cumplimiento de la legislación sobre protección de datos y controlar e interpretar su aplicación, especialmente en lo relativo a los derechos de Consulta, Acceso, Rectificación, Cancelación y Oposición de los datos. Adicionalmente:

1. Inscribir los sistemas de Datos Personales de los Sujetos Obligados.
2. Recomendar sobre las medidas de seguridad de los Sistemas de Datos Personales adoptados por los Sujetos Obligados.
3. Elaborar instructivos y formularios, a que se refiere el numeral Trigésimo Noveno de los Lineamientos de Políticas Generales de Protección de Datos Personales y los demás que establezca la ley.
4. Coadyuvar con los Sujetos Obligados en la publicación de los Sistemas de Datos Personales en el Registro.
5. Responder, a través de la Unidad de Enlace del Instituto, a las solicitudes de información relacionadas con la existencia y finalidad de los Sistemas de Datos Personales.
6. Coadyuvar con las distintas áreas del Instituto en la supervisión, investigación, asesoría, capacitación y difusión en la materia.
7. Expedir a los Sujetos Obligados, las constancias de inscripción de sus Sistemas de Datos Personales al Registro.
8. Formular su programa de trabajo para integrarlo al Programa de Trabajo Institucional (PTI) del Instituto.
9. Preparar el informe correspondiente a sus actividades conforme a lo dispuesto en el Plan de Trabajo Institucional.

(Art. Cuadragésimo Tercero, Lineamientos de Protección de Datos Personales)

Inscripción de los Sistemas

¿Qué es y donde se lleva a cabo la inscripción de los sistemas?



Es la obligación de los Sujetos Obligados de inscribir en el Registro Estatal de Protección de Datos Personales a través del Sistema Electrónico Multimedia de Datos Personales la existencia y creación de sus sistemas.



¿Qué es el Sistema Electrónico Multimedia de Datos Personales?



Es la herramienta electrónica creada por el IEAIP, para llevar a cabo los registros de los Sistemas de Datos Personales en poder de los Sujetos Obligados mediante los formularios de censo y pre-inscripción en línea (Ver anexos 3 y 4).



72

¿Quién y cuando tiene que llevar a cabo la inscripción?



El Titular responsable de cada Sujeto Obligado, tiene la obligación de inscribir la existencia y finalidad de los sistemas en su poder y notificar al Registro Estatal toda creación posterior.



¿Cómo se hace la inscripción?

Presentando un oficio de solicitud de inscripción (Ver anexo 5) ante el Registro Estatal de Protección de Datos Personales, dirigido al Comisionado Presidente del IEAIP, firmado por el Titular del Sujeto Obligado, anexando el formulario de censo debidamente requisitado. De no encontrar deficiencias, el Registro expedirá el oficio de autorización proporcionando la clave de usuario y contraseña para el responsable de los sistemas del Sujeto Obligado, para acceder al Sistema Electrónico Multimedia de Datos Personales con el fin de llevar a cabo la inscripción de sus sistemas.

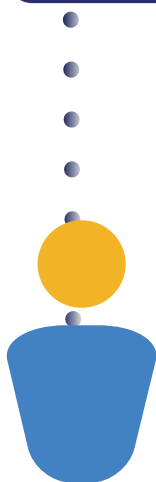
Modificación de los sistemas.

¿Qué es la modificación de los sistemas?

Es la obligación que tiene el responsable de los Sistemas de Datos Personales del Sujeto Obligado previamente inscritos de modificarlos, cuando sean inexactos o incompletos, debiendo comunicar esa modificación al Registro.

¿Cómo se procede a la modificación?

Mediante oficio del titular responsable de los Sistemas de Datos Personales dirigido al Registro Estatal de Protección de Datos Personales, indicando las modificaciones a realizar en los sistemas, previamente inscritos; el registro analizará la procedencia de las mismas. De ser procedente se permitirá nuevamente el acceso al Sistema Electrónico Multimedia de Datos Personales para que proceda a realizar dichos cambios.



Cancelación de los sistemas.

¿Qué es la cancelación de los sistemas?

Es el deber que tiene el responsable de los Sistemas de Datos Personales del Sujeto Obligado de proceder a la cancelación fundada y motivada de los que han dejado de existir y que estuvieron inscritos ante el Registro.

¿Cómo se procede a la cancelación de los sistemas?

El titular responsable de los Datos Personales debe dirigirse al Registro Estatal de Protección de Datos Personales pidiendo la cancelación total o parcial, fundada y motivada, previamente inscritos. El Registro evaluará la procedencia de la solicitud de cancelación y de encontrarla procedente la comunicará al Responsable del Sistema de Datos Personales para permitirle nuevamente el acceso al Sistema Electrónico Multimedia de Datos Personales, para realizar dicha cancelación.



La protesta sancionadora

¿Cómo se sanciona al Sujeto Obligado que no cumpla con sus responsabilidades en materia de Protección de Datos Personales?

Agotado el procedimiento establecido en el Recurso de Revisión previsto en la Ley de Protección de Datos Personales, se determinará la gravedad de la falta en que haya incurrido el responsable, a fin de que el superior jerárquico le aplique la sanción correspondiente que puede ser desde una amonestación hasta la sustitución del cargo, según lo establecido en la Ley de Responsabilidades de los Servidores Públicos del Estado y Municipios de Oaxaca, independientemente de las de orden civil o penal que puedan producirse.

Los responsables de los Sistemas de Datos Personales están sujetos al siguiente régimen sancionador:

75

- I. Usar, sustraer, destruir, ocultar, inutilizar, divulgar o alterar, total o parcialmente y de manera indebida los Datos Personales que se encuentren bajo custodia, a los cuales tengan acceso con motivo de su empleo, cargo o comisión;
- II. Negar sin causa justificada, la corrección o cancelación de Datos Personales.
- III. Efectuar la corrección o cancelación de los Datos Personales fuera de los plazos establecidos.
- IV. Realizar la cesión de datos en contravención a lo dispuesto por la Ley de Protección de Datos Personales del Estado de Oaxaca.
- V. No atender el sentido de una resolución favorable para el recurrente, emitida con motivo de la interposición del recurso revisión.

(Art. 45, Ley de Protección de Datos Personales del Estado de Oaxaca).

Anexos



INSTITUTO ESTATAL DE ACCESO A LA INFORMACIÓN
PÚBLICA DE OAXACA
FORMATO DE ACCESO, RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN
DE DATOS PERSONALES



1 MOTIVO DE LA SOLICITUD
Marque con una "X" la casillas que corresponda al procedimiento que solicita

De Acceso De Rectificación De CANCELACIÓN De Oposición

2 DOCUMENTO OFICIAL CON EL QUE SE IDENTIFICA EL SOLICITANTE O REPRESENTANTE LEGAL
(anexar copia simple)

Credencial de Elector Pasaporte vigente Cartilla del Servicio Militar
 Cedula profesional Credencial de Afiliación del IMSS, ISSSTE o INAPAM Carta o poder notarial

3 DATOS DEL SOLICITANTE O DE SU REPRESENTANTE.

Solicitante	<i>Apellido Paterno</i>	<i>Apellido Materno</i>	<i>Nombre (s)</i>
En caso de Persona Moral		<i>Denominación o razón social</i>	
Representante (en su caso)	<i>Apellido Paterno</i>	<i>Apellido Materno</i>	<i>Nombre (s)</i>
Domicilio	<i>Calle</i>	<i>No. Ext./Int.</i>	<i>Colonia o Fraccionamiento</i>
Correo Electrónico	<i>Teléfono</i>		<i>Fecha de Presentación</i>

78 4 DEPENDENCIA A LA QUE SOLICITA INFORMACIÓN

5 FORMA EN QUE DESEA LE SEA ENTREGADA LA INFORMACION
Elija con una "X" la opción deseada:

Personalmente o a través de su representante legal *En el domicilio de la Unidad de Enlace de la dependencia, entidad u organismo - Sin costo*
Por correo certificado *Con costo.*
Por mensajería *Siempre y cuando el particular, al presentar su solicitud, haya cubierto o cubra, el pago del servicio de Mensajería respectiva.*
Medios electrónicos *A través del Sistema de Solicitudes de Información Sin costo.*

En caso de seleccionar la opción de correo certificado o mensajería, favor de proporcionar los siguientes datos:

<i>Calle</i>	<i>No. Ext./Int.</i>	<i>Colonia o Fraccionamiento</i>	<i>Delegación o Municipio</i>
País	Código Postal		

Elija una opción para reproducir la información de sus datos personales:
Copias simples _____ Sin costo Copias Certificadas _____ Con costo otro tipo de medio (especificar)

6 DERECHO DE ACCESO
Si el espacio no es suficiente, puede anexar hojas a esta solicitud.
A través del Derecho de Acceso el interesado podrá obtener información sobre los datos personales objeto de tratamiento por el sujeto obligado, la finalidad del tratamiento y en su caso, el origen de dichos datos.
Describir la información que solicita, (se sugiere proporcionar todos los datos que considere facilitan la búsqueda de dicha información).

El responsable del sistema resolverá la solicitud de acceso en un plazo de 15 días hábiles desde la recepción de la presente solicitud

7

DERECHO DE RECTIFICACIÓN

Si el espacio no es suficiente, puede anexar hojas a esta solicitud
A través del Derecho de Rectificación el interesado podrá solicitar al sujeto obligado que se modifiquen los datos que resulten ser inexactos o incompletos. Indique a continuación aquellos datos que desea sean rectificadas:

Table with 3 columns: Dato correcto, Dato Incorrecto, Documento Probatorio. Row 1: 1, Anexo, hojas. Row 2: 2, Anexo, hojas.

El responsable del sistema resolverá sobre la solicitud de rectificación en un plazo de 15 días hábiles desde la recepción de la presente solicitud

8

DERECHO DE CANCELACIÓN

Si el espacio no es suficiente, puede anexar hojas a esta solicitud
El ejercicio del derecho de cancelación dará lugar a que se bloquee cualesquiera datos personales que el sujeto obligado disponga de usted en sus sistemas. En caso de que desee ejercer el derecho de cancelación sobre determinados datos, deberá indicar en un documento adicional a que datos se refiere, aportando a efecto el documento que lo justifique, en su caso.

La cancelación no procederá cuando los datos de carácter personal deban ser conservados durante los plazos previstos en las disposiciones aplicables o en las relaciones contractuales entre usted y el sujeto obligado. Especifique en forma clara y precisa los datos personales de los que solicita su cancelación

Indique las razones por las cuales considera que sus datos deben ser cancelados

El responsable del sistema resolverá sobre la solicitud de rectificación en un plazo de 15 días hábiles desde la recepción de la presente solicitud

8

DERECHO DE OPOSICIÓN (Si el espacio no es suficiente, puede anexar hojas a esta solicitud)

El Derecho de Oposición es el derecho del interesado a que no se lleve a cabo el tratamiento de sus datos de carácter personales o se cese en el mismo en los siguientes supuestos:

- 1. Cuando no sea necesario su consentimiento para el tratamiento como consecuencia de un motivo legítimo y fundado, referido a su concreta situación personal.
2. Cuando se trate de sistemas que tengan por finalidad la realización de actividades de publicidad y prospección comercial
3. Cuando el tratamiento tenga por finalidad la adaptación de una decisión referida al interesado
Cuando su oposición se realice con base al punto uno se deberá hacer constar en documento adicional los motivos fundados y legítimos relativos a su relación personal

El responsable del sistema resolverá sobre la solicitud de oposición en un plazo de 15 días hábiles desde la recepción de la presente solicitud

DATOS QUE EL SOLICITANTE PUEDE LLENAR DE MANERA OPCIONAL

*La presente información será utilizada únicamente para efectos estadísticos:

9 CURP _____ Teléfono (Clave): _____ Número: _____
Sexo: M F Fecha de Nacimiento ___/___/___ (dd/mm/aa) Ocupación: _____
¿Cómo se enteró de la existencia del procedimiento de acceso o corrección de datos personales?
Radio Prensa Televisión Cartel o Póster Internet Otro (especificar) _____

Estoy enterado y de acuerdo con el tratamiento que recibirán mis datos personales en términos del numeral Decimo Sexto de los Lineamientos de Protección Datos Personales para el Estado de Oaxaca

Firma del solicitante

Nombre y firma del servidor público que recibe la solicitud

DIAGRAMA DE FLUJO DEL PROCEDIMIENTO DE RECEPCIÓN, PROCESAMIENTO, TRÁMITE, RESOLUCIÓN Y NOTIFICACIÓN DE LAS SOLICITUDES DEL DERECHO ARCO

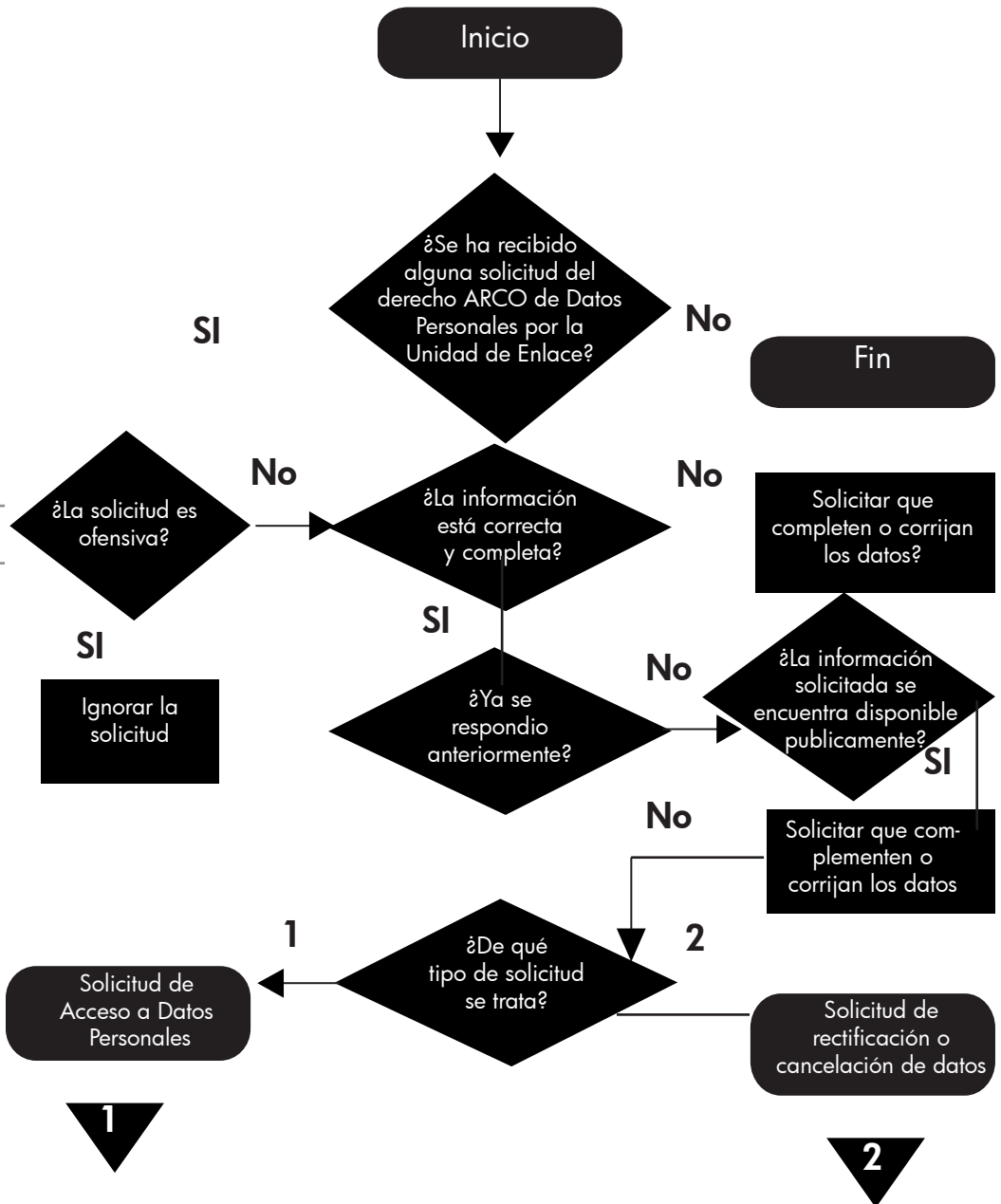


DIAGRAMA DE FLUJO DEL PROCEDIMIENTO DE RECEPCIÓN, PROCESAMIENTO, TRÁMITE, RESOLUCIÓN Y NOTIFICACIÓN DE LAS SOLICITUDES DEL DERECHO ARCO

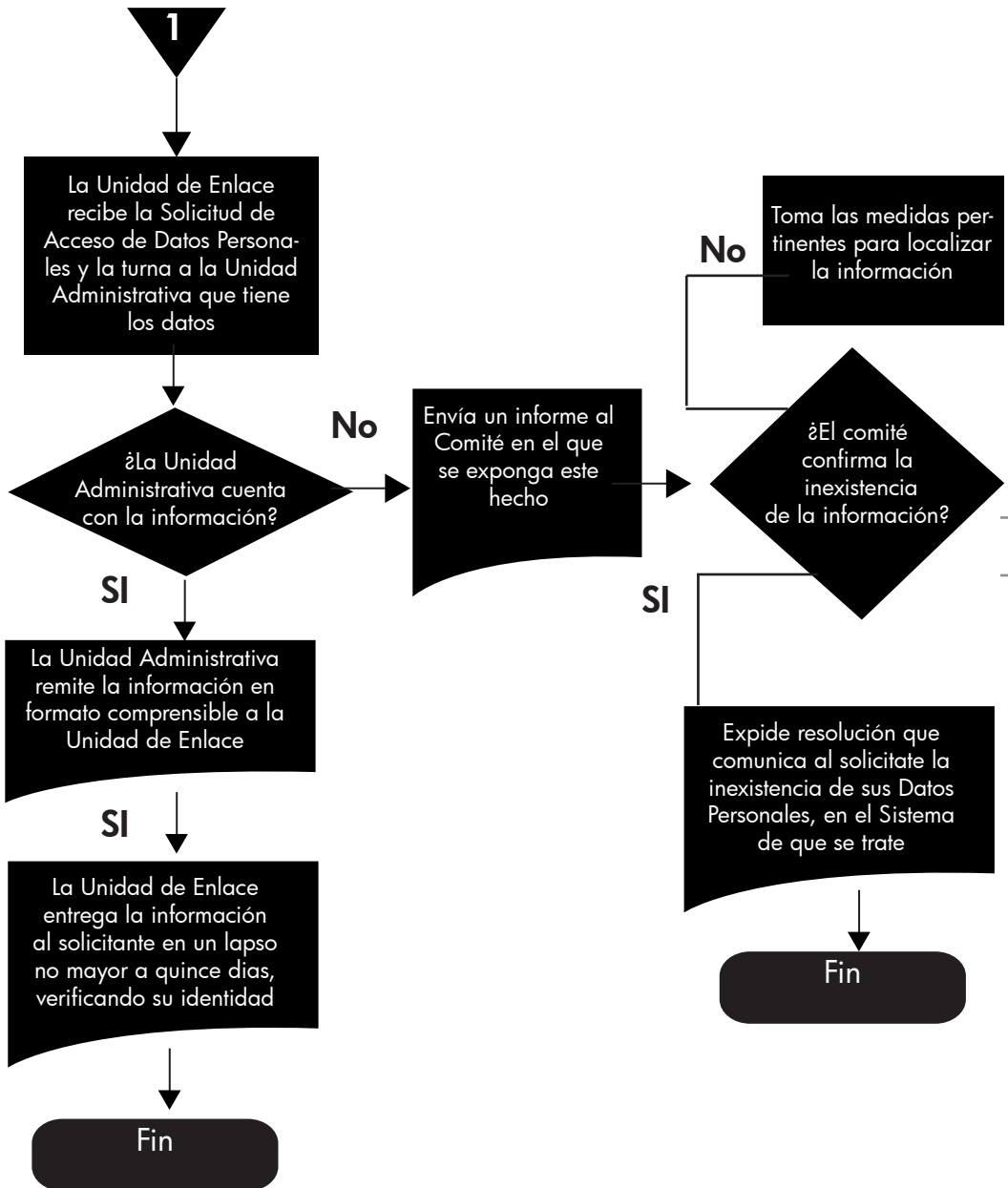
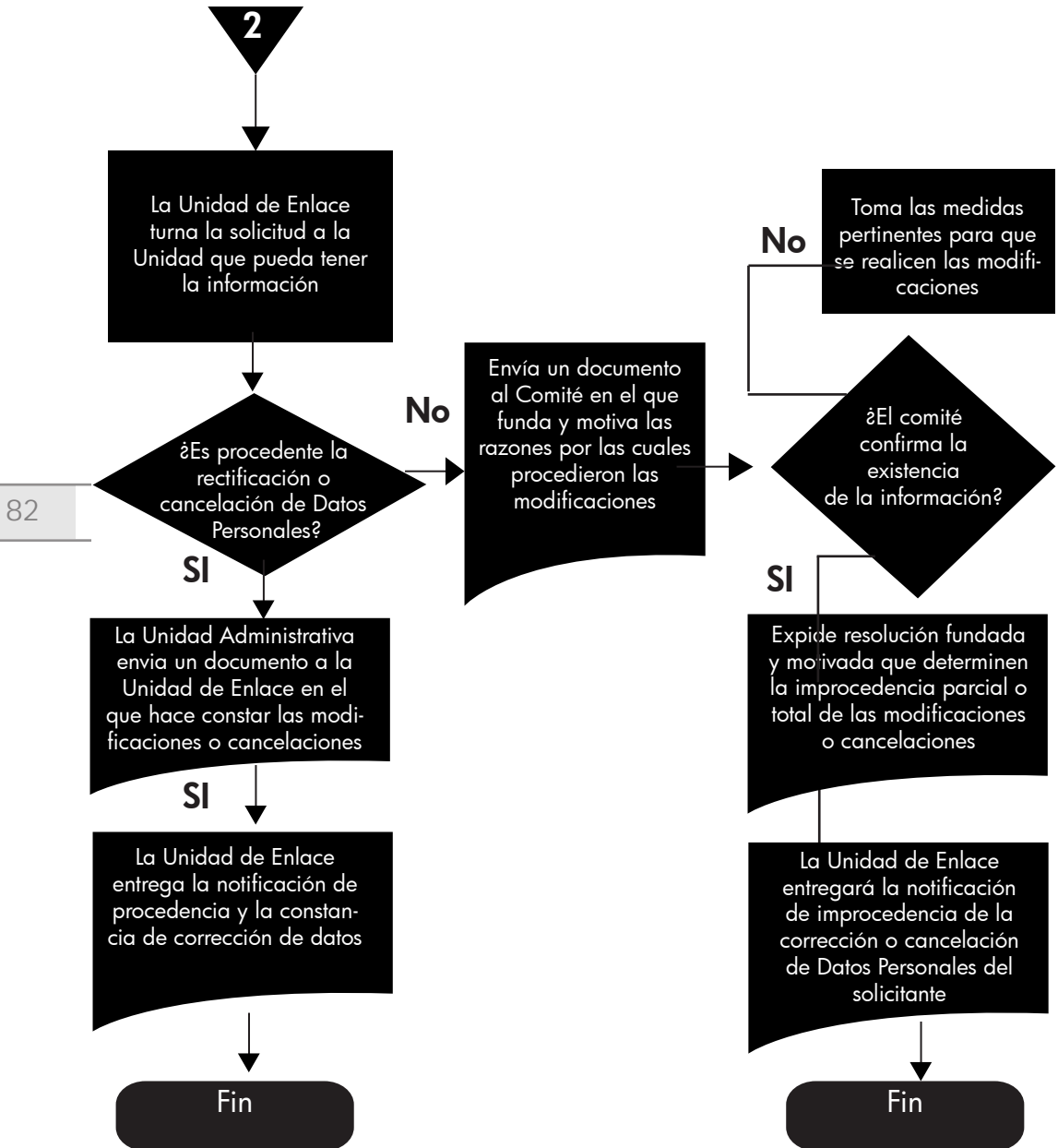


DIAGRAMA DE FLUJO DEL PROCEDIMIENTO DE RECEPCIÓN, PROCESAMIENTO, TRÁMITE, RESOLUCIÓN Y NOTIFICACIÓN DE LAS SOLICITUDES DEL DERECHO ARCO



FORMULARIO 3

CON FUNDAMENTO EN LOS ARTÍCULOS 41 FRACCIONES I, II, III, XIII Y XIV, 42, 43 Y 44 DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES DEL ESTADO DE OAXACA, ASÍ COMO EL ARTÍCULO 53 FRACCIONES I Y IX DE LA LEY DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA PARA EL ESTADO DE OAXACA, EL CONSEJO GENERAL DEL INSTITUTO ESTATAL DE ACCESO A LA INFORMACIÓN PÚBLICA HA APROBADO EL PRESENTE FORMULARIO DE CENSO E INSCRIPCIÓN PARA TODOS LOS SUJETOS OBLIGADO:

FORMULARIO DE CENSO AL REGISTRO DE SISTEMAS DE DATOS PERSONALES

ADVERTENCIA PRELIMINAR

Los datos que se ingresen en el presente formulario serán utilizados para los fines de registro, control y demás facultades que la ley otorga al Registro Estatal de Protección de Datos Personales.

Nota: Los campos indicados con un asterisco (*), son obligatorios y deben ser completados en todos los casos.

CARGA DE DATOS

1.

Marcar con una X la opción que corresponda *

Poder Ejecutivo

Poder Legislativo

Poder Judicial

Órganos Autónomos

Municipios

Otros _____

¿Qué tipo de participación tiene?

Estatal _____ Estatal / Federal _____

2 DATOS DE IDENTIFICACION DE LOS SISTEMAS *

2. a- IDENTIFICAR LOS SISTEMAS DE DATOS PERSONALES

84

N/P	UNIDAD ADMINISTRATIVA	NOMBRE ASIGNADO AL SISTEMA	RESPONSABLE DEL SISTEMA	FINALIDADES DEL SISTEMA	FUNDAMENTO LEGAL	TIPO DE SEGURIDAD	FECHA DE CREACION DEL SISTEMA	FECHA DE ULTIMA ACTUALIZACION	FASE DEL SISTEMA *				
									1	2	3	4	

ENCARGADOS	USUARIOS	DOMICILIO	LOCALIDAD	MUNICIPIO	CÓDIGO POSTAL	TELÉFONO	FAX	CORREO ELECTRÓNICO	PÁGINA ELECTRÓNICA

NOTA: 1 Creación, 2 Modificación, 3 Cancelación,

Formularios de Pre-inscripción

FORMULARIO DE PRE-INSCRIPCIÓN REGISTRO DE SISTEMAS DE DATOS PERSONALES

ADVERTENCIA PRELIMINAR

Los datos que se ingresen en el presente formulario serán utilizados para los fines de registro, control y demás facultades que la ley otorga al Registro Estatal de Protección de Datos Personales.

Nota: Los campos indicados con un asterisco (*), son obligatorios y deben ser completados en todos los casos.

1. RESPONSABLE DEL SISTEMA DE DATOS PERSONALES

a) Sujeto Obligado responsable del sistema de datos personales _____

b) Sitio que ocupa dentro de la estructura administrativa y organismo del que depende en su caso: _____

85

Marcar con una X la opción que corresponda

Poder Ejecutivo

Poder Legislativo

Poder Judicial

Órganos Autónomos

Municipios

Otros

¿Qué tipo de participación tiene?

Estatal _____ Estatal/Federal _____

2.- DATOS DE IDENTIFICACION

Nombre: _____

Domicilio: _____

Localidad: _____

Municipio: _____

Código Postal: _____

Estado: _____

Teléfono: _____

Fax: _____

Correo electrónico: _____

2. a. Nombre de usuario(s) autorizados _____

2. b. Nombre de encargado(s) autorizados

3.- NOMBRE DEL SISTEMA DE DATOS QUE REGISTRA

a) Identificar el Sistema de Datos que registra*

4. FINALIDAD DEL SISTEMA DE DATOS PERSONALES

a) Declarar las finalidades a la que se destinan los datos contenidos en el Banco de Dato

b) Fundamento legal

c) Fecha de creación

d) Fecha de última actualización

e) Tipo de seguridad aplicado

f) Tipificar las finalidades a las que se destinan los datos contenidos en el Sistema de Datos*

Marcar con una X las finalidades que posee su Sistema de Datos*

-Gestión Administrativa: ____

-Gestión de Personal: ____

-Gestión Económica: ____

-Gestión Fiscal: ____

-Gestión de Registro: ____

-Gestión notarial: ____

-Administración de Bienes e Inventarios: ____

-Asesoramiento, consultoría y servicios relacionados: ____

-Asesoramiento Legal: ____

-Auditoría: ____

- Policial: ____
- Inteligencia: ____
- Seguridad interior: ____
- Defensa: ____
- Militar: ____
- Justicia: ____
- Criminalidad y Sistema Penitenciario: ____
- Culto: ____
- Educación: ____
- Medios de Comunicación: ____
- Salud: ____
- Medicamentos, Alimentos y Tecnología Médica: ____
- Administración de Centros de Salud: ____
- Cultura: ____
- Turismo: ____
- Deportes y recreación: ____
- Prensa y difusión: ____
- Medio ambiente: ____
- Recursos Naturales: ____
- Gestión de Servicios Públicos: ____
- Transporte: ____
- Seguridad y Previsión Social: ____
- Asistencia, Servicios y Planes Sociales: ____
- Gestión de empleo y Capacitación: ____
- Minoridad y familia: ____
- Prevención de riesgos de Trabajo: ____
- Gestión Bancaria y Financiera: ____
- Cumplimiento/Incumplimiento de Obligaciones Tributarias: ____
- Gestión de fondos de Jubilación, Pensión y similares: ____
- Publicidad: ____
- Prestación de Servicios de Información: ____
- Encuestas de Opinión, Mediciones y Estadísticas: ____
- Gestión de Servicios de Telecomunicaciones: ____
- Prestación de Servicios de Certificación: ____
- Ciencia y Tecnología: ____
- Finalidades históricas: ____

-Investigación Epidemiológica y similar: ____

-Otros: ____

g) ¿Es un fichero con fines de Defensa Nacional o Seguridad Pública?*

Si ____ No ____

5. NATURALEZA DE LOS DATOS PERSONALES CONTENIDOS EN EL SISTEMA DE DATOS

a) ¿Trata datos sensibles?* Si ____ No ____

b) ¿Trata datos relativos a la salud?* Si ____ No ____

c) Especificar los datos personales que trata:* _____

88

Señalar con una X los datos que posee su archivo*

5.C.1 DATOS DE IDENTIFICACION:

-Acta de Nacimiento: ____

-Credencial de Elector: ____

-Pasaporte: ____

-Licencia de conducir: ____

-CURP: ____

-Nombres y apellidos: ____

-Domicilio: ____

-Correo Electrónico: ____

-Firma Electrónica / Digital: ____

-Firma Manuscrita: ____

-Foto / Imagen: ____

-Voz: ____

-Huella digital: ____

-Teléfono: ____

5.C.2. DATOS VINCULADOS AL ESTADO CIVIL Y CARACTERÍSTICAS PERSONALES:

- Estado Civil: ____
- Fecha de Nacimiento: ____
- Lugar de Nacimiento: ____
- Defunción: ____
- Parentesco y datos de familia: ____
- Edad: ____
- Sexo: ____
- Nacionalidad: ____
- Otros: ____

5.C.3. DATOS SOCIALES:

- Características de alojamiento y vivienda: ____
- Preferencias de consumo: ____
- Viajes: ____
- Pertenencia a Clubes/Asociaciones: ____
- Licencias, Permisos y Autorizaciones: ____
- Otros: ____

5.C.4. DATOS ACADÉMICOS Y PROFESIONALES:

- Expediente del estudiante o profesional: ____
- Títulos: ____
- Asociaciones académicas y/o estudiantiles: ____
- Antecedentes profesionales u oficio: ____
- Pertenencia a Colegios o Asociaciones profesionales: ____
- Becas: ____
- Otros: ____

5.C.5 DATOS LABORALES Y SEGURIDAD SOCIAL:

- Grado o Profesión: ____
- Categoría: ____
- Puesto de Trabajo: ____
- Evaluaciones, Rendimiento: ____
- Informe Socio-Ambiental: ____
- Expediente del Trabajador: ____
- Sanciones: ____
- Historia clínica: ____
- Datos Clínicos /Pre-Ocupacionales: ____
- Obra Social: ____
- Afiliación a Institución de Seguridad Social: ____
- Afiliación a Asociación de Fondo para el Retiro (AFORE): ____
- Afiliación de Sistema de Reparto: ____
- Pensiones: ____
- Jubilaciones: ____
- Afiliación sindical: ____
- Otros: ____

5.C.6. DATOS PATRIMONIALES:

- Actividades y negocios: ____
- Balances y resultados contables: ____
- Contratos y Transacciones comerciales: ____
- Licencias comerciales: ____
- Ingresos, Rentas: ____
- Sueldos y jornales: ____
- Inversiones: ____
- Créditos a percibir: ____
- Operaciones financieras: ____
- Deudas contraídas con el sistema financiero: ____
- Deudas contraídas fuera del sistema financiero: ____
- Fianzas y garantías: ____
- Prendas: ____
- Hipotecas: ____

- Juicios y reclamos: ____
- Cheques y/o Facturas de Créditos: ____
- Datos Bancarios: ____
- Tarjetas de Crédito: ____
- Seguros de Retiro: ____
- Seguros de Vida: ____
- Seguros: ____
- Declaraciones Patrimoniales: ____
- Inmuebles: ____
- Buques: ____
- Aeronaves: ____
- Automotores: ____
- Maquinas y/o Equipos y/o demás bienes registrables: ____
- Acciones y/o Títulos, Valores: ____
- Creaciones artísticas, literarias, científicas o técnicas: ____
- Datos Tributarios: ____
- Otros: ____

5.C.7. DATOS RELATIVOS A LA SALUD:

- Historia clínica: ____
- Estudios Médicos: ____
- Consumo de Medicamentos: ____
- Investigación médica: ____
- Otros: ____

5.C.8. CARACTERISTICAS FISICAS

- Pigmentación ____
- Pelo ____
- Frente ____
- Ojos ____
- Nariz ____
- Señales visibles ____
- Estatura ____

5.C.9. CARACTERISTICAS PERSONALES

- ADN _____
- Tipo de sangre _____
- Huella digital _____

5.C.10. TRANSITO Y MOVIMIENTOS MIGRATORIOS

5.C.11. ¿COMO RELACIONA LA INFORMACION REGISTRADA?

- Por nombre: _____
- Por documento de identidad: _____
- Por Identificación Tributaria (Cédula fiscal R.F.C.): _____
- Por código (clave): _____
- Otros: _____

92

6. PROCEDIMIENTOS DE OBTENCION Y ACTUALIZACION DE DATOS:

- a)¿Recaba los datos directamente de su titular?* Si ___ No ___
- b)¿Los datos deben ser facilitados de manera obligatoria?* Si ___ No ___
- c)¿Recaba los datos por transmisión de otros organismos públicos?*
Si ___ No ___
- d)Recaba los datos por transmisión de personas privadas o entes no estatales?* Si ___ No ___
- e)¿Recaba datos de archivo público?* Si ___ No ___

7. TRANSMISIÓN DE LOS DATOS:

a) ¿Efectúa alguna de las transmisiones previstas por la Ley?* Si ___ No ___

¿Con quien efectúa las transmisiones?

b) ¿Efectúa transmisiones de datos a terceros?* Si ___ No ___

¿Con quien efectúa las transmisiones?

c) ¿Efectúa interconexiones con otros Sistemas de Datos?* Si ___ No ___

¿Con quien efectúa las interconexiones?

d) ¿Efectúa Transferencia Interestatal de datos?* Si ___ No ___

¿Con quien efectúa las transferencias?

e) ¿Efectúa Transferencia Internacional de Datos?* Si ___ No ___

¿Con quien efectúa las transferencias?

8. TIPO DE SOPORTE DEL SISTEMA DE DATOS

a) Indicar con una X la opción que corresponda*

- Manual
- Informatizado
- Manual/Informatizado

b) En el caso de operar mediante una página en internet indicar la Dirección Electrónica:

9. UNIDAD DE ENLACE ANTE LA CUAL LOS TÍTULARES DE LOS DATOS PUEDEN EJERCER SUS DERECHOS:

-Nombre de la Oficina*: _____

-Dirección*: _____

-Localidad*: _____

-Municipio*: _____

-Código Postal*: _____

-Estado*: _____

-Teléfono*: _____

En caso de operar mediante una página en Internet indicar la Dirección Electrónica*: _____

—

10. SERVICIO DE TRATAMIENTO DE DATOS POR TERCEROS

¿Contrata a terceros para realizar el tratamiento de sus datos?*

Si ____ No ____

CONFIRMACION DE CARGA DEL SISTEMA DE DATOS

Confirme si procesa la carga del Sistema de Datos o si desea cancelar el proceso

PROCESAR

CANCELAR

Nota de solicitud de inscripción

En _____, a _____ días de _____

C.

Comisionado Presidente del IEAIP.

Sirva este medio para solicitar que proceda a tomar nota de la solicitud de INSCRIPCIÓN de los Sistemas de Datos que se especifican en la copia simple del formulario que se adjunta a la presente, suscrito en todas sus páginas.

En mi carácter de _____, de _____, responsable del Sistema de Datos, declaro bajo protesta de decir verdad que los datos denunciados en el formulario que adjunto son ciertos.

95

Nombre y apellido del firmante: _____

Tipo de documento: _____ No. hojas _____

Calle: _____ No.: _____ Piso: _____ Depto. Int.: _____

Localidad: _____ C.P.: _____ Municipio: _____

Estado: _____ Teléfono: _____ Fax: _____

Correo Electrónico: _____

El domicilio denunciado se constituye como domicilio especial a los fines de cualquier notificación que corresponda cursar a nuestra parte con motivo de la inscripción en el registro a su digno cargo.

Lo saluda

Referencias Documentales

-IEAP, "Documentos Fundamentales", Ed. IEAIP, Septiembre 2008, Oaxaca de Juárez, Oax.

-IEAIP, "Lineamientos de Protección de Datos Personales" emitidos el 14 Enero 2009, Oaxaca de Juárez, Oax.

-UNAM ; CIDE, IFAI, "Código de Buenas Practicas y Alternativas para el Diseño de Leyes de Transparencia y Acceso a la Información Pública en México", Ed. IFAI, Abril 2008, México, D.F.

-IFAI, "Recomendaciones Sobre Medidas de Seguridad Aplicables a los Sistemas de Datos Personales", Ed. IFAI, México, D.F.

Vinculos de interés

<http://www.ieaip.org.mx>

http://www.ieaip.org.mx/datos_personales

<http://www.ieaip.org.mx/sistema2>

http://ieaip.org.mx/biblioteca_virtual/index



Manual de Protección de Datos Personales
Se terminó de imprimir en el mes de agosto de 2009
Tiraje: 1,000 ejemplares
Edición del Instituto Estatal de Acceso a la Información Pública de Oaxaca



Nota: Se autoriza la reproducción total o parcial de este manual a condición de citarlo completo o las partes del mismo que se utilicen por terceros, con aviso al IEAIP.



Instituto Estatal de Acceso
a la Información Pública de Oaxaca

Instituto Estatal de Acceso a la Información Pública de Oaxaca

Ampolal N. 510 Colonia Reforma, C.P. 68050

Oaxaca de Juárez, Oaxaca.

(951) 51 5 11 90 - 51 5 22 57 - 51 5 23 21

01 800 00 43247

www.ieaip.org.mx