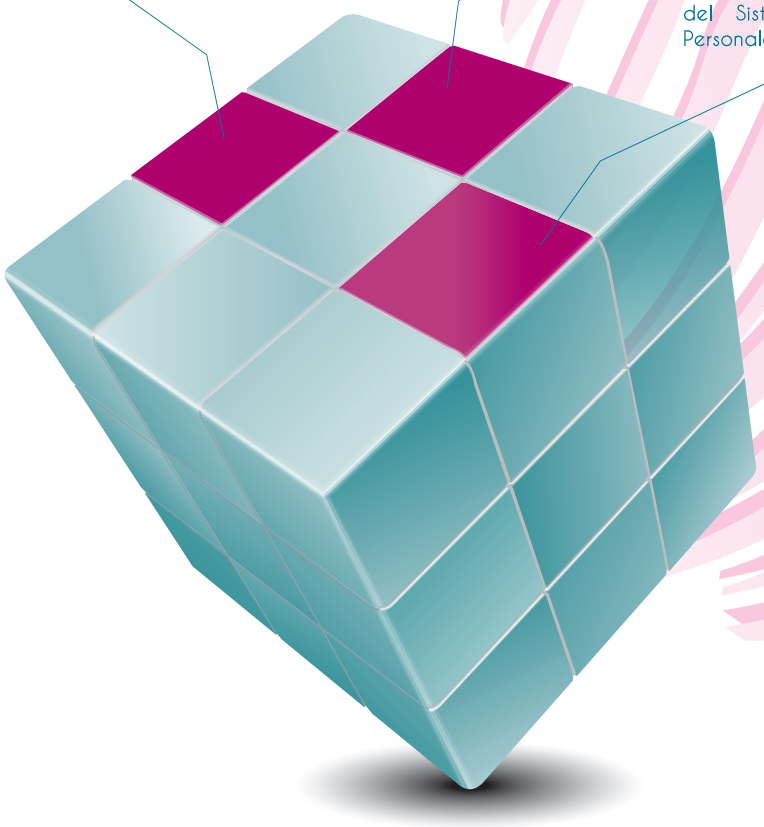
Guía para Servidores Públicos

¿Cómo cumplir con la Ley de Protección de Datos Personales para el Distrito Federal?

¿ En qué norma se regula el derecho a la Protección de los Datos Personales ?

¿ Qué es un Sistema de Datos Personales?

¿ Quién es el responsable del Sistema de Datos Personales ?



infodf
Instituto de Acceso a la Información Pública
y Protección de Datos Personales del Distrito Federal

Guía para Servidores Públicos ¿Cómo cumplir con la

Ley de Protección de Datos Personales para el Distrito Federal?

DIRECTORIO

Oscar Mauricio Guerra Ford
Comisionado Ciudadano Presidente

Mucio Israel Hernández Guerrero
Comisionado Ciudadano

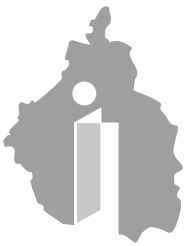
David Mondragón Centeno
Comisionado Ciudadano

Luis Fernando Sánchez Nava
Comisionado Ciudadano

Alejandro Torres Rogelio
Comisionado Ciudadano

Autora del Texto
Gabriela Inés Montes Márquez
Directora de Datos Personales

Equipo Técnico
Ignacio Núñez Ruíz
Perla Isabel López Iturbe
José Fermín Aguilar Mandujano
Luis Pedro González Solís
María del Carmen Saavedra Velasco
Andrés Espinosa Castellanos
David Guzmán Corroviñas



infodf

Instituto de Acceso a la Información Pública
y Protección de Datos Personales del Distrito Federal

Guía para Servidores Públicos ¿Cómo cumplir con la

Ley de Protección de Datos Personales para el Distrito Federal?

ÍNDICE

Apartado I
Conceptos Generales

Apartado II
Enlace en Materia de Datos Personales

Apartado III
De los Responsables de los Sistemas de Datos Personales

Apartado IV
De los Encargados y Usuarios

Apartado V
De las Oficinas de Información Publica y los procedimientos de los Derechos ARCO

Índice
De Conceptos

Introducción

La *Guía para Servidores Públicos, ¿Cómo cumplir con la Ley de Protección de Datos Personales para el Distrito Federal?*, como su nombre lo indica, tiene como propósito poner al alcance de los servidores públicos del Distrito Federal, un instrumento accesible que les permita dar cumplimiento a las diversas obligaciones establecidas en la citada ley.

Este documento está concebido como un instrumento dinámico, que pueda ser fácilmente usado y actualizable por aquellos servidores públicos involucrados en el tratamiento de los datos personales.

Con el objetivo de facilitar su manejo se diseñaron diversos apartados que deben ser revisados de acuerdo al perfil del personal.

En el primer apartado se concentran conceptos generales que es importante conocer. Esta sección debe ser revisada por la totalidad del personal que interviene en el tratamiento de los datos personales, pues en ésta se presenta una contextualización del tema y conceptos como "datos personales" ó "sistemas de datos personales", y se hace un perfil de las personas involucradas en el tratamiento de los datos.

La segunda sección está dirigida al *Enlace* en materia de datos personales. Si bien se recomienda que el *Enlace* conozca la información que corresponde a todos los perfiles, por ser quien coordinará al interior del Ente Público el cumplimiento de las disposiciones contenidas en la *Ley de Protección de Datos Personales para el Distrito Federal* (LPDPDF), es indispensable que tenga un buen nivel de comprensión de la información relacionada con el cumplimiento de la LPDPDF.

La tercera sección de la *Guía* contiene los conocimientos esenciales para el *Responsable* del sistema de datos personales. En la cuarta sección se incluyen algunas recomendaciones específicas para los encargados y usuarios involucrados en el tratamiento de los datos

personales. La información de esta sección también debe ser conocida por el *Responsable,* pues es quien deberá supervisar que las funciones sean cumplidas de manera adecuada.

En quinto lugar, se incluye la información más relevante para el titular de la *Oficina de Información Pública*, instancia estratégica en el régimen de protección de datos personales. En este apartado se incluye la información más importante para el encargado de atender las solicitudes de acceso, rectificación, cancelación y oposición a los datos personales.

Por último, se incluye una sección en la que el lector podrá identificar con mayor facilidad los conceptos clave en materia de datos personales, así como un listado de preguntas frecuentes con la indicación del lugar en donde podrá ser localizada la respuesta a este tipo de preguntas.

Apartado I

Conceptos Generales

Derecho a la Protección de Datos Personales[1]

En México, el derecho a la protección de datos personales es reconocido por la Constitución Política de los Estados Unidos Mexicanos. Es importante señalar que este derecho, si bien guarda estrecha relación con el derecho a la intimidad y el derecho de acceso a la información, es independiente de éstos.

El derecho fundamental a la protección de datos, como anota Piñar Mañas (2005, p. 23) "a diferencia del derecho a la intimidad, con quien comparte objetivos de ofrecer una eficaz protección constitucional de la vida privada y familiar, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización y omisión de determinados comportamientos concretados en la Ley".

De esta manera, este derecho puede ser entendido como la facultad del titular de los datos personales de decidir a quién proporcionar información, cómo y para qué será utilizada; del mismo modo, permite a las personas acceder, rectificar, cancelar y oponerse al tratamiento de su información personal.

Regulación Constitucional del Derecho a la Protección de Datos Personales

Los órganos garantes que tutelan este derecho fundamental son el Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal (INFODF), y el Instituto Federal de Acceso a la Información Pública y Protección de Datos (IFAI). Estos organos velan por el adecuado cumplimiento de lo dispuesto por los artículos 6 y 16 de la Constitución Política de los Estados Unidos Mexicanos, y las leyes que de ellos derivan; en caso de controversia se constituyen como un órgano cuasi-jurisdiccional, que inclina la balanza al que le asista la razón, con neutralidad y autonomía.

---

[1] Se agradece la valiosa colaboración del Mtro. Rodrigo Santisteban Maza en la realización de la presente *Guía*.

A pesar de que en México estamos en la fase de gestación de éste derecho humano, y por ende contamos con muy pocas leyes especializadas en el tema, actualmente 8 entidades federativas cuentan con una normativa en la materia además de la federación. Los legisladores, a fin de no ensanchar más la estructura administrativa, se han valido de la existencia de figuras preexistentes como Consejos, Comisiones o Institutos de Transparencia y Acceso a la Información Pública, para fungir como organos garantes de este derecho.

En forma independiente a las obvias limitaciones territoriales, los órganos estatales o del Distrito Federal –que ya cuentan con una ley en la materia–, tienen un campo de acción circunscrito a los datos personales que se encuentran en posesión del sector público, sin poder vigilar aquellos que se encuentran en poder del sector privado, ya que estos son supervisados por el Instituto Federal de Acceso a la Información y Protección de Datos (IFAI).

Lo anterior se debe a una explicación sencilla. El Congreso de la Unión, previo a la reforma por la que se adicionó un segundo párrafo al artículo 16 constitucional, se atribuyó la competencia exclusiva de regular el tema de protección de datos personales en posesión de los particulares, esto en los términos del artículo 73, fracción XXIX-O, de la Constitución Política de los Estados Unidos Mexicanos, que a la letra señala:

> Artículo 73. El Congreso tiene facultad:
> …
> XXIX-O. Para legislar en materia de protección de datos personales en posesión de particulares.
> …

Lo anterior se traduce en que los congresos locales o incluso la Asamblea Legislativa del Distrito Federal, sólo pueden emitir una legislación que regule dicho tema en el sector público de cada entidad. Es de señalar que, desde el 2010 el Congreso de la Unión expidió la *Ley*

Federal de Protección de Datos Personales en Posesión de los Particulares, la cual entró en plena vigencia en el 2012 y cuyo órgano garante es el IFAI.

A continuación se enlistan las entidades federativas que cuentan con una ley específica en la materia de protección de datos personales:

Cuadro 1. Entidades federativas que cuentan con Ley de Protección de Datos Personales.

Estado de la República con leyes en la materia	Sector Público	Sector Privado
1. Campeche	Sí	No
2. Colima	Sí	Derogado
3. Distrito Federal	Sí	No
4. Estado de México	Sí	No
5. Oaxaca	Sí	No
6. Guanajuato	Sí	No
7. Tlaxcala	Sí	No
8. Veracruz	Sí	No
9. Federación	No	Sí

Fuente: Dirección de Datos Personales del InfoDF, información al 6 de diciembre de 2012.

Es de señalar que, a pesar de que el resto de las entidades federativas o incluso la federación, no cuentan con leyes específicas en la materia de protección de datos personales, no quiere decir que no exista un cierto grado de protección de esa información, ya que las leyes de transparencia y acceso a la información pública incluyen apartados específicos para proteger los datos personales en posesión del sector público.

La anotación anterior es importante, ya que no debemos de perder de vista, que si realizamos una transferencia a otros estados de la República o la (federación), los *Responsables* de los Sistemas de Datos Personales (SDP) tienen la obligación de verificar que el destinatario del dato personal, o del

SDP, cumpla con los estándares fijados por la *Ley de Protección de Datos Personales para el Distrito Federal;* así mismo, cuando se realizan transferencias a particulares, estos pueden ser sujetos obligados de la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares,* por lo que, se les debe exigir el cumplimiento de la misma.

La Ley de Protección de Datos Personales para el Distrito Federal tutela un derecho humano reconocido por este país recientemente en la Constitución Política de los Estados Unidos Mexicanos, que a saber es el Derecho a la Protección de los Datos Personales, el cual se encuentra contemplado en los artículos 6, fracción II y 16, segundo párrafo de nuestra Carta Magna.

El artículo sexto, fracción segunda de nuestra Constitución, establece:

> "Artículo 6. …
> …
> II. 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.
> …"

De la citada fracción, podemos desprender que se encuentra compuesta por diversos componentes, que enlazados imponen una "obligación de hacer" al servidor público del Estado Mexicano, consistente en dar protección a diversa información en los términos y condiciones fijadas por las leyes expedidas para tal efecto. Los componentes se muestran en la Figura 1.

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.

Figura 1. Fuente Santiesteban (2012).

Fuente: Dirección de Datos Personales, InfoDF.

El componente que hace referencia al derecho humano a la vida privada, es comúnmente conocido como "privacidad", el cual, consiste "en la facultad que tienen los individuos para no ser interferidos o molestados, por persona o entidad alguna, en el núcleo esencial de las actividades que legítimamente decide mantener fuera del conocimiento público…" (Miguel Carbonell, 2005). En sí, el fin último del derecho humano en comento, consiste en proteger todas aquellas conductas que el ser humano realiza en un lugar privado, y que en tal contexto decide libremente dejarlo fuera del escrutinio público, lo que podemos traducir en "ser dejado en paz".

Los datos personales se entienden como toda información numérica, alfabética, gráfica, acústica o de cualquier otro tipo concerniente a una persona física identificada o identificable

En otras palabras, la privacidad consiste en facetas de nuestra conducta que, aisladamente consideradas, pueden carecer de un significado en sí mismo pero que, coherentemente enlazadas entre sí, arrojan un retrato de nuestra personalidad.

Lo anterior, nos permite señalar que la privacidad se encuentra conformada por una infinidad de acciones, conductas y datos personales; hago hincapié que éstos últimos pueden definirse como toda información numérica, alfabética, gráfica, acústica o de cualquier otro tipo concerniente a una persona física identificada o identificable, esto, de conformidad al concepto establecido en el artículo 2 de la *Ley de Protección de Datos Personales para el Distrito Federal*.

Los datos personales pueden clasificarse en distintas categorías, las cuales son enlistadas, a manera enunciativa más no limitativa, en el numeral 5 de los *Lineamientos para la Protección de Datos Personales para el Distrito Federal*. Éstas categorías son las siguientes:

> "**I. Datos identificativos:** El nombre, domicilio, teléfono particular, teléfono celular, firma, clave del Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP), Matrícula del Servicio Militar Nacional, número de pasaporte, lugar y fecha de nacimiento,

nacionalidad, edad, fotografía, demás análogos;

II. Datos electrónicos: Las direcciones electrónicas, tales como, el correo electrónico no oficial, dirección IP (Protocolo de Internet), dirección MAC (dirección Media Access Control o dirección de control de acceso al medio), así como el nombre del usuario, contraseñas, firma electrónica; o cualquier otra información empleada por la persona, para su identificación en Internet u otra red de comunicaciones electrónicas;

Categorías de Datos Personales: Identificativos; electrónicos; laborales; patrimoniales; sobre procedimientos; académicos; tránsito o migratorios; salud; biométricos; sensibles; públicos

III. Datos laborales: Documentos de reclutamiento y selección, nombramiento, incidencia, capacitación, actividades extracurriculares, referencias laborales, referencias personales, solicitud de empleo, hoja de servicio, demás análogos;

IV. Datos patrimoniales: Los correspondientes a bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, fianzas, servicios contratados, referencias personales, demás análogos;

V. Datos sobre procedimientos administrativos y/o jurisdiccionales: La información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal, fiscal, administrativa o de cualquier otra rama del Derecho;

VI. Datos académicos: Trayectoria educativa, calificaciones, títulos, cédula profesional, certificados y reconocimientos, demás análogos;

VII. Datos de tránsito y movimientos migratorios: Información relativa al tránsito de las personas dentro y fuera del país, así como información migratoria;

VIII. Datos sobre la salud: El expediente clínico de cualquier atención médica, referencias o descripción de sintomatologías, detección de enfermedades, incapacidades médicas, discapacidades, intervenciones quirúrgicas, vacunas, consumo de estupefacientes, uso de aparatos oftalmológicos, ortopédicos, auditivos, prótesis, así como el estado físico o mental de la persona;

IX. Datos biométricos: huellas dactilares, ADN, geometría de la mano, características de iris y retina, demás análogos;

X. Datos especialmente protegidos (sensibles): origen étnico o racial, características morales o emocionales, ideología y opiniones políticas, creencias, convicciones religiosas, filosóficas y preferencia sexual; y

XI. Datos personales de naturaleza pública: aquellos que por mandato legal sean accesibles al público."

El Derecho Humano a la Protección de Datos Personales permite a las personas conocer y decidir, quién, cómo y de qué manera recaba y utiliza sus datos personales

Es importante señalar que no se debe observar esa categorización realizada por el Instituto de manera rígida, sino más bien, de manera flexible, y dependerá del contexto en el que se encuentre. Por lo cual es posible incorporar nuevos tipos de datos en alguna categoría con el fin que la norma aludida continúe evolucionando.

Por ejemplo, dentro de los datos personales de naturaleza pública se encuentran los siguientes: nombre de servidores públicos, imagen de servidores públicos, número de cédula profesional, etc.

El siguiente componente contemplado en la fracción II del artículo sexto constitucional parte de la privacidad. Es el Derecho a la Protección de Datos Personales, el cual, permite a toda persona conocer y decidir, quién, cómo y de qué manera recaba y utiliza sus datos personales, cuya función es garantizar el control sobre

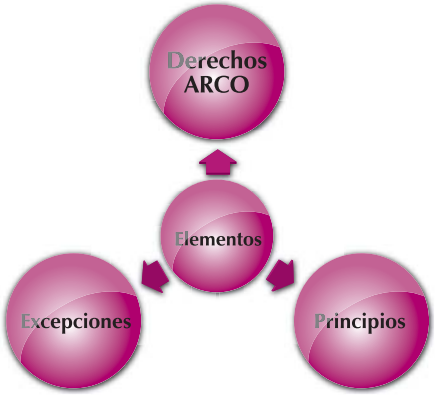
sus datos personales, tanto su uso como su destino, con el propósito de impedir su tráfico ilícito y la potencial vulneración de la dignidad del afectado.

Ahora bien, el artículo 16, segundo párrafo de la Constitución Política de los Estados Unidos Mexicanos, señala lo siguiente:

> "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."

Como se puede apreciar, el segundo párrafo del citado artículo se encuentra conformado por diversos *elementos,* que a saber son:

Figura 2. Componentes del artículo 16, segundo árrafo de la CPEUM.



Fuente: Santiesteban (2011-2)

El primer elemento lo conforman los derechos de Acceso, Rectificación, Cancelación y Oposición, comúnmente conocidos como Derechos ARCO. Las funciones de los Derechos ARCO son las siguientes:

Derechos ARCO:
Acceso
Rectificación
Cancelación y
Oposición

- **Derecho de Acceso** –también reconocido en la fracción II del artículo 6 de nuestra Carta Magna– permite a las personas físicas dar respuesta a las interrogantes planteadas anteriormente: quién, cómo, de qué manera tratarán sus datos, su utilización, y lo que ha derivado de ese tratamiento.

- **Derecho de Rectificación** –al igual que el derecho de acceso, se encuentra reconocido en el artículo 6, fracción II de la Constitución Política de los Estados Unidos Mexicanos–, permite al particular actualizar o corregir algún dato que no fuere preciso o que, por determinada circunstancia, ya no responde a su realidad.

- **Derecho de Cancelación**, este derecho permite al titular de los datos solicitar que se supriman los datos cuyo tratamiento no se encuentre ajustado a lo establecido en la Ley, lo que impone la obligación de bloquear y posteriormente su supresión.

- **Derecho de Oposición**, permite al titular solicitar que se dejen de tratar sus datos personales, cuando no se requirió su consentimiento para tal efecto, lo que, en términos del artículo 30 de la Ley de Protección de Datos Personales para el Distrito Federal, de ser procedente, derivará en una primera instancia en el bloqueo y posterior supresión.

El bloqueo de los datos personales implica que se debe identificar la información, dejarla de tratar dentro del procesamiento que se le está dando; una vez realizado lo anterior, se debe conservar para la atención de posibles responsabilidades legales o contractuales que pudieran nacer del tratamiento de los datos personales. El período de conservación será hasta en tanto haya vencido el plazo para el ejercicio de esa acción; una vez

transcurrido ese plazo, lo que procede es su baja, bajo la lógica establecida en la *Ley de Archivos del Distrito Federal*.

Para definir los plazos de conservación de información que ha sido bloqueada, es importante considerar lo que establecen las normas específicas. Un ejemplo muy claro de este tipo de normas es la *Ley Federal de Responsabilidades Administrativas de los Servidores Públicos,* entre otras leyes más.

Ahora bien, en este punto es importante señalar que el tratamiento de los datos personales, en términos del artículo 2 de la *Ley de Protección de Datos Personales del Distrito Federal,* implica:

El tratamiento de los Datos Personales se inicia en el momento en el que Ente Público los recaba

> "Cualquier operación o conjunto de operaciones que se realicen con los datos personales de una persona, a través de procedimientos automatizados o físicos, que va desde la obtención, registro, organización, conservación, utilización, cesión, difusión, interconexión, hasta la rectificación, cancelación u oposición de sus datos"

De la anterior definición, podemos desprender varios elementos:

Cuadro 2. Elementos del tratamiento de los datos.

Elemento	Componentes
Procesamiento	• Procesamiento manual • Procesamiento automatizado • Procesamiento mixto
Aplicación	• Recolección. • Registro. • Organización. • Conservación. • Extracción. • Utilización. • Elaboración o modificación de archivos. • Consulta • Comunicación o transferencia.

Fuente: Dirección de Datos Personales, InfoDF.

La LPDPDF contempla 7 principios rectores del tema de protección de Datos Personales

Como se puede observar, el tratamiento de los datos personales abarca todas las posibles acciones que el Ente Público puede realizar dentro del sistema de datos personales (SDP), el cual es definido en el artículo 2 de la Ley citada como:

> "… Todo conjunto organizado de archivos, registros, ficheros, bases o banco de datos personales de los Entes públicos, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso"

Ahora bien, los Derechos Humanos se basan en principios fundamentales y en todo momento se debe velar por su cumplimiento; en el caso específico del Derecho Humano relativo a la Protección de Datos Personales, no hay una excepción a la regla, es por ello que se le dio facultades a un órgano garante a efecto de que cuide estrictamente dicho derecho.

La ley reglamentaria en el Distrito Federal, siguiendo la tradición internacional aplicable en la materia, ha incorporado siete principios básicos, los cuales, se encuentran establecidos en el artículo 5, que a saber son los siguientes[2]:

Caudro 3. Principios reconocidos en la LPDPDF y Lineamientos.

Principio	Alcance fijado en la LPDPDF	Alcance fijado en los Lineamientos
1. Licitud:	La obtención y tratamiento de los datos personales obedecerá exclusivamente a las atribuciones legales y reglamentarias del Ente.	"I. Con relación al principio de licitud se considerará que la finalidad es distinta o incompatible cuando el tratamiento de los datos personales no coincida con los motivos para los cuales fueron recabados."

[2] Es de señalar que estos no serán desarrollados con profundidad en este momento, en virtud de que serán analizados en los subsecuentes apartados.

Principio	Alcance fijado en la LPDPDF	Alcance fijado en los Lineamientos
2. Consentimiento:	Expresión libre, inequívoca, específica e informada de la voluntad del titular de los datos personales, por medio de la cual, autoriza el tratamiento de sus datos personales.	La fracción II del, numeral 9, establece que es lo que se debe entender por cada uno de los componentes que conforman el consentimiento. Esos componentes son: "a) Libre: Cuando es obtenido sin la intervención de vicio alguno de la voluntad; b) Inequívoco: Cuando existe expresamente una acción que implique su otorgamiento; c) Específico: Cuando se otorga referido a una determinada finalidad; e d) Informado: Cuando se otorga con conocimiento de las finalidades para las que el mismo se produce."
3. Calidad de los Datos	"Los datos personales recabados deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido. Los datos recabados deberán ser los que respondan con veracidad a la situación actual del interesado"	Al igual que lo señalado en el principio anterior, la fracción III del numeral 9, indica qué es lo que se debe entender por cada uno de los componentes de éste principio, que a saber son: "a) Cierto: Cuando los datos se mantienen actualizados de tal manera que no se altere la veracidad de la información que traiga como consecuencia que el titular se vea afectado

Principio	Alcance fijado en la LPDPDF	Alcance fijado en los Lineamientos
		por dicha situación; b) Adecuado: Cuando se observa una relación proporcional entre los datos recabados y la finalidad del tratamiento; c) Pertinente: Cuando es realizado por el personal autorizado para el cumplimiento de las atribuciones de los entes públicos que los hayan recabado; d) No excesivo: Cuando la información solicitada al titular de los datos es la estrictamente necesaria para cumplir con los fines para los cuales se hubieran recabado."
4. Confidencialidad	Implica que los datos personales que han sido recabados previamente, sean mantenidos bajo secrecía –entendiendo por esto, el secreto profesional– y garantizando que sólo las personas autorizadas (Responsable, Encargado o Usuario, así como el Titular de los Datos) tengan acceso a ella[3].	"IV. Con relación al principio de confidencialidad, se Entenderá que los datos personales son: a) Irrenunciables: El interesado está imposibilitado de privarse voluntariamente de las garantías que le otorga la legislación en materia de protección de datos personales;

[3] Es importante señalar que el deber de confidencialidad o secrecía no es absoluto, toda vez que en caso de que exista una resolución judicial, o bien por razones de seguridad pública, nacional o salud pública, se puede llevar a cabo un tratamiento de datos personales por otra persona facultada para tal efecto.
Asimismo, este secreto o deber de confidencialidad que deben de observar todas las personas que intervengan en el tratamiento de los datos personales, subsistirá aún después de finalizar su relación con Ente Público.

Principio	Alcance fijado en la LPDPDF	Alcance fijado en los Lineamientos
		b) Intransferibles: El interesado es el único titular de los datos y éstos no pueden ser cedidos a otra persona; c) Indelegables: Sólo el interesado tiene la facultad de decidir a quién transmite sus datos personales; El deber de secrecía y el de confidencialidad se considerarán equiparables."
5. Seguridad	Consiste en garantizar que los datos personales de los SDP's serán tratados exclusivamente por los responsables, encargado o usuarios, previo procedimiento fijado para tal efecto.	Los lineamientos no traen señalada una correlación directa. Esto es entendible, en virtud de que el principio de seguridad se encuentra íntimamente relacionado con los tipos y niveles de seguridad[4].
6. Disponibilidad	Implica que los datos personales deben ser almacenados y tratados de tal forma, que en una primera instancia, las personas que intervienen en el tratamiento puedan realizar sus funciones, y en una segunda instancia, dar respuesta con prontitud a las solicitudes ARCO.	

[4] En forma independiente a lo señalado en el párrafo anterior, tenemos el procedimiento de disociación, el cual implica separar aquél o aquéllos datos que hacen identificable a una persona. Es decir, el resultado de la aplicación de dicho procedimiento es la imposibilidad de asociar un dato específico con un sujeto determinado.

Principio	Alcance fijado en la LPDPDF	Alcance fijado en los Lineamientos
7. Temporalidad	Este principio implica que los datos personales una vez que hayan dejado de ser útiles para la finalidad para los que fueron recabados, sean dados de baja (siguiendo para tal efecto la lógica planteada por la *Ley de Archivos del Distrito Federal*). La Ley, exceptúa de lo anterior, en los siguientes casos: …el tratamiento que con posterioridad se les dé con objetivos estadísticos o científicos, siempre que cuenten con el procedimiento de disociación". Y "… Únicamente podrán ser conservados de manera integra, permanente y sujetos a tratamiento los datos personales con fines históricos".	

Fuente: Dirección de Datos Personales, InfoDF.

Es de señalar que, actualmente, la *Ley de Protección de Datos Personales para el Distrito Federal* no reconoce de manera expresa dos principios en las legislaciones de otros países, que a saber son el de "Transparencia" y el de "Información", sin embargo, sí cuenta con algunas disposiciones en la materia, las cuales son traducidas en obligaciones que tiene el Ente Público, y que es de importancia anotarlas en este momento:

Cuadro 4. Principios implícitos en la LPDPDF.

Obligación o Principio	Alcance fijado en la LPDPDF	Alcance fijado en los Lineamientos
Transparencia	Artículo 7, fracción I. *"... Cada Ente Público deberá publicar en la Gaceta Oficial del Distrito Federal la creación, modificación o supresión de su sistema de datos personales..."*	Numeral 6. *" ... La creación, modificación o supresión de sistemas de datos personales de los Entes públicos sólo podrá efectuarse mediante acuerdo emitido por el titular del Ente o, en su caso, del órgano competente..."*
Información	Este es traducido en la Leyenda de Privacidad contemplada en el artículo 9 de la Ley; la cual debe ser informada al titular de los datos personales, previa recolección de su información.	En el numeral 13 se encuentra el modelo que debe ser observado por todos los Entes públicos.

Fuente: Dirección de Datos Personales, InfoDF.

Excepciones al Ejercicio de los Derechos ARCO

Ahora bien, el siguiente y último componente del artículo 16, segundo párrafo, de la Constitución Política de los Estados Unidos Mexicanos, habla de las excepciones que privan el ejercicio de los derechos ARCO, los cuales se refieren a las siguientes materias:

Excepciones contempladas en la Constitución Política de los Estados Unidos Mexicanos: Seguridad nacional, disposiciones de orden público, seguridad, salud pública, derechos de terceros

- Seguridad nacional
- Disposiciones de orden público
- Salud Pública
- Protección de derechos de terceros

Ley de Protección de Datos Personales para el Distrito Federal

La *Ley de Protección de Datos Personales para el Distrito Federal* fue publicada en la Gaceta Oficial del Distrito Federal el 3 de octubre del 2008 y entró en vigor al día siguiente de su publicación. Esta Ley tiene por objeto, en los términos del artículo 1, esta Ley tiene por objeto:

> *"… establecer los principios, derechos, obligaciones y procedimientos que regulan la protección y tratamiento de los datos personales en posesión de los Entes públicos…"*

La LPDPDF debe ser observada por diversos sujetos o Entes Públicos, los cuales se encuentran señalados en el artículo 2, que a saber son los sguientes:

> *"La Asamblea Legislativa del Distrito Federal; el Tribunal Superior de Justicia del Distrito Federal; El Tribunal de lo Contencioso Administrativo del Distrito Federal; El Tribunal Electoral del Distrito Federal; el Instituto Electoral del Distrito Federal; la Comisión de Derechos Humanos del Distrito Federal; la Junta de Conciliación y Arbitraje del Distrito Federal; la Jefatura de Gobierno del Distrito Federal; las Dependencias, Órganos Desconcentrados, Órganos Político Administrativos y Entidades de la Administración Pública del Distrito Federal; los Órganos Autónomos por Ley; los partidos políticos, asociaciones y agrupaciones políticas; así como aquellos que la legislación local reconozca como de interés público y ejerzan gasto público; y los Entes equivalentes a personas jurídicas de derecho público o privado, ya sea que en ejercicio de sus actividades actúen en auxilio de los órganos antes citados o ejerzan gasto público"*

En el cuadro 5 se muestra la estructura de la Ley.

Caudro 5. Estructura de la LPDPDF.

Título Primero	**DISPOSICIONES COMUNES PARA LOS ENTES PÚBLICOS**	
	Capítulo Único	Disposiciones generales
Título Segundo	**DE LA TUTELA DE LOS DATOS PERSONALES**	
	Capítulo I	De los principios
	Capítulo II	De los Sistemas de Datos Personales
	Capítulo III	De las medidas de seguridad
Título Segundo	**DE LA TUTELA DE LOS DATOS PERSONALES**	
	Capítulo IV	Del tratamiento de los Datos Personales
	Capítulo V	De las Obligaciones de los Entes Obligados
Título Tercero	**DE LA AUTORIDAD RESPONSABLE DEL CONTROL Y VIGILANCIA**	
	Capítulo Único	Del Instituto y sus atribuciones
Título Cuarto	**DE LOS DERECHOS Y PROCEDIMIENTOS PARA SU EJERCICIO**	
	Capítulo I	Derechos en materia de datos personales
	Capítulo II	Del procedimiento
	Capítulo III	Del recurso de revisión
Título Quinto	**DE LAS RESPONSABILIDADES**	
	Capítulo Único	De las infracciones
Transitorios		

Fuente: Dirección de Datos Personales, InfoDF.

Las infracciones a la *Ley de Protección de Datos Personales para el Distrito Federal*, se encuentran contempladas en el artículo 41, el cual enlista las siguientes causales:

- Incumplimiento de cualquiera de las disposiciones, principios u obligaciones contenidos en la Ley.
- Crear sistemas de datos personales, sin la publicación en la Gaceta Oficial del Distrito Federal.

- Obtener datos personales de manera engañosa o fraudulenta (por ejemplo: recabar datos personales sin el consentimiento expreso, en los casos que se requiera, o bien, recabarlos sin informar las advertencias contenidas en el Art. 9 de la LPDPDF).
- Destruir, alterar, ceder datos personales, archivos o datos personales sin autorización.
- Transmitir datos personales, fuera de los casos permitidos, particularmente cuando la transmisión haya tenido por objeto obtener un lucro debido.
- Transgredir las medidas de seguridad referidas en la Ley.
- Omisión o irregularidad en la atención, ejercicio de las solicitudes ARCO, así como impedir, obstaculizar o negar el ejercicio de los derechos ARCO.
- Omitir o presentar de manera extemporánea los informes solicitados por el Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal.
- Omitir total o parcialmente el cumplimiento de las resoluciones emitidas por el Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, así como obstruir las funciones del mismo.
- Impedir u obstaculizar la inspección ordenada por el Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, o la instrucción de bloqueo del sistema de datos personales.

Existen diversos ordenamientos emitidos por el Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, que aterriza diversas disposiciones contempladas en la citada Ley, y que se deben estar observando dentro del tratamiento de los datos personales o gestionando las solicitudes que sean presentada. Estos se indican en el cuadro 6:

Caudro 6. Normatividad complementaria a la LPDPDF.

Ordenamiento	Objetivo
Lineamientos para la Protección de Datos Personales en el Distrito Federal.	*"… establecer las directrices y criterios para la aplicación e implementación de la Ley de Protección de Datos Personales para el Distrito Federal"* (numeral 1)
Lineamientos para la gestión de solicitudes de información pública y de datos personales a través del sistema INFOMEX del Distrito Federal.	"… establecer las reglas de operación de INFOMEX[5] en el Distrito Federal…" (numeral 1)
Procedimiento para la Atención de las Denuncias de un posible incumplimiento a la Ley de Protección de Datos Personales para el Distrito Federal.	*"Establecer las políticas y procedimientos, así como, identificar los órganos del Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal responsables de la recepción, atención, resolución y seguimiento de las denuncias que los particulares presenten por un posible incumplimiento a las obligaciones contenidas en la Ley de Protección de Datos Personales para el Distrito Federal, con excepción de aquellas referentes al ejercicio de los derechos de Acceso, Rectificación, Cancelación u Oposición (ARCO) y los relativos a la facultad de inspección del Instituto de Acceso a la Información Pública del Distrito Federal y Protección de Datos Personales, que debe realizar a los sistemas de datos personales de los Entes Obligados"* Numeral I.

[5] El INFOMEX, es el:
"… sistema electrónico mediante el cual las personas podrán presentar sus solicitudes de acceso a la información pública y de acceso, rectificación, cancelación y oposición de datos personales y es el sistema único para el registro y captura de todas las solicitudes recibidas por los Entes obligados a través de los medios señalados en la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal y la Ley de Protección de Datos Personales para el Distrito Federal, así como para la recepción de los recursos de revisión interpuestos a través del propio sistema..."
Esto en los términos del numeral 1, segundo párrafo, de los *Lineamientos para la Gestión de las solicitudes de información pública y de datos personales a través del Sistema INFOMEX del Distrito Federal.*

Ordenamiento	Objetivo
Acuerdo mediante el cual se aprueba la versión 2.0 del Registro Electrónico de Sistemas de Datos Personales.	Mejorar la operación y usabilidad del Registro Electrónico.

Fuente: Dirección de Datos Personales, InfoDF.

Como podemos observar, el Distrito Federal cuenta con un marco jurídico amplio que regula de una u otro forma al Derecho Humano de Protección de Datos Personales. En los siguientes apartados, iremos analizando esa normatividad con detenimiento, de acuerdo a cada uno de los temas que se irán planteando.

Sistemas de Datos Personales

Los datos personales que detentan los Entes Públicos deben estar integrados en un sistema de datos personales para garantizar su adecuada protección. El sistema de datos personales (SDP) puede ser conceptualizado como el "cajón" donde habremos de guardar los datos que recabamos.

Es importante tener plenamente identificados los sistemas de datos personales en posesión de nuestro Ente Público, pues la totalidad de los datos que tratemos, deben formar parte de un sistema.

Los SDP se pueden definir como:

Los SDP se pueden definir como: todo conjunto organizado de archivos, registros, ficheros, bases o banco de datos personales de los Entes públicos, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso

> *"… Todo conjunto organizado de archivos, registros, ficheros, bases o banco de datos personales de los entes públicos, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso"*

De lo anterior podemos desprender que, los SDP son un conjunto de archivos organizados –desde la óptica de la *Ley de Archivos del Distrito Federal*–, que contienen datos personales, cuyo nacimiento o conformación depende de las atribuciones normativas conferidas al Ente Público de que se trate.

La *Ley de Protección de Datos Personales para el Distrito Federal*, reconoce que los sistemas pueden encontrarse en diversos tipos de soportes, los cuales pueden ser: físicos (conjunto de expedientes que contiene datos personales), electrónicos[6] (conjunto de bases o expedientes electrónicos que contienen datos personales). En muchos de los casos puede decirse que los sistemas se encuentran en medios mixtos, pues su soporte se encuentra tanto de forma material como electrónica.

El responsable del sistema debe tener especial cuidado en no confundir la noción de "sistema de datos personales", con una aplicación informática, pues un SDP puede utilizar diversas aplicaciones o software para que los datos puedan ser tratados conforme a la finalidad para la cual fueron recabados.

La totalidad de los sistemas de datos personales en posesión de los Entes Públicos deben estar inscritos en el Registro Electrónico de Sistemas de Datos Personales (RESDP), por ello a continuación nos referiremos a esta herramienta electrónica..

Registro Electrónico de Sistemas de Datos Personales

El RESPD es una aplicación tecnológica que permite conducir el esquema de inscripción y control de los sistemas de datos personales identificados por los Entes Públicos, la cual se basa en "perfiles" o en "roles", en donde el InfoDF tiene el carácter de administrador general; el Enlace del Ente Público en materia de datos personales funge como "Administrador del Ente"; y el Responsable del SDP como "Operario de Unidad Administrativa"[7].

El RESDP es una aplicación tecnológica que permite conducir el esquema de inscripción y control de los SDP identificados por los Entes públicos, la cual se base en perfiles o en roles.

[6] Los programas informáticos COI, NOI, LOTUS, etc., no constituyen sistemas de datos personales por sí mismos, solamente son aplicaciones informáticas para tratar datos personales.
[7] En los subsiguientes apartados, analizaremos las figuras señaladas en el párrafo y los roles u obligaciones que tienen dentro del RESDP.

El RESDP se encuentra conformado por varias secciones o apartados, en los que, se deben asentar las características de cada uno de los SDP. Los apartados y sus componentes son:

I. Datos del Sistema
- Nombre del Sistema;
- Finalidad o uso previsto;
- Fecha de publicación en GODF;
- Unidad Administrativa Responsable;

II. Responsable
- Nombre;
- Cargo Administrativo;
- Domicilio oficial (Calle, Número, Interior, Colonia, Código Postal, Delegación, y Ciudad) Correo electrónico oficial o institucional, Teléfono oficial y Fax (opcional)

III. Encargado
- Nombre
- Cargo administrativo

IV. Usuario
- Nombre Usuario;
- Domicilio (Calle, Número, Interior,
- Colonia, Código Postal, Delegación y Ciudad);
- Denominación del acto jurídico;
- Finalidad permitida;
- Vigencia del acto jurídico.

V. Origen
- Categoría;
- Tipo de datos;
- Origen de los datos personales
- Grupo de personas origen;
- Forma de recolección;
- Medio de actualización;
- Tratamiento.

VI. Destino

- Tipo de destinatario;
- Destinatario;
- Tipos de datos transferidos;
- Finalidad genérica de la transmisión;
- Fundamento legal de la transmisión;

VII. Interrelación

- Relación con otros sistemas;
- Finalidad de la interrelación;

VIII. Tiempo de conservación

- Tiempo de conservación en medio automatizado;
- Tiempo de conservación en el archivo de trámite;
- Tiempo de conservación en archivo de concentración;
- Transferencia de la información contenida en el sistema al archivo histórico.

IX. Seguridad

- Nivel de seguridad utilizado para resguardar los datos contenidos en el sistema, conforme a lo dispuesto en el artículo 14 de la *Ley de Protección de Datos Personales en el Distrito Federal*.

Antes de continuar, es necesario dejar asentado varias recomendaciones sobre el uso del RESDP:

✦ Los navegadores Web recomendables son: Internet Explorer 8 y 9; Mozilla FireFox y Google Chrome.
✦ Durante el uso del RESDP:

- No utilizar las flechas de navegación (Atrás y Adelante) de la página web.
- No cerrar la sesión desde el navegador;
- No tener activado el protector de pantalla cuando se encuentre en sesión;
- No bloquear el equipo cuando se

encuentre en sesión activa;
- No tener la sesión activa por más de dos horas.
- Para cerrar sesión de manera correcta utilizar la opción "Cerrar Sesión" de la barra de menú.

Leyenda de Privacidad

La Leyenda de Privacidad se debe poner a disposición del particular previo a la obtención de sus datos personales, ya que es el medio por el que se le informa del tratamiento que recibirá su información

Una vez que se ha identificado el Sistema de Datos Personales y éste se ha inscrito ante el InfoDF en el RESDP, el Ente Público se encuentra –teóricamente– facultado para recolectar los datos personales, sin embargo, previa a su obtención debe poner a disposición del particular una leyenda, por medio de la cual, se informa al titular de los datos personales sobre tratamiento que recibirán sus datos.

El modelo de leyenda de privacidad, lo localizamos en el numeral 13 de los Lineamientos para la Protección de Datos Personales del Distrito Federal, que se encuentra, en concordancia con el artículo 9 de la LPDPDF. Dicho formato es:

> ***Los datos marcados con un asterisco (*) son obligatorios y sin ellos no podrá acceder al servicio o completar el trámite*** (indicar el servicio o trámite de que se trate)
>
> ***Asimismo, se le informa que sus datos no podrán ser difundidos sin su consentimiento expreso, salvo las excepciones previstas en la Ley.***
>
> ***El responsable del Sistema de datos personales es (nombre del responsable), y la dirección donde podrá ejercer los derechos de acceso, rectificación, cancelación y oposición, así como la revocación del consentimiento es*** (indicar el domicilio de la Oficina de Información Pública correspondiente).
>
> ***El interesado podrá dirigirse al Instituto de Acceso***

a la Información Pública del Distrito Federal, donde recibirá asesoría sobre los derechos que tutela la Ley de Protección de Datos Personales para el Distrito Federal al teléfono: 5636-4636; correo electrónico: datos.personales@infodf.org.mx o www.infodf.org.mx" Excepciones al deber de información.

La información incluida en la Leyenda de Privacidad debe coincidir con la inscrita en el RESDP, así como estar actualizada

Es de señalar que no se recomienda alterar la estructura de ésta leyenda y que sólo deben completarse los campos con la información necesaria, la cual debe corresponder con lo señalado en el RESDP para cada uno de los sistemas de datos personales.

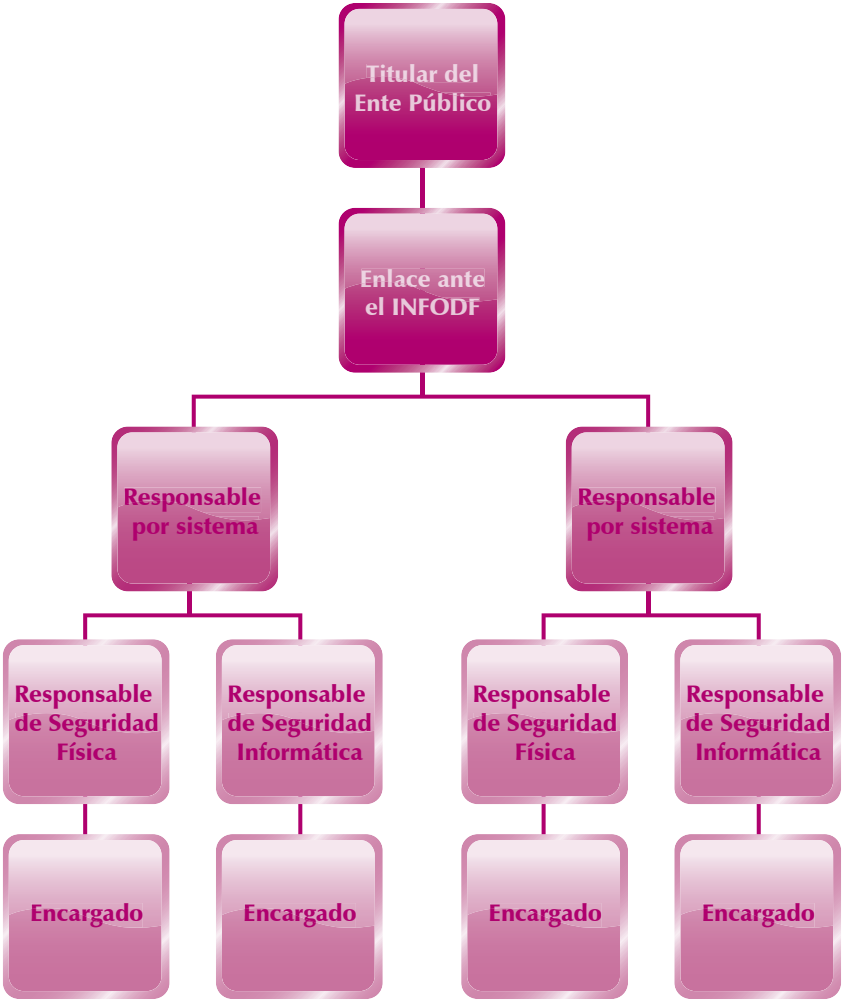
Ahora bien, se recomienda incorporar esta leyenda en los formatos con los se recaban los datos personales. Sin embargo, si esto no es posible, podrán tener carteles o posters o algún otro medio, que sea accesible al titular, previo a su recolección.

Personas que Intervienen en el Tratamiento de los Datos Personales

Es importante tener en consideración que existen diversos perfiles de funcionarios públicos involucrados en el tratamiento de los datos personales. De acuerdo a lo establecido en la Ley y en los Lineamientos, al interior del Ente, podemos identificar al titular del Ente Público, al *Enlace* en materia de datos personales, al *Responsable* del SDP, a los responsable(s) de seguridad, los *encargados*, así como al titular de la *Oficina de Información Pública* (OIP). De manera externa al Ente Público, es posible identificar a los usuarios y a los destinatarios.

En los apartados posteriores se desarrollará con mayor detalle cuáles son las tareas que habrá de desempeñar cada uno de éstos servidores públicos para contribuir al cumplimiento de la Ley de Protección de Datos Personales para el Distrito Federal.

Figura 3. Estructura de servidores públicos involucrados en el cumplimiento de la LPDPDF.



Fuente: Dirección de Datos Personales, InfoDF.

Recapitulando

El derecho a la protección de datos personales es un derecho autónomo al de acceso a la información pública. Si bien el primero constituye un límite al acceso a la información pública, su autonomía en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos.

El derecho a la protección de datos personales otorga a los individuos el poder de control sobre la información que les concierne, por ello establece que los titulares podrán acceder, rectificar, cancelar o bien oponerse al tratamiento de sus datos personales.

Los datos personales son aquella información que le concierne a una persona física identificada e identificable, es decir, que nos permite identificar a una persona.

De acuerdo a la LPDPDF, los datos se agrupan en sistemas de datos personales (SDP); por lo que todo dato utilizado por un Ente Público debe formar parte de un SDP.

Los SDP se pueden definir como todo conjunto organizado de archivos, registros, ficheros, bases o banco de datos personales de los Entes Públicos, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso.

Todos los SDP deben estar registrados ante el InfoDF en el Registro Electrónico de Sistemas de Datos Personales (RESDP), para mayor detalle del cumplimiento de esta obligación consúltese el Acuerdo del InfoDF 0469/SO/02-05/2012, disponible en:
http://www.infodf.org.mx/iaipdf/doctos/pdf/acuerdos/2012/acuerdo0469so020512.pdf

Para el adecuado cumplimiento de la Ley de Protección de Datos Personales para el Distrito Federal se requiere de la colaboración y trabajo en equipo del titular del Ente Público, Enlace en materia de datos personales, los responsables el SDP, los Encargados y los Usuarios.

Apartado II

Enlace en Materia de Datos Personales

Enlace en Materia de Protección de Datos Personales

El Enlace es el servidor público que fungirá como vínculo entre el Ente Público y el InfoDF.

Una de las figuras administrativas creadas a raíz de los Lineamientos para la Protección de Datos Personales del Distrito Federal, que juega un papel fundamental en la coordinación de la vida interna del Ente Público en materia de protección de datos personales y, sobre todo, en comunicación con el Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, es sin duda alguna el *Enlace*.

Esta figura es definida por el numeral 3, fracción VIII de los citados Lineamientos, como:

> *Servidor público que fungirá como vínculo entre el Ente Público y el Instituto para atender los asuntos relativos a la Ley de la materia.*

Esta definición se tiene que ver a la luz del numeral 35, cuarto párrafo, que señala lo siguiente:

> *El servidor público designado como Enlace también coordinará a los responsables de los sistemas de datos personales al interior del Ente Público*

La designación de éste servidor público corre a cargo del titular del Ente Público. De acuerdo a lo señalado en el numeral 38 de los Lineamientos para la protección de datos personales en el Distrito Federal, las principales funciones del Enlace son:

Cuadro 7. Funciones del Enlace.

Funciones al interior del Ente Público	Funciones al exterior del Ente Público
a) Coordinar a los responsables de sistemas de datos personales al interior del Ente Público para el cumplimiento de las disposiciones de la materia.	Fungir como Enlace entre el Ente Público y el Instituto de Acceso a la Información y Protección de Datos Personales del Distrito Federal.

Funciones al interior del Ente Público	Funciones al exterior del Ente Público
b) Supervisar que los responsables mantengan actualizada la inscripción de los sistemas bajo su responsabilidad en el RESDP.	Remitir el informe a que hace referencia la fracción III del artículo 21 de la Ley.
c) Coordinar las acciones en materia de capacitación.	
d) Recopilar la información para remitir al InfoDF la información a que alude el artículo 21, fracción III, de la LPDPDF y el numeral 37 de los Lineamientos.	

Fuente: Dirección de Datos Personales, InfoDF.

a) Coordinación de responsables.

Una de las funciones más importantes del *Enlace* en materia de datos personales es la de coordinar el trabajo interior del Ente Público, para garantizar que los responsables de sistemas de datos personales cumplan con las obligaciones establecidas en la Ley. Por este motivo, es imprescindible que el *Enlace* sea nombrado por el titular del Ente Público y que cuente con su respaldo.

Debe notificarse al InfoDF el nombramiento del Enlace de manera independiente al nombramiento del titular de la Oficina de Información Pública.

Un error que se comete frecuentemente consiste en considerar que el titular de la *Oficina de Información Pública* es por definición el *Enlace* en materia de datos personales, por lo cual es común observar que los Entes Públicos sólo reportan al InfoDF el nombramiento del titular de la OIP. Al respecto, debe decirse que la designación del *Enlace* es independiente, pues éste deberá coordinar los trabajos para garantizar el cumplimiento de la Ley de Protección de Datos Personales para el Distrito Federal, y sus funciones van más allá de realizar gestiones para la atención de las solicitudes de acceso, rectificación, cancelación y oposición de datos personales.

Es importante señalar que la función de capacitación en materia de protección de datos personales que tiene

el *Enlace*, debe ser realizada en coordinación con las unidades o áreas de capacitación del Ente Público, así como con las Direcciones de Capacitación y de Datos Personales del Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, y debe estar encaminada a la socialización del tema entre los servidores públicos, así como de las funciones que desempeñan como encargados o responsables de los SDP's.

b) Mantener actualizada la información del RESDP

Otra de las funciones vitales que tiene a cargo el *Enlace* en materia de protección de datos personales, es la de coordinar a los Responsables de los sistemas de datos personales para que mantengan la información actualizada en el (RESDP) Registro Electrónico de Sistemas de Datos Personales.

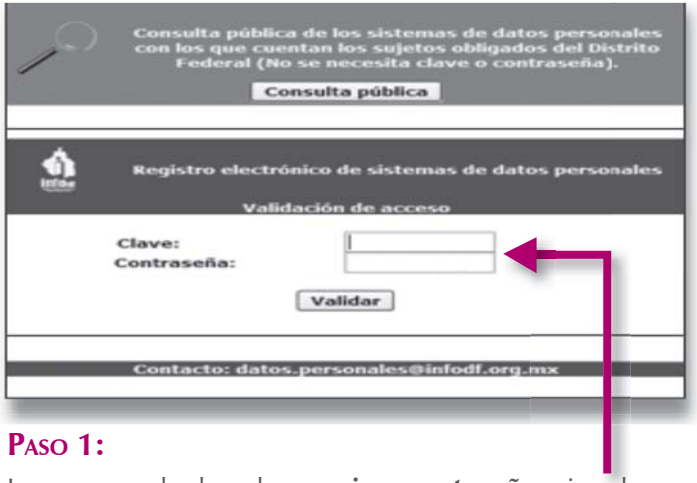
Para asegurar un mejor cumplimiento de esta función, el *Enlace* funge como *"Administrador de Ente"*, con las siguientes obligaciones:

- Dar de alta a las Unidades Administrativas del Ente.
- Asignar, modificar y revocar privilegios a los Responsables.
- Otorgar a los responsables de los SDP's las claves de usuario y contraseñas para ingresar al RESDP y mantener la información actualizada.
- Monitorear y supervisar el estatus de los SDP's inscritos en el RESDP.
- Capacitar a los responsables de los SDP's sobre el uso y operación del RESDP, de manera que sean capaces de mantener actualizada la información.

Para realizar estas acciones es necesario que el *Enlace* cuente con una clave de usuario y contraseña vigentes. Por ello, es necesario informar mediante oficio al InfoDF, la designación del *Enlace* y que éste acuda a la Dirección de Datos Personales del Instituto, a fin de

que ésta le asigne las claves de usuario y contraseña correspondientes.

Para dar de alta una unidad administrativa que cuenta con un SDP, el *Enlace* debe seguir los siguientes pasos:



Paso 1:

Ingresar con la clave de ***usuario y contraseña*** asignadas al *Enlace* por la Dirección de Datos Personales del Instituto.

Paso 2:

1. Dar clic en la opción Catálogo de Áreas de la barra de menús;

2. Registrar el nombre de la unidad administrativa que detecta el sistema, en la barra denominada Nombre Área;

3. Marcar la casilla de Activación;

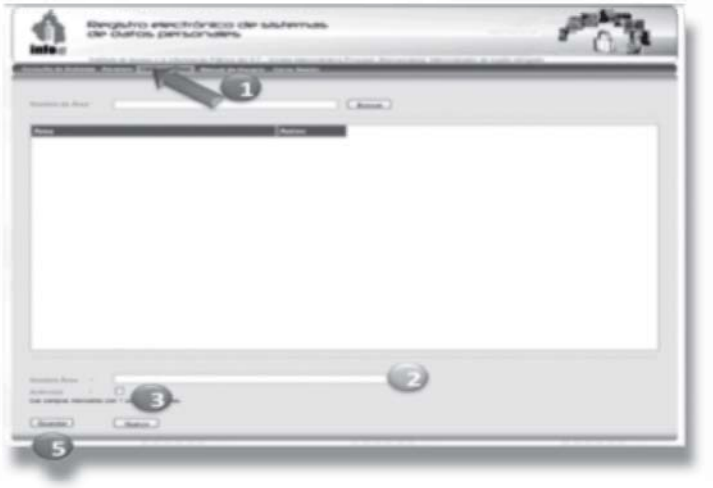
Ahora bien, para otorgar los privilegios a los Responsables dentro del RESDP, el *Enlace* debe seguir los siguientes pasos:

Paso Único:

1. Dar clic en la opción Permisos de Áreas de la barra de menús;
2. Seleccionar de la lista la unidad administrativa;
3. Escribir el nombre del responsable
4. Asigna la clave y contraseña que servirán como datos de identificación
5. Marcar la casilla de Activación
6. Dar clic en el botón Guardar.

Repetir el procedimiento por cada alta de responsable dando clic al botón Nuevo.

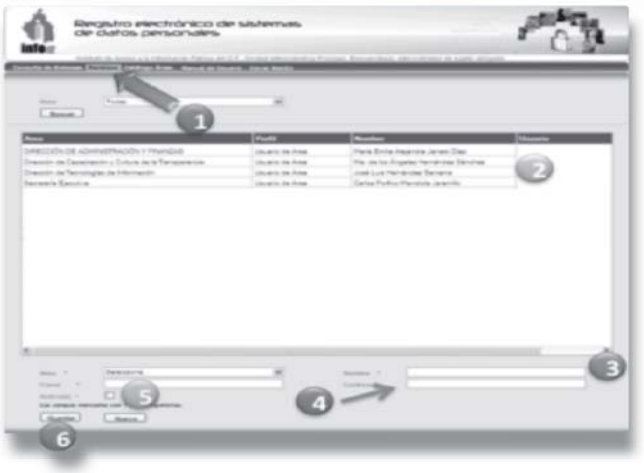
Si un Responsable dejó de laborar en la institución, es importante revocar los derechos que éste tenía, con el objeto de evitar que pueda modificar la información inscrita en el RESDP sin contar con las atribuciones legales. Para revocar los privilegios del Responsable del SDP, el *Enlace* tendrá que seguir los siguientes pasos:



Paso Único:

1. Dar clic en la opción Permisos de Áreas de la barra de menús;
2. Seleccionar de la lista la unidad administrativa;
3. Quitar la marca de la casilla de Activación.
4. Dar clic en el botón Guardar.

Si lo que se desea es modificar los permisos asignados previamente, se tendrá que seguir el siguiente paso:



Paso Único:

1. Ingresar a la opción Permisos de Áreas de la barra de menús;
2. Seleccionar de la lista la unidad administrativa;
3. Inscribir el nombre del nuevo Responsable del sistema
4. Asignarle una nueva clave y contraseña
5. Marcar de casilla de Activación
6. Dar clic en el botón Guardar

c) Tareas de capacitación

Además de tener presente que las acciones de capacitación deben realizarse con el área especializada en el tema dentro del Ente Público, se debe apoyar al responsable en la capacitación específica o focalizada a impartir en materia de los tipos y medidas de seguridad que se implementan en el SDP, y que se encuentran contempladas en el Documento de Seguridad.

En términos de lo establecido en el artículo 23 de la LPDFDF se deben considerar al menos dos tipos de cursos al interior de los Entes Públicos. Estos cursos deben estar dirigidos al personal encargado de dar atención a las solicitudes de acceso, rectificación, cancelación y oposición de datos personales, así como sobre la adopción de medidas de seguridad entre el personal que interviene

en el tratamiento de los datos personales. Para mayor referencia se cita el artículo 23 de la Ley.

> *Artículo 23 , El titular del ente público designará al responsable de los sistemas de datos personales, mismo que deberá:*
>
> *V. Adoptar los procedimientos adecuados para dar trámite a las solicitudes de informes, acceso, rectificación, cancelación y oposición de datos personales y, en su caso, para la cesión de los mismos;* ***debiendo capacitar a los servidores públicos encargados de su atención y seguimiento;*** ….
>
> *X. Elaborar un Plan de capacitación* ***en materia de seguridad de datos personales.***

Al impartir los cursos es importante conservar las listas de asistencia y tomar algunas fotografías, pues con estos documentos se podrá acreditar el cumplimiento de esta obligación ante el InfoDF.

Adicionalmente, se debe destacar que todos los años el InfoDF entrega reconocimientos a los Entes Públicos que cumplieron al 100% con las obligaciones que la LPDPDF establece. Al respecto se sugiere revisar la metodología para la entrega de reconocimientos a las mejores prácticas en materia de datos personales aprobada por el InfoDF, la cual está disponible en la página del Instituto (www.infodf.org.mx)

Los Entes Públicos tienen la obligación de capacitar los servidores públicos en temas de acceso a la información pública y protección de datos personales. La capacitación la brinda el InfoDF en dos modalidades: presencial y virtual. La primera es realizada, entre otros medios, a través de cursos sobre temas específicos impartidos en diversas sedes; la capacitación virtual se lleva a cabo por medio del Aula Virtual de Aprendizaje (AVA) y es un medio idóneo para que los servidores públicos se capaciten desde sus lugares de trabajo.

Con el objeto de atender a los servidores públicos de nuevo ingreso, el InfoDF tiene programados cursos con los temas "Introducción a la Ley de Transparencia y Acceso a la Información Pública del D.F.," "Introducción a la Ley de Datos Personales para el D.F."

La dirección electrónica del Aula Virtual de Aprendizaje es http://www.aula-infodf.org/aulavirtual/. Desde ella los servidores públicos pueden capacitarse en temas relacionados con la transparencia, rendición de cuentas y protección de datos personales.

La Dirección de Capacitación y Cultura de la Transparencia pone a su disposición el teléfono 5636-2120, con las extensiones 137, 159 y 103, para proporcionar mayores informes sobre ambas modalidades de capacitación.

Recapitulando

El *Enlace* es una de las piezas fundamentales dentro de la estructura organizacional en materia de protección de datos personales, puesto que funge como vínculo institucional entre el Ente con el InfoDF. Sobre el *Enlace* recae el rol de Administrador del Ente dentro del RESDP y la función fundamental de coordinar los esfuerzos emprendidos por dicho Ente Público en esa materia.

Asimismo, dentro del tratamiento, el *Enlace* debe proporcionar al Responsable la asesoría necesaria para el cumplimiento irrestricto de los principios contemplados en la Ley de Protección de Datos Personales para el Distrito Federal, y la adopción de todas las medidas y tipos de seguridad por parte de los Responsables.

El Responsable es el titular de la unidad administrativa que detenta los datos personales, los cuales deben estar organizados en Sistemas de Datos Personales. Este servidor público es quien debe responder por el cumplimiento de las obligaciones establecidas en la LPDPDF. El *Enlace* sólo coordina el trabajo de los responsables e integra los informes para su envío al InfoDF.

El *Enlace* debe brindar asesoría a los responsables para garantizar el cumplimiento de las disposiciones establecidas en la LPDPDF. En caso de incumplimiento a la LPDPDF, las infracciones son imputables al Responsable del SDP.

Check List: Enlace en Materia de Protección de Datos Personales

Si fuiste designado como *Enlace*, es importante tener en consideración la siguiente lista, la cual incluye una relación de aspectos básicos a considerar para verificar si el Ente Público para el cual trabajas ha cumplido con lo establecido en la LPDPDF.

PREGUNTAS	Sí	No
1. ¿El Titular del Ente llevó a cabo la designación del servidor público que fungirá como *Enlace* entre el ente obligado y el InfoDF, de manera expresa?		
2. ¿Dicha designación se realizó mediante oficio u otro instrumento normativo que conste por escrito?		
3. ¿Conserva copia del instrumento jurídico que me acredita como Enlace?		
4. ¿Se notificó al InfoDF mi designación como Enlace en materia de datos personales?		
5. ¿Cuenta con el acuse de recibo de la notificación de mi nombramiento como Enlace ante el InfoDF?		
6. ¿Cuenta con evidencia documental de la coordinación de los responsables de sistemas de datos personales, a la que se refiere el numeral 38, fracción I, de los Lineamientos para la Protección de Datos Personales en el Distrito Federal?		
7. ¿Si ha constatado que esté registrado en el RESDP el 100% de los sistemas de datos personales que detenta el Ente Público?		
8. ¿Los formatos que se utilizan para recabar datos personales en el Ente Público incluyen la leyenda a la que hace alusión el artículo 9 de la LPDPDF y el numeral 13 de los Lineamientos para la Protección de los Datos Personales en el Distrito Federal?		
9. ¿Se cuenta con evidencia documental que acredite las acciones para supervisar que la información de los sistemas en el Registro Electrónico de Sistemas de Datos Personales se encuentra actualizada?		
10. ¿Se conserva copia de los acuses de recibo de las modificaciones realizadas en el RESDP de los sistemas de datos personales de mi Ente Público?		
11. ¿Se han realizado las acciones de apoyo necesarias para actualizar los documentos de seguridad de los sistemas de datos personales que se encuentran registrados en el RESDP?		
12. ¿Se cuenta con evidencia documental que muestre las acciones de coordinación en materia de capacitación, implementadas o realizadas?		
13. ¿En el Ente Público se capacitó a los "encargados" involucrados en el tratamiento de los datos en materia de medidas de seguridad?		

PREGUNTAS	Sí	No
14. ¿Se impartió al menos un curso para garantizar que los enlaces de las unidades administrativas ante la OIP den atención a las solicitudes ARCO y cuenten con conocimientos básicos en materia de datos personales?		
15. ¿Se cuenta con evidencia de los cursos de capacitación impartidos al interior del Ente Público?		
16. ¿Se ha asistido a las reuniones de la Red de Protección de Datos Personales convocadas por la Dirección de Datos Personales del InfoDF?		
17. ¿Se cuenta con las constancias que acreditan que tomé la capacitación impartida por el InfoDF para garantizar un mejor desempeño de mis funciones?		
18. ¿Se remitió el informe a que hace referencia la fracción II del artículo 21 de la Ley de Protección de Datos Personales para el Distrito Federal antes del último día hábil de enero?		
19. ¿Se atendieron en tiempo y forma los requerimientos del InfoDF?		
20. ¿Los responsables de SDP cuentan con un nombramiento realizado por el titular del Ente Público para fungir como tal? O bien ¿El reglamento interior del Ente Público, o normatividad equivalente, establece que es obligación de los Directores fungir como Responsable de los sistemas de datos personales que detente el área a su cargo?		
21. ¿Se ha verificado que las publicaciones realizadas en la Gaceta en relación a lo establecido en el artículo 7 de la LPDPDF cumplan con las disposiciones aplicables?		

Apartado III

De los Responsables de los Sistemas de Datos Personales

Introducción

La *Ley de Protección de Datos Personales para el Distrito Federal* da origen en cierta manera, a una jerarquización en la que intervienen diversos servidores públicos que pueden dar tratamiento a los datos personales; recordando lo señalado en el Apartado I, estos puntos son los siguientes:

- ***Enlace:*** Servidor público que fungirá como vínculo entre el ente público y el Instituto para atender los asuntos relativos a la Ley de la materia;

- ***Responsable del Sistema de Datos Personales:*** Es la persona física que decide sobre la protección y tratamiento de datos personales, así como el contenido y finalidad de los mismos. Los Lineamientos establecen que este servidor público pertenece a la unidad administrativa a la que se encuentre adscrito el sistema de datos personales, designado por el titular del ente público, que decide sobre el tratamiento de datos personales.

- ***Responsable de seguridad:*** persona a la que el responsable del sistema de datos personales asigna formalmente la función de coordinar y controlar las medidas de seguridad aplicables, puede ser un solo responsable o bien puede haber varios responsables de seguridad, dependiendo de las necesidades del Ente Público.

- ***Encargado:*** Servidor público que en ejercicio de sus atribuciones, realiza tratamiento de datos personales de forma cotidiana;

En el presente apartado analizaremos una de las figuras más importantes, sobre la cual el recae gran peso de velar que el tratamiento de los datos personales se ajuste a los principios de licitud, consentimiento, calidad de los datos, confidencialidad, seguridad, disponibilidad y temporalidad establecidos en el artículo 5 de la LPDPDF.

Conceptos Clave

El Responsable de los SDP's, en términos de la *Ley de Protección de Datos Personales para el Distrito Federal*, es definido del artículo 3, como:

> *"Persona física que decida sobre la protección y tratamiento de datos personales, así como el contenido y finalidad de los mismos"*

Esa definición se ve complementada por el numeral 3, fracción XVI, de los *Lineamientos para la Protección de Datos Personales del Distrito Federal* (ahora en adelante lineamientos), que señala que el Responsables es:

El Responsable de los SDP´s es toda persona física que decida sobre la protección y tratamiento de los datos personales, así como el contenido y finalidad de los mismos.

> *"El servidor público de la unidad administrativa a la que se encuentre adscrito el sistema de datos personales, designado por el titular del Ente Público, que decide sobre el tratamiento de datos personales, así como el contenido y finalidad de los sistemas de datos personales"*

De esta definición podemos desprender varios elementos esenciales:

Primero. Responsable es un servidor público, cuya existencia nace de un nombramiento que lo faculta para el desempeño de sus funciones ordinarias.

Segundo. Para ser Responsable, es indispensable que la unidad administrativa a la que se encuentre adscrito ese servidor público cuente con uno o más SDP's.

Tercero. El Responsable tiene poder de decisión sobre lo que se debe recolectar, tratar y, por supuesto, definir la finalidad del tratamiento.

Es importante señalar que, de manera implícita en estas definiciones se encuentra la obligación del Responsable de velar por el cabal cumplimiento de los

principios contemplados en la citada Ley.

Ahora bien, para ostentar esa posición jerárquica dentro del ciclo vital de los Sistemas de Datos Personales, es necesario que concurran varios requisitos previos.

El primero de ellos, como ya se apuntaba anteriormente, es ostentar un cargo dentro del Ente Público.

El segundo elemento lo encontramos en el primer párrafo del artículo 21 de la LPDPDF, que señala una obligación a cargo del titular del Ente de que se trate, consiste en la designación de esa persona, es decir, que delegue en ese servidor público la responsabilidad de velar por el tratamiento. Esta delegación pudo haber sido realizada por disposición de una norma, o bien mediante escrito de delegación de atribuciones.

El tercer elemento, que tiene correlación con el punto anterior, se vincula a la existencia de un instrumento normativo que establezca una serie de disposiciones, cláusulas o apartados, que tengan como fin:

- Establecer la obligación de garantizar la seguridad y confidencialidad de los sistemas de datos personales de los que tendrá acceso.

- La prohibición de utilizar los datos personales con una finalidad distinta.

- Guardar secrecía aún después de haber terminado su encargo.

- Establecer las penas convencionales por el incumplimiento de los dos puntos anteriores, esto en forma independiente a las sanciones que correspondan en los términos de la Ley Federal de Responsabilidades de los Servidores Públicos.

Es importante señalar que estas cláusulas o disposiciones tienen como fin último garantizar que se cumplan los principios de confidencialidad y seguridad contemplados en la LPDPDF.

Desde la definición dada con anterioridad podemos desprender que el Responsable juega un papel muy importante dentro del Sistema de Datos Personales, por tal motivo, sus obligaciones se encuentran claramente establecidas en el artículo 21 de la Ley. A continuación transcribiremos esas obligaciones, y las correlacionaremos con los principios analizados previamente:

Cuadro 8. Principios alcanzados y funciones del Responsable.

Principio	Fracción del artículo 21 de la LPDPDF	Objetivo de la fracción
Licitud	**I**	Cumplir con las políticas y lineamientos así como las normas aplicables para el manejo, tratamiento, seguridad y protección de datos personales.
Consentimiento	**IV**	Informar al interesado al momento de recabar sus datos personales, sobre la existencia y finalidad de los sistemas de datos personales, así como el carácter obligatorio u optativo de proporcionarlos y las consecuencias de ello.
	VI	Utilizar los datos personales únicamente cuando éstos guarden relación con la finalidad para la cual se hayan obtenido.

Principio	Fracción del artículo 21 de la LPDPDF	Objetivo de la fracción
Calidad de los Datos Personales[8]	**VIII**	Actualizar los datos personales cuando haya lugar, debiendo corregir o completar de oficio aquellos que fueren inexactos o incompletos, a efecto de que coincidan con los datos presentes del interesado, siempre y cuando se cuente con el documento que avale la actualización de dichos datos. Lo anterior, sin perjuicio del derecho del interesado para solicitar la rectificación o cancelación de los datos personales que le conciernen;
Confidencialidad Seguridad y Disponibilidad	**II**	Adoptar las medidas de seguridad necesarias para la protección de datos personales y comunicarlas al Instituto para su registro, en los términos previstos en esta Ley.
	IX	Establecer los criterios específicos sobre el manejo, mantenimiento, seguridad y protección del sistema de datos personales.
	X	Elaborar un plan de capacitación en materia de seguridad de datos personales.

[8] Es importante señalar que, en términos del artículo 22 de la *Ley de Protección de Datos Personales para el Distrito Federal*, el titular del Ente Público es el que tiene la atribución de decidir sobre la finalidad del tratamiento.

Principio	Fracción del artículo 21 de la LPDPDF	Objetivo de la fracción
	XII	Establecer los criterios específicos sobre el manejo, mantenimiento, seguridad y protección del sistema de datos personales.
	XIV	Coordinar y supervisar la adopción de las medidas de seguridad a que se encuentren sometidos los sistemas de datos personales de acuerdo con la normativa vigente.
Disponibilidad	**VII**	Permitir en todo momento al interesado el ejercicio del derecho de acceso a sus datos personales, a solicitar la rectificación o cancelación, así como a oponerse al tratamiento de los mismos en los términos de esta Ley;
	XI	Resolver sobre el ejercicio de los derechos de acceso, rectificación, cancelación y oposición de los datos de las personas.
	XIII	Llevar a cabo o, en su caso, coordinar la ejecución material de las diferentes operaciones y procedimientos en que consista el tratamiento de datos y sistemas de datos de carácter personal a su cargo.

Principio	Fracción del artículo 21 de la LPDPDF	Objetivo de la fracción
Funciones administrativas	**III**[9]	Elaborar y presentar al Instituto un informe correspondiente sobre las obligaciones previstas en la presente Ley, a más tardar el último día hábil del mes de enero de cada año. La omisión de dicho informe será motivo de responsabilidad.
	XV	Dar cuenta de manera fundada y motivada a la autoridad competente de la aplicación de las excepciones al régimen general previsto para el acceso, rectificación, cancelación u oposición de datos personales.
	XVI	Las demás que se deriven de la presente Ley o demás ordenamientos jurídicos aplicables.

Fuente: Elaborado a partir de la propuesta de Davara (2010).

El Responsable de los SDP´s tiene la obligación de inscribir en el RESDP todos los SDP que se encuentren bajo su tutela

Antes de continuar, y siguiendo la lógica planteada por la Dra. Isabel Davara en la *Ley de Protección de Datos Personales para el Distrito Federal Comentada*, las obligaciones contempladas en el artículo 21 se pueden ver desde la óptica del beneficiario directo de esa obligación a cargo del Responsable del SDP's.

[9] Es de señalar que, está función se encuentra compartida con el Enlace por lo cual el Responsable envía el Enlace la información correspondiente para que el segundo la remita al Infodf.

Cuadro 9. Beneficiario de las obligaciones del responsable.

Beneficiario	Fracciones
Interesado	IV y VII
InfoDF	II, III y XV
Ente Público	I, V, VI,VIII, IX, X, XI, XII, XIII y XIV

Fuente: Elaborado a partir de la propuesta de Davara (2010).

Obligaciones Específicas

a) Deber de publicar en la GODF la creación, modificación o supresión de los SDP.

En la sección de Conceptos generales ya se analizó lo que es un sistema de datos personales.

Es de señalar que los sistemas de datos personales cuya existencia es previa a la promulgación de la *Ley de Protección de Datos Personales para el Distrito Federal*, quedan exentos de la obligación de publicar su creación en la *Gaceta Oficial del Distrito Federal*, en virtud de que ya estaban en posesión de los Entes Públicos; sin embargo, sí subsiste la obligación de inscribirlos en el Registro Electrónico de Sistemas de Datos Personales (RESDP), así como publicar por el mismo medio las modificaciones o supresión de esos sistemas.

Lo anterior, en los términos del numeral 6 de los *Lineamientos para la Protección de Datos Personales del Distrito Federal*. Ahora bien, el acuerdo de creación debe reunir ciertas formalidades fijadas en el numeral 7 del citado lineamiento, que señala:

> *"El acuerdo de creación de sistemas de datos personales deberá contener:*
>
> *I. La identificación del sistema de datos personales, indicando su denominación y normativa aplicable, así como la descripción de la finalidad y usos previstos;*

II. El origen de los datos, indicando el colectivo de personas sobre las que se pretende obtener datos de carácter personal, o que resulten obligados a suministrarlos; su procedencia (propio interesado, representante, Ente Público, etcétera) así como el procedimiento de obtención de los mismos (formulario, internet, transmisión electrónica, etcétera);

III. La estructura básica del sistema de datos personales mediante la descripción detallada de los datos identificativos que contiene y, en su caso, de los datos especialmente protegidos, así como las restantes categorías de datos de carácter personal, incluidas en el mismo y el modo de tratamiento utilizado en su organización (manual o automatizado). En su caso, señalar los datos de carácter obligatorio y facultativo;

La LPDPDF reconoce la existencia de varios tipos de SDP, los cuales pueden ser físicos, electrónicos o mixtos

IV. Las cesiones de datos que se tengan previstas, indicando, en su caso, los destinatarios o categorías de destinatarios;

V. La identificación de la unidad administrativa a la que corresponde el sistema de datos personales, así como del cargo del responsable;

VI. Domicilio oficial y dirección electrónica de la Oficina de Información Pública ante la cual se presentarán las solicitudes para ejercer los derechos de acceso, rectificación, cancelación y oposición, así como la revocación del consentimiento; e

VII. Indicación del nivel de seguridad que resulte aplicable: básico, medio o alto.

Todos los SDP´s que sean modificados, es decir, que alteren sustancialmente sus características, ya sea por mandato de Ley, o por decisión del Titular del Ente Público, requerirán de una publicación en la *Gaceta Oficial del Distrito Federal*. Para tal efecto, al igual que en el momento de creación, debe existir previamente un

acuerdo del titular, en el que se señale los elementos cambiados, entre los que pueden encontrarse los siguientes:

- La finalidad y/o los usos del sistema es distinta.
- La estructura del sistema: procedencia, tipo de datos, tratamiento de datos o los encargados del sistema.
- Cambió la unidad administrativa responsable del sistema, o el nombre de la unidad administrativa.
- La dirección de la Oficina de Información Pública es otra.
- El nivel de seguridad del sistema se incrementó o se redujo.

Una vez publicados los citados acuerdos, en los términos del numeral 10 de los Lineamientos para la Protección de Datos Personales del Distrito Federal, el Ente Público por conducto del Responsable del SDP, deberá dar de alta en el RESDP las modificaciones que haya sufrido. Para tal efecto, contarán con un término no mayor a 10 días hábiles, contados a partir de la publicación.

Es importante que al ingresar en la RESDP no se trabaje en el archivo en blanco que aparece al principio, pues de ser el caso se duplicaría el sistema en lugar de registrar las modificaciones. En caso de que por error se hubiese registrado un SDP de manera duplicada, debe procederse a la eliminación del segundo SDP y realizar los ajustes en el primer SDP registrado.

La supresión de un SDP también debe ser publicada en la *Gaceta Oficial del Distrito Federal*; esta figura de supresión o eliminación se activa cuando por mandato de ley se determine su baja, o por que las atribuciones que daban origen fueron transferidas a otro Ente. Bajo tal circunstancia, los Entes Públicos deben emitir los acuerdos correspondientes, así como publicarlos en la citada *Gaceta* y notificarlo al InfoDF.

En caso de supresión de los SDP los Entes Públicos tienen 30 días hábiles para hacer la supresión del sistema en el RESDP.

b) Deber de registrar los sistemas de datos personales ante el INFODF.

La última fracción del artículo 21 de la Ley nos da pie para señalar otras de las obligaciones que tiene el Responsable de los Sistemas de Datos Personales.

Una de ellas a cargo del Responsable de los SDP's, la localizamos en el artículo 8 de la LPDPDF, que impone el deber de inscribir en el Registro Electrónico de Sistemas de Datos Personales (RESDP)[10] todos los sistemas que se encuentren bajo su tutela. Esta obligación se encuentra íntimamente ligada con los principios de transparencia en el tratamiento de los datos y de consentimiento.

Es de señalar que, dicho registro[11] se encuentra conformado por los siguientes elementos:

I. Nombre y cargo del responsable y de los usuarios;
II. Finalidad del sistema;
III. Naturaleza de los datos personales contenidos en cada sistema;
IV. Forma de recolección y actualización de datos;
V. Destino de los datos y personas físicas o morales a las que pueden ser transmitidos;
VI. Modo de interrelacionar la información registrada;

[10] El RESDP es una aplicación tecnológica que permite conducir el esquema de inscripción y control de los sistemas de datos personales identificados por los Entes Públicos, y cuyo origen deriva del desarrollo de las atribuciones y obligaciones que por Ley les han sido asignadas.
Dicho sistema electrónico, se encuentra diseñado bajo "perfiles", en dónde el administrador es el InfoDF y el "Operario de Unidad Administrativa" es el Responsable del SDP`s; éste perfil es designado por el Enlace de Datos Personales.
[11] Para una mayor referencia del RESPD y los apartados que lo componen, se recomienda ver el Apartado II de éste documento.

VII. Tiempo de conservación de los datos, y
VIII. Medidas de seguridad[12].

Ahora bien, el numeral 10 de los *Lineamientos para la Protección de Datos Personales del Distrito Federal* señala que dicha obligación debe materializarse en un plazo no mayor de 10 días hábiles, contados a partir de la fecha de publicación de dicho Sistema en la *Gaceta Oficial del Distrito Federal*; una vez que se haya inscrito el sistema en el RESDP, Responsable deberá cerciorarse que se haya asignado el número de folio de identificación correspondiente.

Es importante señalar que no basta con el simple hecho de registrar el SDP's, sino que es indispensable que el Responsable mantenga actualizada la información ahí almacenada, a fin de asegurar que ésta es veraz, oportuna y confiable.

No es de omitir que el *Responsable* debe asegurarse que la información inscrita en el RESDP corresponda a los acuerdos de creación, modificación y/o supresión que, en su caso, se hubiesen publicado en la *Gaceta Oficial del Distrito Federal*, así como lo reportado en los diversos informes que tiene que rendir el Ente Público al InfoDF.

Por otra parte, en el RESDP se incluye un elemento adicional a los publicados en la Gaceta Oficial del Distrito Federal referente a los destinatarios. Los destinatarios son aquellos Entes Públicos a los que, en virtud de un mandato legal, tenemos que entregar datos personales que estén en nuestra posición.

Respecto a los destinatarios, debemos tener en consideración que, de acuerdo a nuestras atribuciones, estamos obligados a entregar información, al menos, a los Entes Públicos que se muestran en el cuadro:

---

[12] Las medidas de seguridad en términos de la Ley de Protección de Datos Personales para el Distrito Federal, se encuentran conformadas por "Tipos de seguridad" y "Niveles de Seguridad"

Cuadro 10. Relación de destinatarios de Entes Públicos.

DESTINATARIO	SUPUESTO DE TRANSFERENCIA DE DATOS	FUNDAMENTO LEGAL
COMISIÓN DE DERECHOS HUMANOS DEL DF	En investigación de presuntas violaciones a los derechos humanos.	Ley de la Comisión de Derechos Humanos del Df art. 3, 17 fracc. II y 36.
INFODF	Para la sustanciación del recurso de revisión.	Ley de Transparencia y Acceso a la Información Pública del DF arts. 16 fracc. Ii y v, 80 fracc. II y v; Ley de Protección de Datos Personales para el DF art. 39.
CONTADURÍA MAYOR DE HACIENDA	Para el ejercicio de sus funciones de fiscalización.	Ley Orgánica de la Contaduría Mayor de Hacienda de la Asamblea Legislativa del D.F. art. 2, 3, 6 y 8.
ÓRGANOS DE CONTROL	Para la realización de auditorías o desarrollo de investigaciones por presuntas faltas administrativas.	Ley Orgánica de la Administración Pública del DF arts. 34, fraccs. II y III y 74.
ÓRGANOS JURISICCIONALES	Para la sustanciación de los procesos jurisdiccionales tramitados ante ellos.	Arts. 323 Código Civil del DF; 278, 288, 326, 331, Código de Procedimientos Civiles del DF; art. 180 Código de Procedimientos Penales del df; arts. 131, 132, 147, 149 Ley de Amparo; art. 191 fracc. XIX Ley Orgánica del Poder Judicial de la Federación; art. 180 Código de Procedimientos Penales del DF; arts. 783 y 784 Ley Federal del Trabajo; art. 2, fracc. II Código Federal de Procedimientos Penales del DF.

Fuente: Dirección de Datos Personales, InfoDF.

En adición a los Entes Públicos señalados en el cuadro anterior, deben tenerse presentes otros que, dependiendo de la naturaleza del SDP, deberán incluirse. Por ejemplo, los partidos políticos deberán incluir a las autoridades electorales como destinatarios; aquellos que se relacionen con la administración de recursos humanos deberán incluir al SAT, etc.

Recomendaciones de Operación del RESDP

Por la importancia que tiene el Registro Electrónico de Sistemas de Datos Personales, daremos algunas instrucciones y recomendaciones que el Responsable debe tener en cuenta cuando registre información en el RESDP.

La primera, para ingresar debe tener previamente su usuario y contraseña, el cual, es asignado por el *Enlace* del Ente Público en materia de Protección de Datos Personales ante el InfoDF. En caso de no contar con usuario y contraseña contactar al *Enlace* para que éstos sean generados.

Si no se conoce quién es el *Enlace,* se puede enviar un correo electrónico para realizar la consulta a la cuenta datos.personales@nfodf.org.mx.

Una vez que ha ingresado en la plataforma, para modificar un SDP debe ingresar al área de consultas y seleccionarlo. En ese momento se habilitarán las siguientes opciones: "Detalles", "Editar", "Borrar" y "Acuse"; selecciona la opción "Editar" y modificar la información que sea necesaria. Una vez terminada esta primera parte, se debe seleccionar la opción "Guardar y Enviar", y a continuación elegir "Guardar Completo", una vez realizado esto, el RESPD le generará el "Acuse de Edición", el cual, debe ser guardado para cualquier efecto posterior.

El Responsable es quien debe mantener la información actualizada en el RESDP.

Es importante no capturar la información en la pantalla en blanco que aparece al inicio, pues en este caso se generará un registro duplicado del sistema, por lo tanto

debe tenerse cuidado en elegir la opción "Editar".

En caso de que se haya generado un sistema duplicado por un error de operación del SDP, es importante notificar por oficio esta situación al InfoDF, para que se tomen las acciones correctivas correspondientes.

Para borrar un SDP, el responsable debe seguir los pasos anteriores, pero seleccionando la opción "Borrar". Automáticamente el RESPD arrojará una ventana en donde se dará la opción de continuar o cancelar la operación, al dar clic en continuar, automáticamente el registro será eliminado.

c) Deber de informar.

Otra de las obligaciones que tiene el Responsable de los SDP's la localizamos en el tercer párrafo del artículo 9 de la multicitada Ley:

"Artículo 9.- …

…
En caso de que los datos de carácter personal no hayan sido obtenidos del interesado, éste deberá ser informado de manera expresa, precisa e inequívoca, por el responsable del sistema de datos personales, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad de lo previsto en las fracciones I, IV y V del presente artículo…"

Recuerda, en el caso de que los datos personales no hayan sido obtenidos directamente de su titular, éste deberá ser informado de manera expresa, precisa e inequívoca de la existencia del SDP.

Esta obligación se encuentra íntimamente ligada con el "deber de información" que se encuentra implícito en el principio de consentimiento; este deber se actualiza en forma previa a la recolección del dato personal del titular o representante legal, el cual implica, poner a disposición de éstos últimos la Leyenda de Privacidad; por lo que el párrafo tercero del artículo 9 de la LPDPDF "regulariza" el tratamiento. No olvidemos que el consentimiento expreso o tácito –según sea el caso– es

pieza fundamental para que se configure la licitud del sistema de datos personales de que se trate.

El citado párrafo contempla diversas excepciones a esta obligación de notificación, las cuales son:

1. Cuando una ley así lo estipule (es decir, que exente del deber de información).
2. Cuando los datos personales se hayan recolectado de una fuente pública.

d) Deber de adoptar medidas de seguridad para proteger los datos personales

Los responsables de SDP deben cumplir con el principio de seguridad, consistente en garantizar que sólo quien esté autorizado para ello tenga acceso a la información ahí tratada, es decir, busca garantizar la confidencialidad de los datos personales objeto de tratamiento.

El artículo 14, inciso A, fracción I de la Ley de Protección de Datos Personales para el Distrito Federal establece los tipos de seguridad de los sistemas de datos personales que se deben de observar:

Cuadro 11. Tipos de seguridad y alcances.

Tipo	Alcance	Ejemplo
Física	I. "Se refiere a toda medida orientada a la protección de instalaciones, equipos, soportes o sistemas de datos para la prevención de riesgos por caso fortuito o causas de fuerza mayor"	Control de acceso físico del personal autorizado; puertas de seguridad blindadas, candados, gavetas con cerradura de llaves, extinguidores, croquis de localización, cajas de ácido, fundas transparentes de polipropileno o poliéster, todo tipo de hardware de seguridad, dispositivos de radiofrecuencia (Near Field Communication), tarjeta inteligente, etc.
Lógica	II. "Se refiere a las medidas de protección que permiten la identificación y autentificación de las personas o usuarios autorizados para el tratamiento de los datos personales de acuerdo con su función"	Bitácoras de acceso, sistemas de control por medio del uso y portación de credenciales de identificación con fotografía, control de acceso biométrico, reloj checador por medio de huella digital para acreditar la pertenencia o estancia en las instalaciones respectivas.
Desarrollo y aplicaciones	III. "Corresponde a las autorizaciones con las que deberá contar la creación o tratamiento de sistemas de datos personales, según su importancia, para garantizar el adecuado desarrollo y uso de los datos, previendo la participación de usuarios, la separación de entornos, la metodología a seguir, ciclos de vida y gestión,	La administración de cuentas de usuarios; acceso remoto (acceso desde una computadora a un recurso ubicado físicamente en otra computadora que se encuentra geográficamente en otro lugar, a través de una red local o externa, como Internet); la autenticidad de documentos por medio del uso de la firma digital;

Tipo	Alcance	Ejemplo
	así como las consideraciones especiales respecto de aplicaciones y pruebas"	el uso del Certificado Digital (declaración firmada de manera digital que enlaza el valor de una clave pública con la identidad de una persona, un dispositivo o un servicio que posee la clave privada correspondiente); sistemas de detección de intrusos; sistema de protección de correo electrónico; antivirus, etc.
Cifrado	IV. "Consiste en la implementación de algoritmos, claves, contraseñas, así como dispositivos concretos de protección que garanticen la integralidad y confidencialidad de la información"	Cifrado simétrico: (crear una misma clave para cifrar y descifrar mensajes) Claves y contraseñas de acceso al RESDP, INFOMEX, SICRESI, correo electrónico oficial, etc. Cifrado asimétrico (cuando ambas claves son distintas).
Comunicaciones y redes	Se refiere a las restricciones preventivas y/o de riesgos que deberán observar los usuarios de datos o sistemas de datos personales para acceder a dominios o cargar programas autorizados, así como para el manejo de telecomunicaciones.	Firewall (software), sistemas de detección de intrusos, sistemas de protección de correo electrónico, control de acceso de derechos, etc.

Fuente: Dirección de Datos Personales, InfoDF.

Los tipos de seguridad se encuentran dirigidos tanto a los SDP cuyo soporte es físico y/o electrónico; los cuales son aplicables a los niveles de seguridad, que se encuentran

señalados en el inciso B del mismo artículo, que a saber son:

La LPDPDF contempla diversos tipos de seguridad que se deben implementar en los SDP. Esos tipos de seguridad son aplicados a los niveles de seguridad: Nivel Básico, Medio y Alto

- Nivel básico
- Nivel medio
- Nivel alto

Es de señalar que estos niveles de seguridad son acumulativos, es decir, la aplicación del nivel alto, abarca al nivel medio y básico, los que serán aplicado dependiendo del tipo de dato personal objeto de tratamiento.

Cuadro 12. Niveles y medidas de seguridad.

Nivel	Tipo de dato	Aspectos que comprende esa medida de seguridad, esto en los términos del inciso B, del artículo 14 de la Ley		
		Nivel Básico	Nivel Medio	Nivel Alto
Básico	Todos los datos personales.	• Documento de seguridad; • Funciones y obligaciones del personal que intevenga en el tratamiento de los sistemas de datos personales; • Registro de incidencias; • Identificación y autentificación; • Control de acceso; • Gestión de soportes, • Copias de respaldo y recuperación.		

Nivel	Tipo de dato	Aspectos que comprende esa medida de seguridad, esto en los términos del inciso B, del artículo 14 de la Ley		
		Nivel Básico	Nivel Medio	Nivel Alto
Medio	La relativa a Infracciones administrativas o penales. Datos personales de tipo hacendario. Datos personales patrimoniales. Datos personales financieros. Aquella información que a través de ella se pueda obtener una evaluación de la personalidad.			• Resposable de seguridad. • Auditoría. • Control de acceso físico. • Prueba de datos reales.
Alto	Toda aquella información relacionada a los datos sensibles, tales como: • Ideología. • Religión. • Creencias. • Afiliación política. • Origen racial o étnico. • Vida sexual. Dentro de este nivel, también se deberán incluir todos aquellos datos recabados con fines:			• Distribución de soportes. • Registro de acceso. • Telecomunicaciones.

Nivel	Tipo de dato	Aspectos que comprende esa medida de seguridad, esto en los términos del inciso B, del artículo 14 de la Ley		
		Nivel Básico	Nivel Medio	Nivel Alto
	• Policiales. • Seguridad. • Prevención del delito. • Investigación del delito. • Persecución del delito.			

Fuente: Dirección de Datos Personales, InfoDF.

La Ley de Protección de Datos Personales para el Distrito Federal señala que estos niveles de seguridad son los mínimos exigibles, por lo que abre la posibilidad de que el Ente Público, dependiendo su naturaleza, opte por la adopción de niveles aún mayores, para garantizar el cumplimiento de los principios contemplados en ella. Es de enfatizar, que los sistemas de datos personales no se encuentran aislados y tienen una interacción con otra información que sea administrada, generadá, se encuentre en posesión del Ente Público, por lo que, si esa información tiene un mayores estándares de seguridad, al sistema de datos personales con el que tiene interacción, también debería complementarse con esos estándares.

Sin embargo, la adopción de un nivel mayor de seguridad en los sistemas de datos personales dependerá exclusivamente del Ente Público, en específico del responsable, quien es el que decide sobre el contenido, finalidad y, por ende, los niveles de seguridad aplicables al sistema que se encuentre bajo su tutela y resguardo.

e) Deber de elaborar el Documento de Seguridad.

La siguiente obligación la localizamos en el inciso B, fracción I, del artículo 14 de la LPDPDF, la cual, a pesar que se encuentra inmersa dentro de las obligaciones

señaladas en el cuadro anterior, es importante realizar una referencia expresa a ella. Dicha fracción impone la obligación al Responsable del Sistema de Datos Personales de elaborar y mantener actualizado el Documento de Seguridad.

El Responsable de los SDP´s es el encargado de elaborar el Documento de Seguridad.

Ese instrumento es considerado como pieza fundamental dentro del Derecho de Protección de Datos Personales, ya que –en términos del numeral 16, fracción I, inciso a)– por medio de él, se difundirá –entre los encargados y usuarios– e implementarán las políticas, tipos y medidas de seguridad que se deben observar durante el tratamiento de los datos personales, que se encuentran amparados en el Sistema de Datos Personales al que les es aplicable.

El Documento de Seguridad[13] debe cumplir con todos y cada uno de los requisitos señalados en el numeral 16 de los *Lineamientos para la Protección de Datos Personales del Distrito Federal*, los cuales, se traducen en sus apartados:

> *"I. Nombre del sistema;*
>
> *II. Cargo y adscripción del responsable;*
>
> *III. Ámbito de aplicación;*
>
> *IV. Estructura y descripción del sistema de datos personales;*
> *V. Especificación detallada de la categoría de da-*

[13] La actualización del Documento de Seguridad debe ser al menos cada año, o cuando sufra una modificación el Sistema de Datos.
Aquí algunas recomendación para realizar las modificaciones:

1. Modificar las fojas que resulten ser necesarias para el registro de la afectación correspondiente a cualquier parte del Documento de Seguridad;
2. Incluir en un Anexo al documento de seguridad, las versiones anteriores de las secciones del documento de seguridad que fueron actualizadas;
3. Los Responsables deberán inscribir dichas modificaciones en el Registro Electrónico de Sistemas de Datos Personales (Para ver cómo se modifica la información del Registro electrónico véase la sección de preguntas sobre éste tema).
4. Los Responsables deberán notificar dichas modificaciones al INFODF (las medidas de seguridad son confidenciales, por lo que no se envía copia del documento, sólo se informa sobre la fecha de la última actualización).

tos personales contenidos en el sistema;

VI. Funciones y obligaciones del personal que intervenga en el tratamiento de los sistemas de datos personales;

VII. Medidas, normas, procedimientos y criterios enfocados a garantizar el nivel de seguridad exigido por el artículo 14 de la Ley y los presentes Lineamientos;

El Responsable de los SDP´s desde el nivel medio de seguridad, debe designar a uno o más responsables de seguridad, quienes son los encargados de coordinar y controlar las medidas de seguridad adoptadas.

VIII. Procedimientos de notificación, gestión y respuesta ante incidencias;

IX. Procedimientos para la realización de copias de respaldo y recuperación de los datos, para los sistemas de datos personales automatizados; y

X. Procedimientos para la realización de auditorías, en su caso"

Dentro de ésta misma lógica, en la fracción II del inciso B del citado artículo (que habla del nivel medio de seguridad), encontramos otra obligación que tiene el Responsable del SDP, consistente en designar a uno o más responsables de seguridad, quienes tienen, en los términos del numeral 3, fracción XVII de los multicitados *Lineamientos*, la función de coordinar y controlar las medidas de seguridad contempladas en el Documento de Seguridad aplicable.

f) Deber de realizar auditorías a la implementación de las medidas de seguridad

Las auditorías tienen como propósito verificar el cumplimiento de la implementación de las disposiciones contenidas en el o los documentos de seguridad correspondientes, con el objetivo de proteger los datos personales contenidos en los SDP;

Como hemos observado en el cuadro 13, en el nivel medio se exige, entre otros elementos, que los sistemas de datos personales con ese nivel sean auditados. Esa auditoría tiene como propósito verificar el cumplimiento de la implementación de las disposiciones contenidas en el o los documentos de seguridad correspondientes, con el objetivo de proteger los datos personales contenidos en los sistemas de datos personales

que los Entes Públicos posean, así como revisar que el Documento de Seguridad haya sido elaborado conforme a lo establecido en la *Ley de Protección de Datos Personales para el Distrito Federal* y en los *Lineamientos para la Protección de Datos Personales*, ambas del Distrito Federal.

Ahora bien, dicha auditoría debe ser realizada por lo menos cada dos años, y puede ser efectuada por el órgano interno de control o por un auditor externo; en éste último escenario, debe existir todo tipo de cláusulas que se encuentren encaminadas a garantizar la confidencialidad de la información a la que tendrá acceso ese auditor.

g) Deber de firmar las respuestas a las solicitudes de acceso, rectificación, cancelación u oposición de datos personales.

Las auditorias deben ser realizadas, por lo menos, cada dos años.

No obstante de que en los siguientes apartados se aborde el tema de los procedimientos contemplados en la Ley de Protección de Datos Personales para el Distrito Federal y que esta obligación se encuentra contemplada en las fracciones V, VII, VIII, y XV, del artículo 21 de la citada ley, es importante señalar que el artículo 32, último párrafo, impone una obligación importante al *Responsable* de los SDP`s, que consiste en levantar un acta circunstanciada, cuando a raíz de una solicitud ARCO no se localiza la información requerida por el titular de los datos; esa "Acta Circunstanciada de no Localización", debe ser firmada no solamente por el Responsable, sino que debe estar acompañada por las firmas del responsable de la Oficina de Información Pública y el representante del Órgano Interno de Control del ente público.

En foprma adicional las respuestas a las solicitudes ARCO deberán estar firmadas por el servidor público registrado como responsable del SDP en el RESDP.

h) Otras obligaciones derivadas del tratamiento de los datos.

El artículo 18 de la LPDPDF se encuentra íntimamente relacionado con el principio de disponibilidad, e impone diversas obligaciones a los Responsables de los Sistemas de Datos Personales en materia de salud, las cuales son:

1. Para la recolección y tratamiento de los datos personales, se debe de observar lo dispuesto en Ley General de Salud, la Ley de Salud para el Distrito Federal y demás normas que de ellas deriven.
2. En el tratamiento y/o cesión, los datos personales identificativos deben ser mantenidos de manera separada de los de tipo de salud (un claro ejemplo de disociación de los datos personales); queda exento de lo anterior, según el citado artículo, cuando:

    a. El titular lo consienta expresamente.
    b. Se trate de investigaciones de salud o judiciales, y sea indispensable mantenerlos hilados.

Ahora bien, el artículo 19 de la LPDPDF establece diversas obligaciones a los Responsables del SDP's, que le ayudarán a dar cumplimiento a los principios de Calidad y Disponibilidad, al señalar el deber que tienen de suprimir (dar de baja) aquellos datos personales, o incluso el SDP, cuando estos hayan cumplido con la finalidad por la que se recabaron, y hubiere finalizado el plazo de conservación fijado por la norma aplicable. El segundo párrafo del artículo 19 impone otra obligación, que consiste en incorporar en el documento jurídico que da base a la transferencia, una cláusula o apartado, en el que se fije los plazos en que el usuario deberá conservar los datos personales y el de devolución, en su caso.

El artículo 20 de la citada Ley versa sobre las transferencias o cesiones nacionales o internacionales que se pueden realizar de los sistemas de datos personales, o incluso

de los datos personales; dicho artículo se encuentra vinculado con los principios de confidencialidad y seguridad, e impone diversas obligaciones:

Figura 4. Obligaciones en materia de cesiones o transferencias de datos.

Fuente: Santiesteban (2011-2).

Recapitulando

Los artículos de la *Ley de Protección de Datos Personales para el Distrito Federal* que contemplan algunas de las obligaciones de los Responsables de los Sistemas de Datos Personales, son:

Cuadro 14. Obligaciones del *Responsable*.

Artículo	Principio o deber
6 y 7	Deber de crear, modificar o suprimir los SDP mediante publicación en la GODF.
8	Deber de registrar los SDP.
9	Deber de información.
9 tercer párrafo	Deber de información en caso de contar con datos recabados por un tercero.
14, inciso B, fracción I	Principio de seguridad
14, inciso B, fracción II	Principio de seguridad
18	Disponibilidad
19	Calidad y de disponibilidad
20	Confidencialidad y de seguridad
21	Licitud, consentimiento, calidad, confidencialidad, seguridad y disponibilidad.
32 último párrafo	Disponibilidad

Fuente: Dirección de Datos Personales, InfoDF.

Check List: Responsable de los SDP

Si eres titular de una unidad administrativa que detenta datos personales, entonces eres Responsable en términos de la LPDPDF. Por ello, es necesario que tengas en consideración el siguiente check list, que tiene como propósito ayudarte a cumplir con tus obligaciones.

PREGUNTAS	Sí	No
EJERCICIO DE FACULTADES		
1. ¿El Titular del Ente llevó a cabo la designación del servidor público que fungirá como Responsable del SDP?		
2. ¿Dicha designación se realizó mediante oficio u otro instrumento normativo que consta por escrito?		
3. ¿Conservas copia del instrumento jurídico que te acredita como Responsable del SDP?		
4. En caso de no haber sido designado ¿existe disposición expresa en la normatividad (por ejemplo, en el manual de procedimientos, manual de organización, reglamento interior, etc)?		
CUMPLIMIENTO DEL DEBER DE PUBLICAR EN LA GACETA OFICIAL (ARTÍCULO 6 Y 7)		
5. ¿Has publicado en la *Gaceta Oficial del Distrito Federal* la creación de los SDP generados después del 3 de octubre de 2008?		
6. ¿Has publicado las modificaciones a los SDP en la *Gaceta Oficial del Distrito Federal*?		
7. Si el SDP del que eres Responsable ha cumplido su finalidad por el que fue creado y se ha decretado su baja ¿has publicado en la *Gaceta Oficial del Distrito Federal* su supresión?		
8. En caso de haber realizado supresión de SDP ¿éstas han sido publicadas en la *Gaceta Oficial del Distrito Federal*?		
9. En el caso de que se haya determinado la supresión de un SDP o de uno más datos personales, ¿cuentas con los procedimientos internos para garantizar la no recuperación de esa información?		
10. En caso de que se haya determinado la baja de un SDP físico o de uno o más datos personales ¿cuentas con la autorización del Comité Interno de Administración de Documentos (COTECIAD)?		
11. En el caso de que realices transferencias locales, nacionales o internacionales ¿cuentas con un procedimiento interno para verificar que el receptor cumpla con los niveles de seguridad aplicables?		
12. ¿Has notificado al InfoDF las publicaciones realizadas?		

PREGUNTAS	Sí	No
CUMPLIMIENTO DEL DEBER DE REGISTRAR (ARTÍCULO 8)		
13. ¿Tienes registrado en el RESDP los sistemas de datos personales que detentas?		
14. ¿Verificaste que la información estuviera actualizada?		
CUMPLIMIENTO DEL DEBER DE INFORMAR (ARTÍCULO 9)		
15. ¿Tienes plenamente identificados los medios y formatos a través de los cuales recabas datos personales?		
16. ¿Cuentas con el formato de leyenda establecido en el artículo 9 de la LPDPDF para informar a los interesados al momento de recabar sus datos?		
17. ¿La leyenda reúne todos los requisitos señalados por la LPDPDF y el numeral 13 de los *Lineamientos para la Protección de Datos Personales del Distrito Federal*?		
18. ¿La información incluida en mi leyenda coincide con la registrada en el RESDP?		
19. ¿Cumplí con las recomendaciones emitidas por el INFODF en el acuerdo 0528/SO/16-05/2012?		
20. Si el sistema de datos personales es anterior a la entrada en vigencia de la LPDPDF ¿has notificado a los titulares de los datos personales la existencia de ese sistema y les has proporcionado copia de la leyenda?		
21. ¿Cuentas con la evidencia de lo anterior? (en relación a las preguntas 19 y 20)		
22. En caso de recabar datos mediante escritos libres ¿cuento con la leyenda establecida en el artículo 9?		
23. En caso de recabar datos mediante escritos libres ¿Tengo plenamente identificado el momento procesal en el que daré a conocer dicha leyenda al interesado?		
24. ¿Cuentas con la evidencia de lo anterior? (en relación a las preguntas 22 y 23)		
25. Los encargados ¿proporcionan al titular de los datos personales la leyenda de privacidad antes de recabar sus datos?		
26. Si recabas datos personales sensibles ¿cuentas con evidencia de haber recabado el consentimiento expreso del titular del dato?		

PREGUNTAS	Sí	No
MEDIDAS DE SEGURIDAD (ARTÍCULO 14)		
27. ¿Utilizas los datos personales exclusivamente para la finalidad por la que me fueron entregados?		
28. ¿Has realizado un inventario de todos los datos personales que conforman el SDP?		
29. ¿Cuentas con procedimientos para asegurar la calidad de los datos personales que se encuentran en el SDP?		
30. ¿Cuentas con el Documento de Seguridad?		
31. ¿Has adoptado medidas de seguridad para tu cargo?		
32. ¿Has adoptado el nivel o niveles de seguridad aplicable(s) al SDP?		
33. ¿Has implementado las bitácoras de acceso?		
34. En el documento de seguridad ¿has descrito las funciones y obligaciones que tienen los encargados?		
35. ¿Cuentas con un plan de capacitación en materia de seguridad de datos personales?		
36. ¿Cuentas con la evidencia de la impartición de esos cursos?		
37. ¿Has proporcionado a los encargados la parte que le corresponde del Documento de Seguridad?		
38. ¿Cuentas con procedimientos internos y que se encuentren reflejados en el Documento de Seguridad para autorizar la salida de documentos y su reincorporación?		
39. ¿Has implementado un procedimiento interno para la notificación de incidencias?		
40. ¿Has implementado un procedimiento interno para la recuperación de la información en caso de una incidencia?		
41. ¿Has implementado un procedimiento interno para la identificación y autenticación de los encargados y tuyo?		
42. ¿Cuentas con un procedimiento o política que de evidencia del cómo se debe realizar el tratamiento de los datos personales?		
43. ¿Realizas las copias de seguridad periódicas del SDP?		

PREGUNTAS	Sí	No
44. En el caso de que el SDP se le haya asignado el nivel medio de seguridad o alto ¿Has designado al o a los Responsables de Seguridad?		
45. En el caso de que el SDP se haya asignado el nivel medio de seguridad o alto ¿has incorporado dentro del Documento de Seguridad sus funciones y obligaciones?		
46. Dentro del Documento de Seguridad –en el caso de que se haya designado el nivel medio o alto de seguridad– ¿se ha incorporado un procedimiento para la realización de las pruebas con datos reales?		
47. ¿Has realizado las pruebas con datos reales que se hace mención en el punto anterior?		
48. ¿Cuentas con procedimiento o políticas dentro del Documento de Seguridad para la práctica de auditorías?		
49. Si te han practicado una auditoría en el SDP ¿has adoptado las recomendaciones emitidas por el auditor?		
50. Si cuentas con usuarios ¿han firmado un acuerdo de confidencialidad?		
51. Si cuentas con usuarios, dentro del documento por el que los has contratado ¿se establece la finalidad del tratamiento y el destino de la información una vez terminado el objeto de su contrato?		
52. ¿Cuentas con un procedimiento para verificar que efectivamente el usuario se está ajustando a los lineamientos fijados en su contrato?		
53. ¿Has inscrito en el Registro Electrónico de Sistemas de Datos Personales del InfoDF los SDP que se encuentran en tu posesión?		
54. ¿Has realizado las modificaciones pertinentes en el RESDP?		
ATENCIÓN A SOLICITUDES ARCO		
55. ¿Cuentas al interior de la Unidad de Administrativa en la que se encuentra el SDP y del que eres Responsable, con procedimiento para dar atención a las solicitudes ARCO?		
56. ¿Atiendes puntualmente los requerimientos realizados por el titular de la OIP?		

PREGUNTAS	Sí	No
INFORMES		
57. ¿Has rendido los informes a los que se hace referencia en la fracción III del artículo 21 de la LPDPDF, en los plazos requeridos por el Enlace en materia de datos personales?		
58. ¿Has entregado en tiempo y forma los informes pedidos por el Enlace en materia de datos personales?		

Apartado IV

De los Encargados y Usuarios

De los Encargados:

Otra de las figuras fundamentales dentro de la estructura de la protección de datos personales en el Distrito Federal, es sin duda alguna los encargados. El *Encargado* es definido por el numeral 3, fracción VII de los Lineamientos para la Protección de Datos Personales del Distrito Federal, como:

> *"Servidor público que en ejercicio de sus atribuciones, realiza tratamiento de datos personales de forma cotidiana"*

De esta definición podemos desprender dos elementos fundamentales, el primero de ellos es que para tener el estatus de encargado se requiere ser un servidor público adscrito a la unidad administrativa en la que se encuentra el SDP, y depende jerárquicamente del Responsable del SDP; el segundo elemento consiste que dentro de su perfile de puesto se encuentren establecidas con toda claridad las atribuciones específicas de las cuales se derivan las razones por las que el servidor público está facultado para dar tratamiento a los datos personales.

Es de señalar que esas funciones específicas sobre las acciones que pueden desempeñar los encargados dentro del SDP, deben estar claramente establecidas en el *Documento de Seguridad* que corresponda, en el cual, se debe establecer a qué partes del sistema, a qué datos y/o qué documentos tiene o tienen acceso autorizado.

Ahora bien, siguiendo la lógica planteada por los *Lineamientos para la Protección de Datos Personales del Distrito Federal*, podemos señalar que el encargado, tiene diversas obligaciones específicas que a saber son:

1. Bitácoras.- Registrar en los instrumentos que para tal efecto haya implementado el *Encargado* del SDP, en el que se deje asentadas las acciones emprendidas por los encargados.

2. Acceso y procesamiento.- Acceder exclusivamente a los datos personales a los que se encuentre autorizado para tal efecto.

3. Inventario.- Colaborar con el *Responsable* en la elaboración del inventario del SDP.

4. Incidencias: Reportar, en los términos y condiciones señaladas para tal efecto en el *Documento de Seguridad*, toda aquella anomalía que "… afecte o pudiera afectar la seguridad de los datos personales"[14]. Dicho reporte, debe contener por lo menos, en los términos del numeral 16, inciso c), de los Lineamientos para la Protección de Datos Personales del Distrito Federal:

    a. Tipo de incidencia
    b. Momento en que se ha producido
    c. Nombre la persona que realiza el reporte
    d. A quién se lo comunica
    e. Los efectos que se hubieran derivado de la misma
    f. Las acciones implementadas

5. Salida de documentos.- Gestionar ante el *Responsable* la salida de soportes y/o documentos que contengan datos personales, la cual, es recomendable que quede plasmada en una bitácora. Así mismo, dentro del traslado del soporte físico y/o electrónico, adoptar todas las medidas físicas necesarias, a fin de evitar su sustracción, pérdida o acceso no autorizado[15].

6. Auditorías: Permitir al auditor (interno o externo), la verificación de los SDP, así como permitir el acceso y dar facilidades e informes que le sean requeridos[16].

---

[14] Numeral 3, fracción X, de los Lineamientos para la Protección de Datos Personales del Distrito Federal.
[15] Numeral 9, inciso f), tercer párrafo, de los Lineamientos para la Protección de Datos Personales del Distrito Federal.
[16] Numeral 41, fracción II, de los Lineamientos para la Protección de Datos Personales del Distrito Federal.

7. Principios: Observar los principios de consentimiento (en el caso de que se encuentre en el área de recolección de datos personales), confidencialidad, seguridad y disponibilidad, así como, acatar los plazos y términos fijados por el *Responsable* para la conservación de los datos personales.

   Asimismo, es recomendable que al igual que el *Responsable* del SDP, el *Encargado* firme un acuerdo de confidencialidad.

8. Solicitudes ARCO y de Revocación del Consentimiento: colaborar con el *Responsable* y el *Titular de la Oficina de Información Pública* en la atención de las solicitudes ARCO y de Revocación del Consentimiento que se presenten y se encuentren relacionadas con el SDP.

9. Informes: Coadyuvar con el *Responsable*, si es el caso, en la elaboración de los informes a que se hace referencia en la fracción III, del artículo 21 de la *Ley de Protección de Datos Personales para el Distrito Federal*.

10. Documento de Seguridad y Capacitación: Participar en las acciones de capacitación emprendidas por el *Responsable* para la socialización del *Documento de Seguridad* y de las Medidas de Seguridad aplicables al SDP.

Como podemos observar, el encargado cuenta con diversas funciones fundamentales previo y dentro del proceso de tratamiento de los datos personales, las cuales, se ven complementadas con lo señalado por el Documento de Seguridad del SDP, el Manual de Organización y el Perfil de Puesto.

De los Usuarios:

El usuario es definido en el artículo 3 de la Ley de Protección de Datos Personales para el Distrito Federal como:

> *Aquel autorizado por el Ente Público para prestarle servicios para el tratamiento de datos personales*

Es decir, es aquella persona física o moral que presta sus servicios al ente público, siendo una de sus actividades tener contacto con los SDP's o dar tratamiento a nombre el ente.

Ahora bien, para ostentar tal carácter dentro de la lógica empleada por la Ley, presupone la existencia de un contrato, en el que se establezca a parte de objeto del mismo y demás clausulado necesario para su existencia jurídico administrativo, la inclusión de ciertas clausulas que regulen los siguientes temas:

a) Finalidad del tratamiento, es decir, las directrices bajo las que se deberá realizar.
b) Tipos de seguridad que el Ente Público por conducto del Responsable del SDP empleará para transmisión de los datos personales.
c) Cumplimiento de los tipos y niveles de seguridad que deberá observar durante el tratamiento.
d) Deber de confidencialidad.
e) Sanciones por el incumplimiento de los dos puntos anteriores.
f) Resultados esperados del tratamiento de los datos personales.
g) Devolución de los datos personales una vez terminado el objeto del contrato y el período de conservación fijados para tal efecto[17], así como los tipos de seguridad que se deben emplear para su transmisión. En el caso de que se hubiere pactado la destrucción de los datos personales,

[17] Artículo 19 de la Ley de Protección de Datos Personales para el Distrito Federal.

los mecanismos que debe observar el usuario para llevar a cabo dicho fin y las evidencias que deberá entregar al Responsable.
h) Acatar las actualizaciones que los titulares de los datos personales realicen a sus datos personales.
i) Acatar las resoluciones correspondiente a la Revocación del Consentimiento y de los Derechos ARCO.

Es de señalar que en caso de que existieran usuarios dentro del SDP, el Documento de Seguridad que corresponda, debe señalar:

a) Nombre del Usuario.
b) Domicilio (calle, número exterior e interior, colonia, código postal, Municipio o Delegación, Estado de la República).
c) Denominación del acto jurídico.
d) Finalidad permitida.
e) Vigencia del contrato.

También es recomendable que dentro del clausulado se estipule la obligación de permitir a las autoridades, tales como el Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, el Instituto Federal de Acceso a la Información y Protección de Datos[18], las Contralorías Internas y a las autoridades jurisdiccionales, el acceso a los SDP's objeto del contrato, así como rendir los informes que se le requieran.

Es de notar que los usuarios son sujetos obligados de la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, por lo que en forma independiente a lo señalado en el presente apartado, ellos deben de observar todos y cada uno de los principios y disposiciones que contempla dicha Ley, en el supuesto del ejercicio de los Derechos ARCO y de

[18] No debemos de olvidar que en el mundo del sector privado existe la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, y cuyo órgano garante es el Instituto Federal de Acceso a la Información y Protección de Datos.

Revocación del Consentimiento, los usuarios en el caso de que dichos requerimientos llegasen al Ente Público, deberán sujetarse en su caso, a lo establecido en la *Ley de Protección de Datos Personales para el Distrito Federal*.

Check List: Encargado de los SDP

Si en el ejercicio de tus funciones tratas datos personales de manera cotidiana, entonces eres encargado de un SDP. Por este motivo, es necesario que tengas en consideración el siguiente check list, que tiene como propósito ayudarte a cumplir con las obligaciones que la Ley de Protección de Datos Personales para el Distrito Federal (LPDPDF) establece y evites cometer alguna infracción a esta Ley que pueda traducirse en sanciones.

PREGUNTAS	Sí	No
1. ¿Cuentas con facultades para tratar datos personales? (en caso de respuesta afirmativa saltar a la pregunta 4)		
2. En caso de no contar con facultades ¿cuentas con una designación realizada por el titular de la unidad administrativa en la que te designa como encargado?		
3. ¿Dicha designación se realizó mediante oficio u otro instrumento normativo que consta por escrito?		
4. ¿Has participado en las acciones de capacitación que ha emprendido el Responsable del SDP en materia los tipos y niveles de seguridad aplicables?		
5. ¿Cuándo recabas los datos personales pones a disposición del titular la leyenda de privacidad a la que alude el artículo 9 de la LPDPDF?		
6. Si el titular de los datos personales tiene dudas sobre el alcance de la leyenda de privacidad ¿le explicas su contenido?		
7. Si el titular de los datos personales se reúsa proporcionar sus datos personales ¿le has comentado las consecuencias de no hacerlo?		
8. Si recabas datos personales sensibles ¿has solicitado el consentimiento expreso del titular de esa información?		

PREGUNTAS	Sí	No
9. ¿Cuándo realizas la consulta de un expediente que contiene datos personales, inscribes dicha consulta en la bitácora implementada por el Responsable del SDP?		
10. ¿Dentro del Documento de Seguridad se señalan tus funciones y obligaciones?		
11. ¿Dentro del Documento de Seguridad se señala a qué datos personales puedo dar tratamiento?		
12. ¿Dentro de tu perfil de puestos o manual de organización o instrumento equivalente se señalan tus funciones y obligaciones dentro del SDP?		
13. ¿Has realizado el inventario de los datos personales a los que les puedes dar tratamiento?		
14. ¿Conoces el procedimiento implementado por el Responsable del SDP para reportar una incidencia que ponga en riesgo los datos personales?		
15. En el caso de que tengas que trasladar un expediente o documento que contenga datos personales fuera de las instalaciones del Ente Público ¿has solicitado la autorización del Responsable del SDP?		
16. Bajo la misma lógica del punto anterior ¿Has registrado esa salida en el instrumento que para tal efecto haya implementado el Responsable del SDP?		
17. ¿Has implementado los tipos de seguridad a fin de garantizar el acceso no autorizado a ese documento?		
18. En el caso de que tengas que dejar el expediente o documento a un tercero ajeno al SDP, ¿te aseguras de entregarlo a la persona a la que se encuentra dirigida?		
19. En el caso de que haya terminado la vigencia documental del expediente o del dato personal y el Responsable del SDP te ha dado la instrucción de darlo de baja, te ¿has asegurado de que esa información no se pueda recuperar?		
20. ¿Has firmado un documento o convenio de confidencialidad?		
21. ¿Archivas los expedientes que contienen datos personales de tal forma en que se responda a las políticas internas del ente en materia archivística?		

PREGUNTAS	Sí	No
22. ¿Al término de utilizar el expediente o datos personales, te aseguras de no dejarlo a simple vista de las demás personas?		
23. En el caso de que los datos personales se encuentren en una computadora, al levantarte de tu lugar ¿te aseguras de bloquear el acceso a la misma?		
24. En el caso de que los datos personales se encuentren en una computadora, te aseguras que los antivirus y firewall se encuentren actualizados		
25. ¿Has realizado o has solicitado al área competente la realización de los respaldos de los datos personales a los que tengas acceso, en los términos fijados en el Documento de Seguridad?		
26. ¿Has sido capacitado en materia de atención de las solicitudes ARCO y de Revocación del Consentimiento?		
27. ¿Te abstienes de comentar con colegas sobre la información confidencial a la que tienes acceso?		

Check List: Usuario de los SDP

Si eres un particular que por virtud de un contrato realizado con un Ente Público tienes que tratar datos personales, entonces eres un *Usuario* y como tal es necesario que tengas en consideración el siguiente check list, que tiene como propósito ayudarte a cumplir con tus obligaciones.

PREGUNTAS	Sí	No
1. ¿Cuentas con una copia del contrato o convenio por el que se te faculta dar tratamiento a los datos personales?		
2. En dicho instrumento ¿se establece la finalidad del tratamiento de los datos personales?		
3. En dicho instrumento ¿se establece los tipos y medidas de seguridad que deberás estar observando?		
4. En dicho instrumento ¿se establece el deber de confidencialidad?		
5. En dicho instrumento ¿Se establece si deberás regresar los datos personales al Ente Público una vez terminado el objeto del contrato?		
6. En caso de que sea negativa la respuesta al punto anterior ¿En dicho instrumento se establece el procedimiento de supresión de los datos?		
7. ¿En dicho instrumento se establecen los procedimientos por los cuáles el *Responsable* del SDP te notificará la actualización de los datos personales?		
8. ¿En dicho instrumento se establece los procedimientos por los cuáles el Responsable del SDP te notificará el resultado del procedimiento de Revocación del Consentimiento ejercitado por el titular de los datos personales y las acciones que deberás emprender para dar cumplimiento a esa resolución?		
9. ¿En dicho instrumento se establece el procedimiento por el cual se dará atención a las solicitudes ARCO que sean presentadas?		
10. ¿Dentro del Documento de Seguridad se señala tus funciones y obligaciones?		
11. ¿Dentro del Documento de Seguridad se señala a que datos personales puedes tratar?		

PREGUNTAS	Sí	No
12. ¿El Responsable del SDP te ha comunicado los procedimientos por los cuales debes notificar una incidencia?		
13. ¿El Responsable del SDP te ha señalado que en caso de que seas un sujeto obligado por la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, deberás sujetarte también a lo señalado en dicha Ley?		
14. ¿Cumples con las disposiciones contenidas en la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*?		
15. En el caso de que prestes tus servicios afuera de las instalaciones que ocupa el ente público, ¿Cuentas con procedimientos para asegurar la confidencialidad de los datos personales en el traslado de la información?		
16. ¿Has adoptado procedimientos internos para asegurar el cumplimiento de los principios de licitud, confidencialidad y seguridad?		

Apartado V

De las Oficinas de Información Pública y los procedimientos de los Derechos ARCO

De la Oficina de Información Pública

La Ley de Protección de Datos Personales para el Distrito Federal (LPDPDF) aprovechó parte del andamiaje creado por la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal; en específico nos referiremos en el presente apartado a la Oficina de Información Pública (OIP), la cual, su actividad central, se activa en la gestión de las solicitudes de los Derechos de ARCO.

La OIP es la unidad administrativa receptora de las solicitudes ARCO, y la que estará a cargo de su Entre las funciones que tiene están:

1. Recibir de revocación del consentimiento y las solicitudes ARCO.

2. Gestionarlas al interior del Ente.

3. Comunicar la respuesta recaída, previa acreditación de la personalidad.

La OIP es definida en el artículo 3 de la LPDPDF como:

> *La unidad administrativa receptora de las solicitudes de acceso, rectificación, cancelación y oposición de datos personales en posesión de los Entes públicos, a cuya tutela estará el trámite de las mismas, conforme a lo establecido en esta Ley y en los lineamientos que al efecto expida el Instituto;*

A estas funciones que desempeña la OIP se tiene que agregar que es ante esta instancia donde el titular de los datos personales puede ejercer otro de los derechos contemplados en el artículo 16 de la LPDPDF, consistente Revocación del Consentimiento, la cual procede cuando exista a consideración del titular de los datos una causa justificada para su ejercicio y no se le atribuya efectos retroactivos; es decir, en el caso de que proceda el ejercicio de ese derecho, el tratamiento que el Ente Público haya realizado a los datos personales previo a su ejercicio, se mantendrá intacto, así como las consecuencias jurídicas que de esto derive.

Ahora bien, de la definición dada con anterioridad podemos desprender algunas de las obligaciones esenciales que tiene la OIP:

1. Recibir el requerimiento de revocación del consentimiento y las solicitudes de los Derechos ARCO.

2. Gestionarlas ante los Responsables de los SDP's que corresponda.

3. Ser el único canal del Ente Público para dar respuesta a la revocación del consentimiento y de las solicitudes ARCO.

A estas obligaciones esenciales se tiene que agregar lo señalado en el tercer párrafo del artículo 16 de la LPDPDF, que indica la obligación de la OIP de mantener en sus instalaciones los formatos necesarios para recabar el consentimiento del titular, en el que se asiente fehacientemente la intención de autorizar la cesión o difusión de sus datos personales.

Derechos ARCO

Antes de continuar, es necesario recapitular un poco lo analizado en los Apartados I y II de esta Guía. Para tal efecto, daremos un par de definiciones:

- Derechos ARCO: Derechos de Acceso, Rectificación, Cancelación y Oposición.

- Derecho de Acceso: Es la prerrogativa para solicitar y obtener información de los datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las cesiones realizadas o que se prevén hacer, en términos de la LPDPDF.

- Derecho de Rectificación: Es la potestad para solicitar la rectificación de datos del interesado en los sistemas de datos personales, cuando tales datos resulten inexactos o incompletos, inadecuados o excesivos, siempre y cuando no resulte imposible o exija esfuerzos desproporcionados.

- No obstante, cuando se trate de datos que reflejen hechos constatados en un procedimiento administrativo o en un

proceso judicial, aquellos se considerarán exactos siempre que coincidan con éstos, lo anterior de conformidad con los términos señalados en el artículo 28 de la LPDPDF.

- Derecho de Cancelación: Es la facultad del titular de los datos para pedir a un Ente Público que cancele los datos que posee sobre su persona. Se podrá solicitar la cancelación de sus datos cuando el tratamiento de los mismos no se ajuste a lo dispuesto en la Ley o en los lineamientos emitidos por el Instituto, o cuando hubiere ejercido el derecho de oposición y éste haya resultado procedente[19].

- Derecho de Oposición: es la facultad que tiene el titular de los datos personales a oponerse al tratamiento de los datos que le conciernan, en el supuesto en que los datos se hubiesen recabado sin su consentimiento, cuando existan motivos fundados para ello y la ley no disponga lo contrario. De actualizarse tal supuesto, el responsable del sistema de datos personales deberá cancelar los datos relativos al interesado.

- Prueba de Interés público: es la obligación que recae en el InfoDF de fundar y motivar, objetiva, cuantitativa y cualitativamente, el beneficio que representa la publicidad de la información de acceso restringido, por motivos de interés público; esto es, que los beneficios sociales de divulgar la información son

[19] La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de los Entes Públicos para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el plazo deberá procederse a su supresión, en términos de la normatividad aplicable.
Es de señalar que la supresión de datos no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando exista una obligación legal de conservar dichos datos

mayores al daño que se pudiera generar por su publicación[20].

Procedimiento para la Atención de Solicitudes ARCO

Las solicitudes correlativas al ejercicio de los derechos ARCO son presentadas ante la OIP. Para que el titular pueda ejercitar esos derechos, deben cubrir los requisitos establecidos en el artículo 34 de la LPDPDF:

Para presentar una solicitud ARCO se deben cubrir diversos requerimientos de forma y fondo

> *I. Nombre del Ente Público a quien se dirija;*
>
> *II. Nombre completo del interesado, en su caso, el de su representante legal;*
>
> *III. Descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos antes mencionados;*
>
> *IV. Cualquier otro elemento que facilite su localización;*
>
> *V. El domicilio, mismo que se debe encontrar dentro del Distrito Federal, o medio electrónico para recibir notificaciones, y*
>
> *VI. Opcionalmente, la modalidad en la que prefiere se otorgue el acceso a sus datos personales, la cual podrá ser consulta directa, copias simples o certificadas.*

Con referencia a la fracción II del artículo citado, es importante señalar que, a diferencia de una solicitud de

[20] La prueba de interés público no debe ser confundida con la prueba de daño, ya que esta última sólo procede cuando el Ente se encuentra enfrente de información reservada (artículo 37 de la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal), y tiene como finalidad justificar que la divulgación de cierta información solicitada, lesiona el interés jurídicamente protegido por la ley y que su publicidad puede producir un daño mayor al interés de conocerla.

acceso a la información pública, en éste caso es necesario la acreditación de la personalidad del titular de los datos personales, ya que no debemos de perder de vista el principio de confidencialidad contemplado en dicha ley, que señala para estos efectos, que sólo el titular y las personas autorizadas podrán tener conocimiento de los datos personales; por tal efecto, es necesario que el titular o su representante acrediten su personalidad, la cual, como señala el segundo párrafo del artículo 34 de la LPDPDF se acredita al momento de que alguna de estas personas asista a la OIP para recoger la resolución que haya recaído a la solicitud[21]. Para tal efecto, contará el particular con 10 días hábiles[22].

La identidad del solicitante se acredita al acudir a la OIP a recoger la información

Ahora bien, el artículo 34 de la LPDPF impone también un requisito de fondo o de procedencia, en específico cuando se trata del ejercicio del derecho de rectificación. En este caso, el titular de los datos personales deberá señalar qué dato personal es erróneo y deberá acompañar los documentos necesarios que sustentan su afirmación. Dentro de ésta misma lógica, en el caso de que se ejercite el derecho de cancelación u oposición, debe señalar las causas que dan sustento a su solicitud.

Las solicitudes ARCO pueden ser presentadas por diversas vías.

Las solicitudes ARCO pueden ser presentadas por diversas vías, las cuales se encuentran contempladas en el artículo 33 de la LPDPDF, que a saber son:

---

[21] En este mismo sentido el segundo párrafo, del numeral 18, de los Lineamientos para la gestión de las solicitudes de Información Pública y de Datos Personales a través del Sistema Infomex del Distrito Federal establece que "Independientemente del medio a través de cual se reciba la solicitud, la identidad del interesado o la personalidad, identidad y facultades de su representante legal, se acreditarán en el momento que se presenten en la Oficina de Información Pública correspondiente para obtener la respuesta sobre la solicitud de sus datos personales."

[22] En el supuesto de que, hubiere tenido costo por reproducción, la OIP notificará al solicitante los costos respectivos, calculándolos a través de la aplicación informática de INFOMEX, indicándole los datos para realizar el pago en las instituciones autorizadas. En este caso el solicitante deberá acreditar su identidad ante la Oficina de Información Pública, así como el pago correspondiente, en un plazo máximo de diez días hábiles a partir de la notificación de la determinación, esto en los términos del numeral 21, segundo párrafo, de los Lineamientos para la gestión de solicitudes de información pública y de datos personales a través del sistema INFOMEX del Distrito Federal.

I. Por escrito material, será la presentada personalmente por el interesado o su representante legal, en la oficina de información pública, o bien, a través de correo ordinario, correo certificado o servicio de mensajería;

II. En forma verbal, será la que realiza el interesado o su representante legal directamente en la oficina de información pública, de manera oral y directa, la cual deberá ser capturada por el responsable de la oficina en el formato respectivo;

III. Por correo electrónico, será la que realiza el interesado a través de una dirección electrónica y sea enviada a la dirección de correo electrónico asignada a la oficina de información pública del Ente Público;

IV. Por el sistema electrónico que el Instituto establezca para tal efecto, y

V. Por vía telefónica, en términos de los lineamientos que expida el Instituto.

Es de señalar que si el titular de los datos personales no realizó la solicitud ARCO por medio de INFOMEX o vía TEL-INFO, la OIP tiene la obligación de inscribir en INFOMEX esa solicitud, y enviar al solicitante por el medio señalado para oír y recibir las notificaciones, en un término no mayor a tres días hábiles contados a partir de la fecha de recepción, el acuse generado por dicho sistema. Lo anterior, en los términos del numeral 19 de los Lineamientos para la gestión de solicitudes de información pública y de datos personales, a través del sistema INFOMEX del Distrito Federal.

Si al ser presentada la solicitud no es precisa, o no contiene todos los datos requeridos, en ese momento el Ente Público, en caso de ser solicitud verbal, deberá ayudar al solicitante a subsanar las deficiencias. Si los detalles proporcionados por el solicitante no bastan para localizar los datos personales, o son erróneos, la oficina

de información pública del Ente Público podrá prevenir, por una sola vez y, dentro de los cinco días hábiles siguientes a la presentación de la solicitud, para que aclare o complete su solicitud, apercibido de que de no desahogar la prevención se tendrá por no presentada la solicitud[23].

En el supuesto de que en la solicitud de rectificación el titular de los datos personales no adjuntara a sus requerimientos los documentos probatorios, la OIP deberá requerírselo en un término no mayor de tres días hábiles, contados a partir de la fecha en que recibió la solicitud, con el apercibimiento al particular que, de no proporcionar la información que da sustento a su requerimiento en un término igual, o de no realizar dicho acto, la OIP podrá prevenir al titular o su representante legal. Es de señalar que, a partir de que se reciban los documentos probatorios, es cuando se iniciará el cómputo del plazo de los quince días hábiles señalado en la LPDPDF[24].

Una vez recibida la respuesta a la prevención formulada por la OIP, o en su caso, de ser procedente la solicitud, la OIP deberá turnar vía INFOMEX el requerimiento a los Responsables de los SDP`s (Unidades Administrativas), que a su criterio considere son competentes para dar atención a dicho requerimiento[25], donde se tendrán que realizar las gestiones necesarias para dar atención al requerimiento formulado por el titular de los datos.

En el supuesto de que fuere procedente el ejercicio de los Derechos ARCO, el *Responsable* del SDP deberá notificar al titular de la OIP –vía INFOMEX–, la resolución correspondiente y, en su caso, el señalamiento de que su reproducción tiene un costo.

[23] Artículo 32 de la LPDPDF.
[24] Numeral 19, fracción V de los Lineamientos para la gestión de solicitudes de información pública y de datos personales a través del sistema INFOMEX del Distrito Federal.
[25] Numeral 19, fracción III de los Lineamientos para la gestión de solicitudes de información pública y de datos personales a través del sistema INFOMEX del Distrito Federal.

Ahora bien, en el supuesto de que no se localizare la información requerida, el *Responsable* del SDP, en coordinación con el titular de la OIP y un representante del órgano interno de control, deberán levantar un acta circunstanciada en la que se indique los SDP's en los que se realizó la búsqueda y el resultado obtenido[26]. En el supuesto de que el Ente Público no tenga las atribuciones legales (principio de licitud) para detentar los datos personales sobre los que se ejercita los Derechos ARCO –esto en virtud de que corresponde a otro Ente Público– el Responsable del SDP, en coordinación con la OIP, elaborarán un documento fundado y motivado en el que se plasme las razones por las que no procedió la solicitud; dicho documento debe ser firmado por estas dos personas.

Los Derechos ARCO tienen límites, estos son:

1. Información relacionada con fines policiales.

2. Se obstaculice las actuaciones de las autoridades durante el cumplimiento de sus atribuciones.

3. En defensa del Estado, la seguridad pública o los derechos de terceros.

Es de señalar que los Derechos ARCO no son absolutos y se puede negar su ejercicio en los siguientes casos[27]:

- Cuando los datos estén en sistemas de datos personales con fines policiales, tributarios o de investigación científica;
- Cuando los mismos obstaculicen la actuación de la autoridad durante el cumplimiento de sus atribuciones; o bien,
- En defensa del Estado, la seguridad pública o los derechos de terceros.

De ser el caso, el Responsable del SDP, en colaboración con la OIP, deberán fundar y motivar por escrito las causas por las que no es procedente el ejercicio de los Derechos ARCO[28]. El escrito debe estar firmado por ambos servidores públicos.

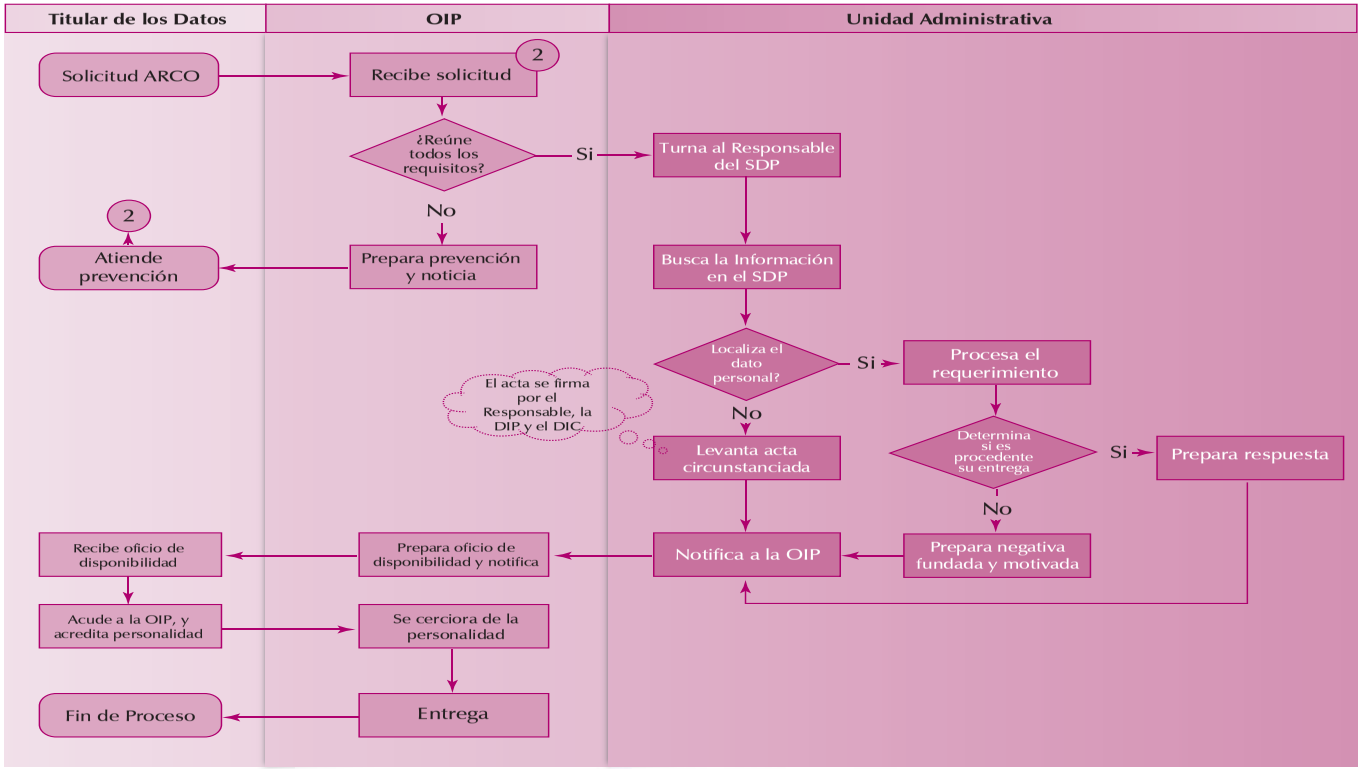
Ahora bien, en el supuesto de que el plazo de quince días hábiles no fuere suficiente para dar atención a la

[26] Último párrafo del artículo 32 de la LPDPDF.
[27] Artículo 12 de la LPDPDF.
[28] Artículo 36 de la LPDPDF.

solicitud ARCO, la OIP deberá notificar al titular de los datos personales, o en su caso al representante, la necesidad de ampliar dicho término por uno igual. Dicha notificación deberá estar fundada y motivada.

En la siguiente gráfica se ejemplificará el procedimiento de la solicitud ARCO.

Figura 5. Procedimiento para el ejercicio de los Derechos ARCO.



Fuente: Santiesteban (2011).

Criterios Adoptados en Materia de Datos Personales por el Pleno del INFODF

Como se ha mencionado en múltiples ocasiones, no todos los datos personales que se encuentran en posesión de los Entes Públicos reciben el estatus de confidenciales en los términos de la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal. Incluso, se ha señalado que, en términos de lo establecido en el numeral 5 de los Lineamientos para la Protección de Datos Personales en el Distrito Federal, existe una categoría de datos que recibe la denominación de públicos.

No todos los datos personales en posesión de los Entes públicos reciben el estatus de confidenciales en los términos de la LTAIPDF

Al respecto, el Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, ha emitido diversos criterios al respecto, los que a continuación se desarrollarán:

Datos de los Miembros que Integran una Sociedad Anónima Contenidos en las Actas Constitutivas de las Personas Morales pueden ser Considerados como Personales

Los datos de los miembros que integran una sociedad anónima son considerados como personales, debido a que diversas disposiciones de la Ley General de Sociedades Mercantiles establecen la factibilidad de que las actas constitutivas de personas morales contengan información que identifique o haga identificable a una persona física, como es el nombre, la nacionalidad, el domicilio, el Registro Federal de Contribuyentes, la Clave Única de Registro de Población, los teléfonos particulares, la matrícula del Servicio Militar Nacional, el número de pasaporte, lugar y fecha de nacimiento y edad de los integrantes de la sociedad; así como datos patrimoniales, entre los que se encuentran el importe del capital social, la expresión de lo que cada socio aporta en dinero o en otros bienes, el valor atribuido a éstos y el criterio seguido para su valorización, la manera de distribuir las utilidades y pérdidas entre los miembros de la sociedad y el importe del fondo de reserva.

En general, estos datos son de naturaleza tal que se considera información de acceso restringido en la modalidad de confidencial, de acuerdo con lo dispuesto por los artículos 4, fracciones II, VII, VIII y X, y 38, fracciones I y IV, de la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal, por lo que únicamente resulta procedente acceder a ellas en versiones públicas.

Para mayor referencia véase la resolución del Recurso de Revisión RR. 099/2011, interpuesto en contra de la Procuraduría Social del Distrito Federal; la resolución del Recurso de Revisión RR.161/2011, interpuesto en contra de la Secretaría de Desarrollo Urbano y Vivienda del Distrito Federal; así como el Recurso de Revisión RR.1054/2011, 1065/2011 y 1088/2011, interpuesto en contra de la Procuraduría Social del Distrito Federal.

El Nombre y Resultados Obtenidos en Evaluaciones Practicadas a los Aspirantes que Participan en las Convocatorias para la Selección y Admisión de Personal para Ocupar un puesto Público

Si se solicitan los nombres y resultados de evaluaciones practicadas a aspirantes en convocatorias de selección y admisión de personal para ocupar un puesto público, la información debe ser clasificada como de acceso restringido en la modalidad de confidencial, con base en los artículos 4, fracción VII, y 38, fracciones I y IV, de la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal, en relación con el numeral 5, fracción III, de los *Lineamientos para la Protección de Datos Personales en el Distrito Federal*, en virtud de que la información relacionada con el honor no puede ser divulgada bajo ninguna circunstancia, pues su divulgación puede afectar el honor y la imagen de aquellas personas que, habiendo participado en un proceso de selección, no acreditaron todas y cada una de sus etapas, o bien que no hubiesen resultado ganadoras del puesto.

Esta salvedad no resulta aplicable en el caso del personal que sí aprobó todas las fases de selección y funge como

servidor público, toda vez que dicha información permite verificar a la ciudadanía que los seleccionados obtuvieron un resultado óptimo en el proceso de selección para desempeñar el cargo público que ostentan.

Para mayor referencia consúltese las resoluciones de los Recursos de Revisión RR.1411/2010, y RR.1589/2010, ambos contra del Instituto de Verificación Administrativa del Distrito Federal, así como la resolución al Recurso de Revisión RR.1691/2010, interpuesto en contra de la Contraloría General del Distrito Federal.

Acceso Integro a la Información Contenida en el Curriculum Vitae de los Servidores Públicos

El currículum vitae constituye una relatoría de vida de los títulos, honores, cargos, trabajos realizados y datos biográficos, que permite calificar a una persona en cuanto a su trayectoria y experiencia en el ámbito profesional.

El artículo 14, fracción V, de la *Ley de Transparencia y Acceso a la Información Pública del Distrito Federal* impone a los Entes Públicos la obligación de divulgar en sus sitios de Internet, los perfiles de puestos especificados en toda su estructura, siempre que la normatividad aplicable al Ente Público lo establezca, así como el currículum de quienes ocupan dichos cargos a partir de Jefe de Departamento y niveles superiores. No obstante, si se solicita el currículum de un servidor público, para atender la solicitud, el Ente Público debe testar la información de acceso restringido que se encuentre en el documento que lo contiene, como podría ser el caso de la CURP, RFC, domicilio particular, estado civil, y restringir su acceso en cualquiera de sus modalidades: reservada y/o confidencial.

Para mayor referencia consúltese las resoluciones a los Recursos de Revisión RR.1411/2010, y RR.1589/2010, interpuestos en contra del Instituto de Verificación Administrativa del Distrito Federal, resueltos en las sesiones del doce y el diecinueve de enero de dos mil once por unanimidad de votos.

Publicidad del Domicilio y el Registro Federal de Contribuyentes de un Proveedor

De conformidad con lo dispuesto por el artículo 38, fracciones I y IV, de la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal y el numeral 5 de Lineamientos para la Protección de Datos Personales en el Distrito Federal, el Registro Federal de Contribuyentes y el domicilio de las personas revisten el carácter de información confidencial al tratarse de datos personales relacionados con su vida privada. No obstante, sin perjuicio de lo expuesto, la información incluida en contratos celebrados con los Entes Públicos reviste el carácter de información pública, ya que estos datos permiten verificar que las personas con las que contratan los sujetos obligados se encuentran al corriente en el cumplimiento sus obligaciones fiscales.

Para mayor referencia véase la resolución del Recurso de Revisión RR.857/2010, interpuesto en contra de la Delegación Coyoacán.

Publicidad de la Información Relativa de aquellos Particulares que han obtenido una Autorización, Licencia, Concesión o Permiso de alguna Autoridad del Distrito Federal

La Ley de Protección de Datos Personales para el Distrito Federal establece la obligación a los Entes Públicos, de proteger los datos personales que detentan en el ejercicio de sus atribuciones. Así, los datos no podrán ser cedidos ni difundidos sin el consentimiento de su titular. Sin embargo, la Ley también prevé excepciones a este tratamiento. En su artículo 16 indica que el consentimiento quedará exceptuado, cuando la transmisión de los datos esté prevista expresamente en una ley. Tal es el caso de la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal, marco normativo en el que la interpretación armónica de sus artículos 14, fracción XVIII, y 38, fracción I, arroja que los datos personales cuya publicidad esté prevista en una Ley, no

tienen el carácter de confidencial, verbigracia, la relativa al nombre del titular de concesiones, licencias, permisos y autorizaciones para el ejercicio de determinada actividad, prevista en la normatividad respectiva.

En este sentido, el conocimiento de datos relativos al nombre o nombres de personas involucradas en el ejercicio de alguna actividad autorizada y permitida por la autoridad administrativa competente, debe darse a conocer y ser entregada a quien la solicite por la vía del ejercicio del derecho de acceso a la información pública.

Para mayor referencia véase la resolución del Recurso de Revisión RR0799/2011 y RR800/2011 acumulados, en contra de la Delegación Iztacalco.

Nombre y la Firma de un Representante o Apoderado Legal son Sustentables de Publicación

De conformidad con los artículos 4, fracción VII, de la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal, y 2, acepción segunda, de la Ley de Protección de Datos Personales para el Distrito Federal, y numeral 5, fracción I, de los Lineamientos para la Protección de Datos Personales en el Distrito Federal, los datos identificativos de una persona física, como el nombre y la firma del representante o apoderado legal de una persona moral, revisten el carácter de información confidencial, al tratarse de datos relacionados con su vida privada. Sin perjuicio de lo anterior, cuando esta información se encuentre en contratos o convenios celebrados con Entes Públicos, reviste el carácter de información pública, ya que forma parte del conjunto de datos que permiten verificar que las personas con las que contratan los sujetos obligados están autorizadas para celebrar actos jurídicos de carácter público.

Para mayor referencia véase la resolución del Recurso de Revisión RR.805/2011, interpuesto en contra de la Sistema para el Desarrollo Integral de la Familia del Distrito Federal, así como del Recurso de Revisión RR.1351/2011, interpuesto en contra del Sistema de Aguas de la Ciudad de México.

Padrón de Contribuyentes del Impuesto Predial, Publicidad de

No es pública la información relativa al padrón de contribuyentes del impuesto de predial, esto en los términos del artículo 37, fracción V, de la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal, ya que restringe el acceso a información protegida por el secreto fiscal. Así mismo, de conformidad con el artículo 124 del Código Financiero del Distrito Federal, el secreto fiscal es la obligación que tienen las autoridades fiscales de guardar absoluta reserva respecto de los datos suministrados por los contribuyentes, como parte de los trámites relativos a la aplicación de las disposiciones tributarias, y sólo son accesibles a su titular y los servidores públicos que requieran conocerla para el ejercicio de sus funciones.

Por otra parte, la información de carácter fiscal se encuentra relacionada con el patrimonio de las personas, adquiriendo la naturaleza de información confidencial, en términos de los artículos 38 y 44 de la Ley de Transparencia, manteniendo ese carácter de manera indefinida. En ese orden de ideas, si la información contenida en el padrón de contribuyentes se recolecta y actualiza mediante declaraciones o promociones presentadas por los contribuyentes, por terceros con ellos relacionados, o se obtiene por la autoridad fiscal en ejercicio de sus facultades de comprobación, se entiende que se encuentra protegida por el secreto fiscal y, por tanto, constituye información de acceso restringido en su carácter de reservada; sin embargo, al encontrarse dicha información relacionada con el patrimonio de los contribuyentes, la misma debe ser clasificada y protegida siguiendo las reglas aplicables a la información confidencial.

Al respecto consúltese la resolución del Recurso de Revisión RR.813/2009, interpuesto en contra de la Secretaría de Finanzas del Distrito Federal.

Datos Personales de Servidores Públicos que Participan en Blogs o Redes Sociales como Twitter o Facebook, no son Públicos

Los nombres de servidores públicos que laboran en entidades públicas del Distrito Federal no constituyen información confidencial. Sin embargo, si se asocian con información relativa a su vida privada y afectiva y están disponibles para el Ente Público al que se ha dirigido una solicitud con tales características, sí son susceptibles de protección, en términos de la fracción VII del artículo 4 y de la fracción I y último párrafo del artículo 38, de la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal, pues se considera que esta información debe ser protegida, en virtud de que tener un blog o una cuenta en cualquier red social es decisión relativa a la vida privada de cada individuo.

Es un hecho que las redes sociales no tienen la finalidad exclusiva de que los servidores públicos mantengan comunicación con los gobernados. Su fin es propiciar un espacio para el intercambio de mensajes entre un círculo de personas que deciden recibirlos (Twitter); conectar a personas con intereses comunes e intercambiar información entre sí, como pueden ser fotos y mensajes (Facebook); o que las personas suban a la red una especie de tarjeta de presentación en la que quince amigos principales agregan comentarios sobre amistad o fotos del usuario (Hi5), y recibir comentarios sobre la forma en la que cada persona se presenta en su blog, así como obtener respuesta a ese comentario hasta entablar un diálogo, acciones todas relativas a la vida privada de quienes participan en diversas redes sociales por decisión propia.

Número de Seguridad social de un Solicitante de Servicios de Salud

De conformidad con los artículos 2 de la Ley de Protección de Datos Personales para el Distrito Federal y 38, fracción I, de la Ley de Transparencia y Acceso a la Información Pública el Distrito Federal, los datos personales revisten del carácter de información confidencial, que requieren del consentimiento de las personas para su difusión, distribución o comercialización, salvo las excepciones previstas en el artículo 16 de la Ley de Protección de Datos Personales para el Distrito Federal, por lo que el número de seguridad social no es susceptible de divulgación.

Publicidad de la Firma de un Servidor Público

Sólo es pública cuando consta en actos de autoridad. La firma puede ser considerada como información de acceso restringido en la modalidad de confidencial, por tratarse de información gráfica que concierne a una persona física, identificada o identificable, en términos de lo dispuesto por el artículo 38, fracciones I y IV de la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal, en relación con la acepción tercera del artículo 2 de la Ley de Protección de Datos Personales para el Distrito Federal.

Sin embargo, dado que se estima que la totalidad de los actos por los cuales un servidor público da curso a las funciones o actos de autoridad que por ley debe ejercer, o bien externa su voluntad manifiesta en un caso como su renuncia, acciones que deben ser expuestas al público, por lo que, para tener certeza de la ejecución de estos actos, se debe permitir el acceso a información (como la firma) que brinda certeza de que el acto ejecutado es atribuible a un determinado servidor público.

Para mayor referencia léase la resolución del Recurso de Revisión RR.730/2009, interpuesto en contra de la Delegación Tláhuac.

Datos Públicos de la Cédula Profesional

El número de la cédula y la fotografía son datos personales que se ubican en la categoría de los datos identificativos (artículos 4, fracción VII, y 38, fracción I y IV, de la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal, en relación con el numeral 5, fracción I, de los Lineamientos para la Protección de Datos Personales en el Distrito Federal). No obstante, para efectos de acceso a la información y rendición de cuentas, estos datos son susceptibles de entrega para asegurar que la persona que se identifica con la cédula es reconocida por la autoridad competente (Dirección General de Profesiones dependiente de la Secretaría de Educación Pública) para el ejercicio de la profesión o técnica que se asienta en la cédula profesional correspondiente. Así, junto con el nombre y la profesión o denominación de la técnica, el número de la cédula y la fotografía de su titular son información pública, aun cuando constituyan datos personales, al ser elementos determinantes en la identificación de una persona, respecto de sus conocimientos para ejecutar las actividades avaladas en ella.

La conclusión anterior se robustece con lo dispuesto por el artículo 23, fracción IV, de la Ley Reglamentaria del Artículo 5o. Constitucional, en cuanto al ejercicio de las profesiones en el Distrito Federal, ya que la cédula profesional es expedida por la Dirección General de Profesiones para que el titular de la cédula acredite su identidad en sus actividades profesionales.

Para mayor referencia consúltese la resolución del Recurso de Revisión RR.0099/2011, interpuesto en contra de la Procuraduría Social del Distrito Federal y del Recurso de Revisión RR.0332/2011, interpuesto en contra de la Delegación Gustavo A. Madero.

Momento Idóneo para hacer Público el Nombre de un Servidor Público Sancionado

El nombre de un servidor público relacionado con una sanción de inhabilitación se constituye en información reservada, cuando la resolución que la impuso no es firme, pues todavía puede ser modificada por el órgano revisor, o bien puede quedar sin efectos. De darse esta hipótesis, al revelar la sanción se afectaría el honor de la persona, toda vez que quedaría la impresión de que incurrió en responsabilidad administrativa, cuando la resolución sancionatoria no subsistió.

Por el contrario, el nombre relacionado con una sanción de inhabilitación impuesta por sentencia firme, no constituye información reservada ni confidencial, pues la resolución que la impuso no es susceptible de ser modificada. Aunque la información requerida pudiese ser considerada susceptible de afectar el honor de las personas, constituye información de interés público que al constar en una resolución o sentencia firme no se encuentra salvaguardada por el derecho al honor, por estar relacionada con servidores públicos y su desempeño. Lo anterior, con fundamento en los artículos 33 y 34, fracción I de la Ley de Responsabilidad Civil para la Protección de la Vida Privada, el Honor y la Propia Imagen en el Distrito Federal.

Adicionalmente, el artículo 68 de la Ley Federal de Responsabilidades de los Servidores Públicos impone al Ente Público la obligación de llevar un registro de las sanciones impuestas, con motivo del procedimiento disciplinario administrativo establecido en el mismo ordenamiento jurídico. De esta manera, toda la información generada, administrada o en posesión de los Entes públicos con motivo del desarrollo de sus funciones es de naturaleza pública, con excepción de aquella que la propia ley especial clasifica como de acceso restringido, en sus modalidades de reservada o confidencial. Sin embargo, el derecho de los servidores públicos respecto al honor e imagen se encuentra limitado, ya que los datos e información, relacionados con su desempeño dentro del

servicio público, se consideran información de interés público.

Para mayor referencia revísese la resolución del Recurso de Revisión RR.493/2007, interpuesto en contra de la Contraloría General del Distrito Federal.

Acceso a Datos del registro Civil Mediante el Ejercicio del Derecho de Acceso a Datos Personales

La entrega de datos registrales relacionados con un acta del estado civil de una persona no es susceptible de ser proporcionada por vía del derecho de acceso a la información. En términos del artículo 50, párrafo primero del Reglamento de la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal, cuando se advierta que el solicitante pretende desahogar trámites o servicios prestados por el Ente obligado a través de solicitudes de información pública, éste debe orientarlo sobre los procedimientos establecidos para acceder a dichos trámites o servicios.

Para mayor referencia véase la resolución del Recurso de Revisión RR.885/2011 y RR.896/2011, Acumulados interpuesto en contra de la Consejería Jurídica y de Servicios Legales del Distrito Federal.

Generación de un Documento Nuevo Mediante el ejercicio del Derecho de Acceso a Datos Personales

Cuando una persona solicita un documento en el que constan sus datos personales, y éste obra en algún expediente en particular, el Ente Público debe dar acceso a los datos en él contenidos, ya sea mediante copia simple, copia certificada —sólo si el Ente tiene facultades para expedirla y es posible certificar su contenido, sin testar ninguna de las partes— o consulta del documento. De no obrar el documento en el expediente, sólo debe hacerlo del conocimiento del solicitante en términos del

artículo 32 de la Ley de Protección de Datos Personales para el Distrito Federal, quedando exento de la obligación de generarlo, independientemente de si cuenta o no con un procedimiento específico para ello.

El único documento que puede ser generado mediante el ejercicio del derecho de acceso a datos personales es el informe sobre el tratamiento que han recibido los datos personales.

¿Procede el Ejercicio del Derecho de Cancelación de Datos Personales en el Caso de Información Publicada en Internet por un Ente Público y Localizada Mediante el uso de un Motor o Mecanismo de Búsqueda?

El derecho de cancelación es una prerrogativa del titular de los datos personales a solicitar la eliminación de datos que resulten inadecuados o excesivos en un sistema de datos personales a cargo de un Ente Público y que estén publicados en Internet. Serán inadecuados cuando no guarden relación con el ámbito de aplicación y finalidad por los que fueron recabados; o bien, si dejaron de ser necesarios con respecto a dicha finalidad. Los datos serán excesivos cuando se obtuvieron más de los estrictamente necesarios en relación con la finalidad.

Para que proceda la cancelación de datos personales a petición de parte deben cumplirse los siguientes requisitos:

1. Sólo el titular de los datos personales o su representante legal podrá solicitar la cancelación de sus datos personales;

2. Los datos personales que le conciernan deberán encontrarse en posesión de los Entes obligados;

3. Deberán señalarse las razones por las que el interesado considera que el tratamiento de sus datos no se ajusta a la ley o los lineamientos

emitidos por el Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal; o bien, acreditar que ejerció previamente el derecho de oposición y éste fue procedente;

4. Los datos personales que obren en poder del Ente obligado deberán ser inadecuados o excesivos. Serán inadecuados cuando no guarden relación con el ámbito de aplicación y finalidad por la cual se recabaron, o si dejaron de ser necesarios para esa finalidad. Serán excesivos cuando se obtuvieron más datos de los estrictamente necesarios en relación con la finalidad que motivó su recolección.

Solicitud de Copias Certificadas de Escrituras Públicas mediante el Ejercicio del Derecho de acceso a Datos Personales

El derecho de acceso a los datos personales es la prerrogativa de las personas para solicitar y obtener información de los datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las cesiones realizadas o que se prevén hacer, en términos de lo dispuesto por la Ley.

El acceso puede ser otorgado mediante la entrega de copias simples, copias certificadas o consulta directa (artículo 34, fracción VI de la Ley). Sin embargo, en el caso de copias certificadas de escrituras públicas, se deberá estar atento a lo dispuesto en el artículo 50, párrafo primero del Reglamento de la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal, que indica que cuando se advierta que el solicitante pretende desahogar trámites o servicios prestados por el Ente obligado a través de solicitudes de información pública, éste debe orientarlo sobre los procedimientos establecidos para acceder a dichos trámites o servicios.

Check List: Titulares OIP

Si eres titular de la Oficina de Información Pública del Ente, es necesario que tengas en consideración el siguiente check list, que tiene como propósito ayudarte a cumplir con tus obligaciones.

PREGUNTAS	Sí	No
1. ¿Cuentas en las instalaciones de la OIP con los formatos empleados por el ente para recabar el consentimiento de los titulares de los datos personales?		
2. ¿Cuentas con formatos por medio de los cuales el titular de los datos personales pueda revocar su consentimiento?		
3. ¿Cuentas al interior del ente público con procedimientos para dar gestión al requerimiento de revocación y las solicitudes ARCO?		
4. En términos de la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal ¿has capacitado a los Responsables de los SDP, Encargado y Usuarios en el manejo de la información confidencial?		
5. ¿Cuentas con procedimientos internos para levantar el acta circunstanciada a la que hace referencia el artículo 32 de la Ley de Protección de Datos Personales para el Distrito Federal?		
6. ¿Cuentas con políticas internas a fin de garantizar que has proporcionado la respuesta recaída a las solicitudes ARCO al titular de los datos personales o a su representante?		
7. ¿Cuentas con procedimientos internos relativos a la notificación del resultado del ejercicio del Derecho de Revocación del Consentimiento?		
8. ¿Cuentas con procedimientos internos tendientes a asegurar la confidencialidad de la información "complementaria" que proporcione el titular del dato que está ejercitando el Derecho de Rectificación?		
9. ¿Atiendes las solicitudes ARCO en los términos establecidos en la LPDPDF?		
10. ¿Has informado al *Enlace* en materia de datos personales del envio de los informes requeridos en tiempo y forma al InfoDF?		
11. ¿Has rendido de manera trimestral los informes sobre la atención a las solicitudes ARCO?		

Recomendaciones Generales en caso de cambio de Personal Involucrado en el Cumplimiento de la LPDPDF

Considerando que el proceso de Entrega-Recepción es un acto público y por ende queda sujeto a la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal, es importante tener presentes ciertos aspectos a fin de evitar incurrir en faltas administrativas.

Con independencia de lo que establezca la normatividad interna de cada Ente Público para los Procesos de Entrega-Recepción, es importante recordar que las obligaciones en transparencia y los derechos de acceso a la información y de protección de datos personales no quedan suspendidos durante el proceso de Entrega-Recepción. Por ello, se presentan algunas recomendaciones generales que ofrecen elementos operativos que garanticen la transparencia, el derecho de acceso a la información, la rendición de cuentas y la protección de datos personales en los procesos de Entrega-Recepción al interior de los Entes Públicos del Distrito Federal.

A manera enunciativa, más no limitativa, se proponen las siguientes:

Recomendaciones Generales:

1. Mantener operando y en constante actualización el Sistema Electrónico de Solicitudes de Información (INFOMEX) con el objeto de dar respuesta en tiempo y forma a las solicitudes de información pública y de acceso, rectificación, cancelación y oposición de datos personales (solicitudes ARCO) que se encuentran en proceso, de conformidad con los "Lineamientos para la gestión de solicitudes de información pública y de datos personales a través del sistema Infomex del Distrito Federal" y los

"Lineamientos que regirán la operación del Centro de Atención Telefónica del Instituto de Acceso a la Información Pública del Distrito Federal (Tel-InfoDF)".

La Dirección de Datos Personales atenderá todo tipo de consultas y dudas sobre aspectos relacionados con la protección de datos personales, el registro de sistemas de datos personales y la atención de solicitudes ARCO, en las extensiones 189, 243, 174 y 148.

2. Mantener operando y en constante actualización el portal de obligaciones de transparencia del Ente Público, con apego a los "Criterios y metodología de evaluación de la información pública de oficio que deben dar a conocer los Entes Públicos en sus portales de Internet".

   Para atender sus consultas sobre el mantenimiento y actualización del portal de Internet, la Dirección de Evaluación de Estudios pone a su disposición el teléfono 5636-2120 con las extensiones 139, 199 y 230.

   En este aspecto, es importante tener especial cuidado en no publicar datos personales adicionales a los establecidos en los Criterios, pues esto podría traducirse en infracciones a la Ley de Protección de Datos Personales para el Distrito Federal.

3. Elaborar los respectivos informes trimestrales, semestrales o anuales, según corresponda, al concluir los meses de marzo, junio, septiembre y diciembre. Esta obligación se encuentra prevista en la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal, en el artículo 71 fracción XII, así como el Artículo 24, fracción X, de la Ley de Protección

de Datos Personales del Distrito Federal. En caso de dudas, se recomienda contactar alpersonal de la Dirección de Evaluación de Estudios al teléfono 5636-2120 con la extensión 176.

4. El Capítulo II de la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal se refiere al recurso de revisión que los ciudadanos pueden interponer ante el InfoDF cuando están inconformes con la respuesta que recibieron a una solicitud de información, o cuando no reciban respuesta alguna. Es importante verificar si hay informes de ley pendientes de rendir pues la omisión en el cumplimiento de esta obligación es causa de responsabilidad.

La Dirección Jurídica y Desarrollo Normativo del InfoDF es el área encargada de sustanciar y proyectar las resoluciones a los recursos de revisión. Su titular así como su equipo de colaboradores, podrán aclarar sus dudas en el teléfono 5636-2120, en las extensiones 130, 191 y 106.

Recomendaciones en Términos de las Actas de Entrega - Recepción

En términos de los elementos que de forma general se consideran en las actas tipo de Entrega - Recepción, se emiten las siguientes recomendaciones sobre los temas y asuntos que el InfoDF considera importante incorporar en materia de transparencia, acceso a la información pública y protección de datos personales, en las actas mencionadas. Es importante subrayar que los elementos propuestos son sólo de forma indicativa, más no limitativa y que adicionalmente a lo aquí señalado debe tenerse en consideración la normatividad específica aplicable al Ente Público para el desarrollo de los procesos de Entrega - Recepción.

a) En términos del reporte de la Estructura Orgánica, entregar y recibir información sobre:

- Estructura de la Oficina de Información Pública y/o su ubicación en la estructura orgánica del Ente Público.

b) En términos de recursos humanos, entregar y recibir información sobre:

- Responsable de la Oficina de Información Pública: nombre, categoría, clave, puesto, sueldo, sobresueldo, compensaciones y demás remuneraciones.
- Responsable (s) operativo (s) de la Oficina de Información Pública: nombre, categoría, clave, puesto, sueldo, sobresueldo, compensaciones y demás remuneraciones.
- Personal de apoyo: nombre, categoría, clave, puesto, sueldo, sobresueldo, compensaciones y demás remuneraciones.

c) En términos de derechos y obligaciones, precisar información sobre:

- Convenios de colaboración y fortalecimiento en materia de transparencia, acceso a la información y protección de datos personales.

d) En términos de Recursos Materiales, ofrecer y recibir información sobre:

- Mobiliario, equipo e instrumentos y aparatos con los que cuenta la Oficina de Información Pública.

e) En términos de bienes informáticos y otros, ofrecer y recibir información sobre:

- Bienes informáticos de uso exclusivo de la Oficina de Información Pública: indispensable indicar equipo(s) de cómputo, impresora(s), escáner.
- Dirección electrónica del portal de Internet del Ente Público.

- Respaldos electrónicos de la información pública de oficio publicada en la sección de transparencia.
- Dirección de correo electrónico de la Oficina de Información Pública.
- Clave de acceso y contraseña para consultar correo electrónico de la Oficina de Información Pública.
- Claves de acceso de la Oficina de Información Pública y de las unidades administrativas para operar el Sistema INFOMEX.

f) En términos de relación de archivos, ofrecer y recibir información sobre:

- Expedientes de las solicitudes de acceso, rectificación, cancelación y oposición de datos personales (solicitud, respuesta y, en su caso, recibo de pago).
- Expedientes de los recursos de revisión y, en su caso, los documentos relativos al cumplimiento de las resoluciones del Pleno del InfoDF, con motivo de las solicitudes de acceso, rectificación, cancelación y oposición de datos personales.
- Informes trimestrales y anuales de las solicitudes de información pública y acceso, rectificación, cancelación y oposición de datos personales 2010, 2011, 2012, etc. (impresos y electrónicos).

g) En términos de relación de archivos, ofrecer y recibir información sobre:

- Resultados de las evaluaciones-diagnósticas realizadas por el InfoDF respecto del cumplimiento de lo dispuesto por los artículos 8 y 9 de la Ley de Protección de Datos Personales para el Distrito Federal 2011 (impresas y electrónicas).
- Actividades que derivan de la implementación del Acuerdo 0795/SO/04-07/2012, mediante

el cual se aprueban los criterios y la metodología de evaluación de la calidad de la información inscrita en el Registro Electrónico de Sistemas de Datos Personales.
- Recomendaciones para el cumplimiento de obligaciones en protección de datos personales 2011 y 2012.
- Documentos mediante los cuales se notifica la solventación de las recomendaciones realizadas por el InfoDF.
- Registro de los Sistemas de Datos Personales a cargo de la demarcación.
- Registro y disponibilidad del documento de seguridad que establece las medidas, procedimientos y niveles de seguridad con que son resguardados los sistemas.

h) En términos de asuntos en trámite, ofrecer y recibir información sobre:

- Solicitudes de acceso, rectificación, cancelación y oposición de datos personales pendientes de atención.
- Solventaciones pendientes, en su caso, sobre del cumplimiento de lo dispuesto por los artículos 8 y 9 de la Ley de Protección de Datos Personales para el Distrito Federal.
- Entrega de informes de solicitudes de información pública al InfoDF.
- Entrega del informe trimestral, en su caso, de las solicitudes de acceso, rectificación, cancelación y oposición de datos personales.
- Informes al InfoDF sobre recursos de revisión.

i) En términos de asuntos en trámite, ofrecer y recibir información sobre:

- Entrega de informes de solicitudes de información pública al InfoDF.
- Entrega del informe trimestral, en su caso, de las solicitudes de acceso, rectificación, cancelación y oposición de datos personales.

Índice

De Conceptos

Índice de Conceptos Relevantes

Índice de preguntas relevantes agrupadas por tema de interés

CONCEPTOS GENERALES

Instancias Responsables en el Cumplimiento de la Ley

ÍNDICE DE CONCEPTOS

Deber de Publicar en la GODF la Creación, Modificación o Supresión de los Sistemas de Datos Personales

Deber de Registrar los Sistemas de Datos Personales ante el INFODF

Deber de Informar al Titular de los Datos

Medidas de Seguridad

Obligaciones en Materia de Capacitación

ÍNDICE DE CONCEPTOS

Atención a Solicitantes ARCO

Publicidad de datos Personales por Razones de Interés Publico

ÍNDICE DE CONCEPTOS

Referencias

Davara, Isabel (2010) "Artículo 21" en Carbonell M (Coord.) Ley de Protección de Datos Personales, Comentada, Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal; Gobierno del Distrito Federal; Secretaría de Gobierno; Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México; Asamblea Legislativa del Distrito Federal; y Tribunal Superior de Justicia del Distrito Federal, México, 2010.

Santisteban Maza Rodrigo, (Diciembre 2011) "Algunos aspectos generales y los procedimientos contemplados en la Ley de Protección de Datos Personales para el Distrito Federal" en Bustillos Roqueñí R (Coord.) Transparencia y Datos Personales en el Distrito Federal, Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, Distrito Federal, México, 2011.

Santisteban Maza, Rodrigo, (2012) "Los datos personales en tus primeros pasos de tu vida profesional" conferencia dictada durante la Tercera Expo Conexión Transporte, Instituto Politécnico Nacional, Unidad Profesional Interdisciplinaria de Ingeniería y Ciencias Sociales y Administrativas, 19 de septiembre de 2012.

Santisteban Maza Rodrigo, (Agosto 2011) "Datos Personales… un nuevo reto" conferencia dictada en Executive Development Center Santa Fe, Universidad del Valle de México, 25 de agosto de 2011.

Santisteban Maza Rodrigo, (Mayo 2011) "El Derecho Humano a la Protección de Datos Personales en América Latina", módulo impartido dentro de la cátedra del Seminario Internacional, en la Maestría en Derecho, Universidad Anáhuac del Sur S.C., Mayo de 2011.

Villanueva, Ernesto (2005) "Derecho a la Privada" en Carbonell M (Coord.) Diccionario de Derecho Constitucional, México, Distrito Federal, México: Porrúa, Universidad Nacional Autónoma de México.

Marco Normativo.

Constitución Política de los Estados Unidos Mexicanos.

Ley de Protección de Datos Personales para el Distrito Federal.

Lineamientos para la Protección de Datos Personales en el Distrito Federal.

Instituto de Acceso a la Información Pública
y Protección de Datos Personales del Distrito Federal

Guía para Servidores Públicos ¿Cómo cumplir con
la Ley de Protección de Datos Personales
para el Distrito Federal?

Se terminó de imprimir en los
talleres de Servicio Editorial Gráfico en
diciembre de 2012, con un tiraje de 1,000 ejemplares