TALLER
MEDIDAS DE SEGURIDAD E INTEGRACIÓN DE DOCUMENTOS DE SEGURIDAD DE LOS SISTEMAS DE DATOS PERSONALES

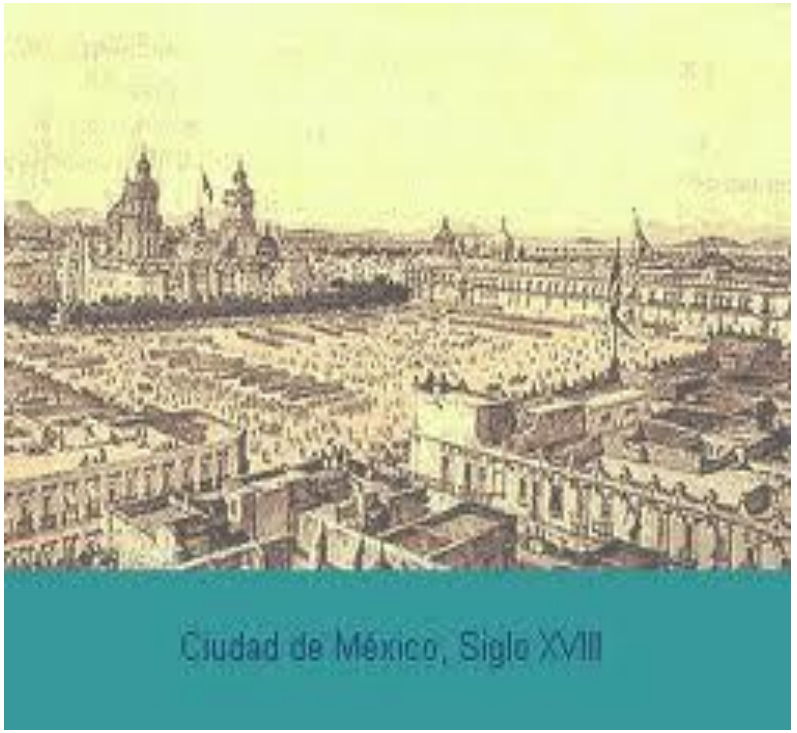
INTRODUCCIÓN

La protección de datos personales ha surgido como un nuevo derecho para las transformaciones sociales y culturales por lo que la importancia de su creación se debió a la intimidad necesaria para proteger las creencias, los pensamientos, emociones y sensaciones de la persona, por lo que su origen se ha justificado como protección de este derecho frente a cualquier intromisión injustificada del gobierno o persona ajena, en la vida privada del individuo, garantizando la seguridad de los ciudadanos en su persona, domicilio o correspondencia, reputación, etc.

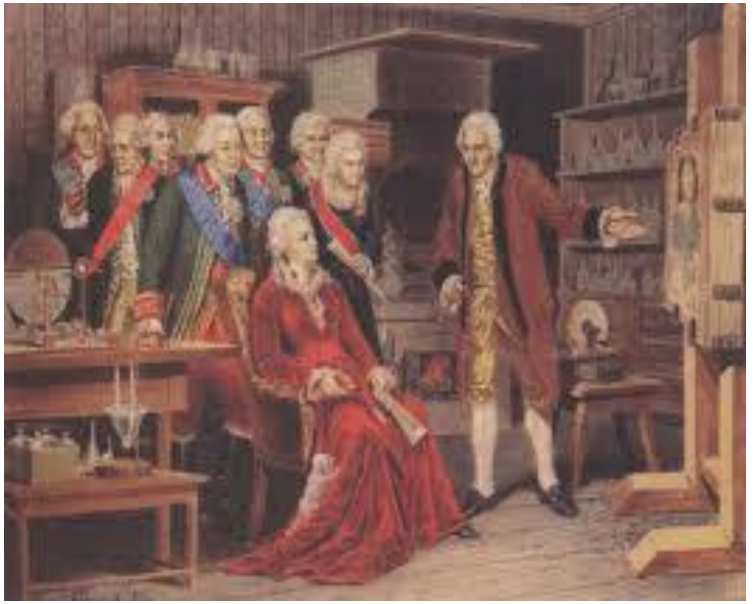
El ser humano a lo largo de su vida va dejando una enorme estela de datos que se encuentran dispersos, por lo que actualmente, con la utilización de nuevos medios tecnológicos, resulta posible agrupar y tratar de interpretar dichos datos, mismos que podrían ser utilizados como objeto de manipulaciones, extorsiones, o bien que podría interferir en su vida.

El derecho del ciudadano a preservar el control sobre sus datos personales y la aplicación de las nuevas tecnologías de la información, deben ser el contexto en el cual el legislador puede consagrar el derecho fundamental a la protección de datos personales.

ANTECEDENTES



A partir del siglo XVIII los Derechos Humanos comenzaron a estar presentes, y con su reconocimiento en la normativa constitucional fueron alcanzando su consolidación como prerrogativas inherentes a todo ser humano.



El derecho a la intimidad a la protección de datos personales.

El **derecho a la intimidad** abarca aquello que se considera más propio y oculto del ser humano (entendiéndose por propio y oculto la información que mantiene para sí mismo). Pero es insoslayable que el contacto permanente del ser humano con sus semejantes al interior de la sociedad a la que pertenece, así como todos aquellos avances tecnológicos que han venido desarrollándose en la sociedad, han comenzado a transgredir aquellos hábitos que forman parte de la intimidad el ser humano.

Al tratarse de un derecho con un carácter abierto y dinámico que está frente a la sociedad donde la informática se ha convertido en el símbolo emblemático de la cultura actual.

Cada ciudadano fichado en un banco de datos se halla expuesto a una vigilancia continua e inadvertida que afecta potencialmente, incluso en los aspectos más sensibles de su vida privada, a aquellos que en épocas anteriores quedaban fuera de todo control, por su variedad y multiplicidad, y que hoy, además de tomar conciencia de ello, comienzan a exigir un reconocimiento sobre el uso y control de sus datos.

La protección de la intimidad frente a la informática no significa impedir el proceso electrónico de informaciones, necesarias en el funcionamiento de cualquier Estado moderno, sino el aseguramiento de un uso democrático de la Información Tecnológica.

El derecho a la intimidad a la protección de datos personales.

El **derecho a la intimidad** abarca aquello que se considera más propio y oculto del ser humano (entendiéndose por propio y oculto la información que mantiene para sí mismo). Pero es insoslayable que el contacto permanente del ser humano con sus semejantes al interior de la sociedad a la que pertenece, así como todos aquellos avances tecnológicos que han venido desarrollándose en la sociedad, han comenzado a transgredir aquellos hábitos que forman parte de la intimidad el ser humano.

Al tratarse de un derecho con un carácter abierto y dinámico que está frente a la sociedad donde la informática se ha convertido en el símbolo emblemático de la cultura actual.

Cada ciudadano fichado en un banco de datos se halla expuesto a una vigilancia continua e inadvertida que afecta potencialmente, incluso en los aspectos más sensibles de su vida privada, a aquellos que en épocas anteriores quedaban fuera de todo control, por su variedad y multiplicidad, y que hoy, además de tomar conciencia de ello, comienzan a exigir un reconocimiento sobre el uso y control de sus datos.

La protección de la intimidad frente a la informática no significa impedir el proceso electrónico de informaciones, necesarias en el funcionamiento de cualquier Estado moderno, sino el aseguramiento de un uso democrático de la Información Tecnológica.

Marco normativo

DECLARACIÓN UNIVERSAL DE LOS DERECHOS HUMANOS

PUNTOS RELEVANTES.

Se creo el 10 de diciembre de 1948

ARTICULO 2.

1.- Toda persona tiene todos los derechos y libertades proclamados en esta Declaración sin distinción alguna de raza, posición económica, nacimiento o cualquier otra condición.

2.- Además, no se hará distinción alguna fundada en la condición política, jurídica o internacional del país o territorio bajo administración fiduciaria, no autónomo sometido a cualquier otra limitación de soberanía.

ARTÍCULO 19. Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones y de difundirlas sin limitación de fronteras, por cualquier medio de expresión.

Marco normativo

PACTO INTERNACIONAL DE DERECHOS CIVILES Y POLÍTICOS

Tiene relación al reconocimiento de la Dignidad inherente a todos los miembros de la familia humana y de sus derechos iguales e inalienables (igual que en la declaración Universal de los Derechos Humanos).

ARTÍCULO 2:
Cada uno de los Estados Partes en el Presente pacto se compromete a respetar y a garantizar a todos los individuos que se encuentren en su territorio y estén sujetos a su jurisdicción, los derechos reconocidos en el presente pacto, sin idioma, religión, opinión política o de otra índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición.

ARTICULO 16:
Todo ser humano tiene derecho, en todas partes, al reconocimiento de su personalidad Jurídica.

ARTÍCULO 17:
1.- Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.
2.- Toda persona tiene derecho a la Protección de la Ley contra esas injerencias o esos ataques.

ARTÍCULO 18:
1.- Toda persona tiene derecho a la libertad de pensamiento, de conciencia y de religión; este derecho incluye
la libertad de tenerlo de adoptar la religión o sus creencias, individual o colectivamente, tanto en público como en privado mediante el culto, la celebración de rito, las prácticas y las enseñanzas.

Marco normativo

CONVENCIÓN AMERICANA SOBRE DERECHOS HUMANOS

"PACTO DE SAN JOSÉ DE COSTA RICA"

CAPITULO II.- DERECHOS CIVILES Y POLÍTICOS

ARTÍCULO 4.- DERECHO A LA VIDA

Toda persona tiene derecho a que se respete su vida, Este derecho estará protegido por la ley y, en general, a partir del momento de la concepción. Nadie puede ser privado de la vida arbitrariamente.

ARTÍCULO 5.- DERECHO A LA INTEGRIDAD PERSONAL

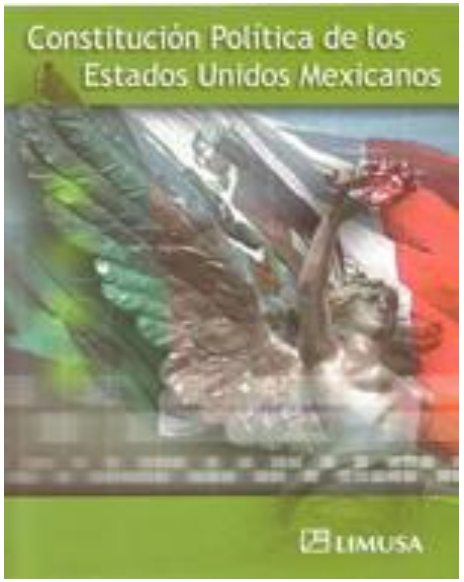
Toda persona tiene derecho a que se respete su integridad física, psíquica y moral.

ARTÍCULO 11.- PROTECCIÓN A LA HONRA Y DE LA DIGNIDAD

Toda persona tiene derecho al respeto de su honra y el reconocimiento de su dignidad.
Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.
Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

Marco normativo

CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS



Artículo 6° .- La manifestación de las ideas no serán objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, los derechos de tercero, provoque algún delito, o perturbe el orden público; el derecho de réplica será ejercido en los términos dispuestos por la ley. El derecho a la información será garantizado por el Estado,

Para el ejercicio del derecho de acceso a la información, la Federación, los Estados y el Distrito Federal, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases:

I.- Toda la información en posesión de cualquier autoridad, entidad, organismo federal, estatal y municipal, es pública y sólo podrá ser reservada temporalmente por razones de interés público en los términos que fijen las leyes. En la interpretación de este derecho deberá prevalecer el principio de máxima publicidad.

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.

Marco normativo

III.- Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos.

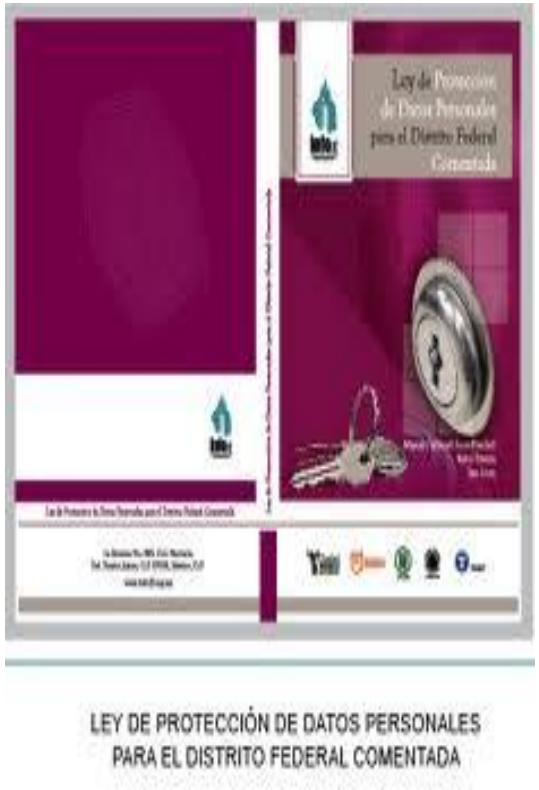
IV.- Se establecerán mecanismos de acceso a la información y procedimientos de revisión expeditos. Estos procedimientos se sustanciarán ante órganos u organismos especializados e imparciales, y con autonomía operativa, de gestión y de decisión.

V.- Los sujetos obligados deberán preservar sus documentos en archivos administrativos actualizados y publicarán a través de los medios electrónicos disponibles, la información completa y actualizada sobre sus indicadores de gestión y el ejercicio de los recursos públicos.

VI.- Las leyes determinarán la manera en que los sujetos obligados deberán hacer pública la información relativa a los recursos públicos que entreguen a personas físicas o morales.

VII.- La inobservancia a las disposiciones en materia de acceso a la información pública será sancionada en los términos que dispongan las leyes.

Marco normativo



RELACIÓN CON EL ARTÍCULO 3° DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES PARA EL DISTRITO FEDERAL

Art. 3.- La interpretación de esta Ley se realizará conforme a la Constitución Política de los Estados Unidos Mexicanos, La Declaración Universal de los Derechos Humanos, el pacto Internacional de Derechos Civiles y Políticos, la Convención Americana sobre Derechos Humanos, y demás instrumentos internacionales suscritos y ratificados por el Estado Mexicano y la interpretación que de los mismos hayan realizado los órganos internacionales respectivos.

DE LOS SISTEMAS DE DATOS PERSONALES

IDENTIFICACIÓN DE UN SISTEMA DE DATOS PERSONALES

Se estará en presencia de un sistema de datos personales , si estamos ante un conjunto de datos que se obtienen de un colectivo de personas para el cumplimiento de una finalidad determinada.

Esta finalidad comúnmente, esta estrechamente vinculada al ejercicio de competencias legales y al cumplimiento de funciones administrativas. Entonces, serán las funciones y atribuciones normativas las que requieren que se recabe información personal de los ciudadanos, y darán lugar a la identificación de un sistema de datos personales.

La identificación de los sistemas de datos personales existentes en un ente determinado, debe realizarse a partir de las competencias administrativas, atribuciones normativas o funciones, que justifican el desarrollo de una actividad y la existencia de procesos de gestión pública donde se manejan datos personales.

Un sistema de datos personales se identifica, entonces, por el propósito o finalidad con la que se tratan los datos de carácter personal contenidos en éste, sobre el cual deberán cumplirse las obligaciones contenidas en la Ley y demás normativa aplicable, tales como su registro ante el InfoDF y la adopción de las medidas de seguridad corresponderá a la categoría de datos que el sistema contega.

DE LOS SISTEMAS DE DATOS PERSONALES

EJEMPLO:

* Se cuenta con un sistema de datos en cada Entidad por lo menos de el personal que conforma los Recursos Humanos.

* Sistemas de Datos Personales de los proveedores: como el RFC, Trayectoria académica, ETC.

DE LOS SISTEMAS DE DATOS PERSONALES

Por lo tanto un **sistema de datos personales,** *es un conjunto organizado de datos de carácter personal, cualquiera que sea su soporte organización o acceso, siempre que tenga una estructura que permita un fácil acceso a los datos de una persona determinada.*

A cada Ente público le corresponde determinar a través de su titular o, en su caso responsable que asigne el titular del órgano competente la creación modificación y supresión de sistemas de datos personales de acuerdo a su ámbito de competencia, esta determinación debe ser publicada en la Gaceta Oficial del Distrito Federal.

DE LOS SISTEMAS DE DATOS PERSONALES

Debe ser publicado en la Gaceta Oficial del Distrito Federal.

Se debe incluir cuando menos estos aspectos:

(Art. 7 LPDPDF)

a) La finalidad del sistema de datos personales y los usos previstos para el mismo.
b) Las personas o grupos de personas sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.
c) El procedimiento de recolección de los datos de carácter personal.
d) La estructura básica del sistema de datos personales y la descripción de los tipos de datos incluidos en el mismo.
e) De la cesión de las que pueden ser objeto los datos.
f) Las instancias responsables del tratamiento del sistema de datos personales.
g) La unidad administrativa ante la que podrán ejercitarse los derechos de acceso, rectificación, cancelación u oposición.
h) El nivel de protección exigible.

Cuando exista una modificación se deberá publicar en la Gaceta Oficial indicando cuáles de éstos aspectos fueron modificados.

Cuando exista supresión del sistema se deberá indicar el destino que tendrán los datos contenidos en los mismos y las medidas previstas para su destrucción.

DE LOS SISTEMAS DE DATOS PERSONALES

DATOS SENSIBLES

Son aquellos que por su propia naturaleza impulsan a la persona a la más absoluta reserva de dicha información y suponen que su divulgación, le coloque en una situación de vulnerabilidad en el entorno social o familiar. **La salud, la sexualidad, la ideología política, así como las creencias religiosas** son consideradas como datos sensibles que se colocan en la esfera íntima del ser humano y que sólo el titular del dato puede divulgar.

DE LOS SISTEMAS DE DATOS PERSONALES MEDIDAS DE SEGURIDAD

Los entes públicos están obligados a adoptar medidas de seguridad por el hecho de contar con sistemas de datos personales y realizar el tratamiento de datos, tanto de particulares como de servidores públicos.

Las medidas de seguridad se encuentran reguladas en el Capítulo III de la Ley de Protección de Datos Personales para el Distrito Federal y en el Capítulo segundo de los lineamientos para la Protección de Datos Personales en el Distrito Federal.

Dichas medidas deberán tomar en consideración las recomendaciones, que en su caso, emita el Instituto, con el objeto de garantizar la confidencialidad, integridad y disponibilidad de los datos personales durante su tratamiento.

DE LOS SISTEMAS DE DATOS PERSONALES MEDIDAS DE SEGURIDAD

Las medidas de seguridad previstas en la Ley revisten dos características principales:

1)Se trata .de medidas que constituyen mínimos exigibles, por lo que el ente público deberá observarlas sin perjuicio del estado, la tecnología, la naturaleza de los datos almacenados y los riesgos a los que están expuestos. El ente público debe adoptar las medidas adicionales que estime necesarias para garantizar la protección y resguardo de la información.

2)Las medidas son acumulativas, es decir, el nivel medio implica la adopción de medidas de seguridad descritas en este nivel, más las dispuestas para el nivel básico. Las de nivel alto, implican la adición de las medidas definidas para los tres niveles (básico, medio y alto)

DE LOS SISTEMAS DE DATOS PERSONALES MEDIDAS DE SEGURIDAD

REQUISITOS DE LAS MEDIDAS DE SEGURIDAD

ART. 13 LPDPDF párrafo tercero:

Nombre y cargo del servidor público, en su caso, la persona física o moral que intervengan en el tratamiento de datos personales o usuario, según corresponda.

Para la actualización o modificación se notificará al Instituto dentro de los 30 días hábiles siguientes a la fecha que se efectuó.

Establecerán las medidas de seguridad técnica y organizativa para garantizar la confidencialidad.

Las medidas se tomarán en cuenta con relación al mayor o menor grado de protección que ameriten los datos personales.

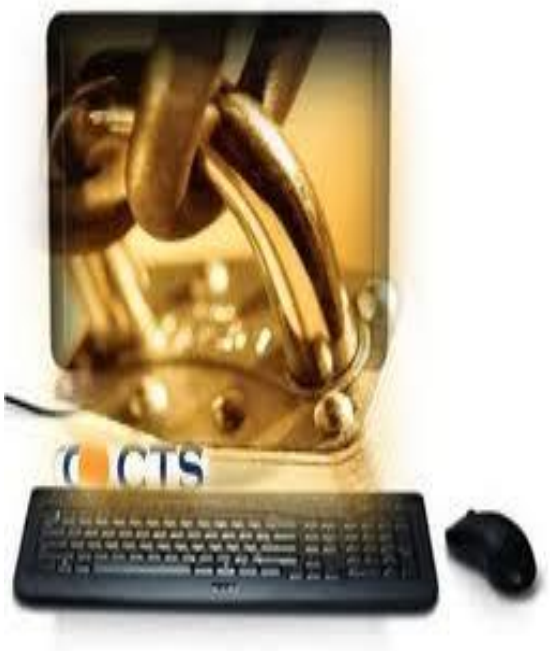
DE LOS SISTEMAS DE DATOS PERSONALES NIVELES DE SEGURIDAD (ART. 14 LPDPDF)

TIPOS DE SEGURIDAD

FÍSICA.- 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.

LÓGICA.- Se refiere a las medidas de protección que permiten la identificación autentificación de las personas o usuarios autorizados para el tratamiento de los datos personales de acuerdo con su función.

DE DESARROLLO Y APLICACIONES.- Las autorizaciones con las que deberá contar la creación o tratamiento de sistemas de datos personales, previendo la participación del usuario y uso de los datos, la separación de entornos, la metodología a seguir, ciclos de vida y gestión, así como consideraciones especiales respecto de aplicaciones y pruebas.



DE CIFRADO.- Consiste en la implementación de algoritmos, claves, contraseñas, así como dispositivos concretos de protección que garanticen la integridad y confidencialidad de la información; y

DE COMUNICACIÓN Y REDES.- Se refiere a las restricciones preventivas y/o de riesgos que deberá 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.

DE LOS SISTEMAS DE DATOS PERSONALES NIVELES DE SEGURIDAD:

BÁSICO.- Su aplicación es obligatoria para todos los sistemas de datos personales y comprende los siguientes aspectos:

A) Documento de seguridad.

El responsable elaborará, difundirá e implementará la normativa de seguridad mediante el documento de seguridad que será de observancia obligatoria para todos los servidores públicos del ente público, así como para toda aquella persona que debido a la presentación de un servicio tenga acceso a los sistemas de datos personales y/o al sitio donde se ubican los mismos.

1) Nombre del sistemas;
2) Cargo y adscripción del responsable;
3) Ámbito de aplicación;
4) Estructura y descripción del sistema de datos personales;
5) Especificación detallada de la categoría de datos personales contenidos en el sistema;
6) Funciones y obligaciones del personal que intervenga en el tratamiento de los sistemas de datos personales;
7) Medidas, normas, procedimientos y criterios enfocados a garantizar el nivel de seguridad exigido;
8) Procedimientos de notificación, gestión y respuesta ante incidencias;
9) Procedimiento para la realización de copias de respaldo y recuperación de los datos, para los sistemas de datos personales automatizados; y
10) Procedimientos para la realización de auditorías, en sus caso.

DE LOS SISTEMAS DE DATOS PERSONALES NIVELES DE SEGURIDAD

B) Funciones y obligaciones del responsable, encargado y de toda persona que intervenga en el tratamiento de los sistemas de datos personales.

Deben estar claramente definidas en el documento de seguridad. El responsable adoptará las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones, así como las responsabilidades y consecuencias en que pudiera incurrir en caso de incumplimiento.

C) Registro de incidencias

Los procedimientos de notificación gestión y respuesta ante incidencias contarán necesariamente con un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación a quien se le comunica, los efectos que se hubieran derivado de la misma y las acciones implementadas.

D) Identificación y autentificación

El responsable tendrá a su cargo la elaboración de una relación actualizada de servidores públicos que tengan acceso autorizado al sistema de datos personales y de establecer procedimientos que permitan la correcta identificación y autenticación para dicho acceso.

DE LOS SISTEMAS DE DATOS PERSONALES NIVELES DE SEGURIDAD:

E) Control de Acceso

El responsable deberá adoptar medidas para que los encargados y usuarios tengan acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.

El responsable deberá mantener actualizada una relación de personas autorizadas y los accesos autorizados para cada una de ellas. Asimismo, deberá establecer los procedimientos para el uso de bitácoras respecto de las acciones cotidianas llevadas a cabo en el sistema de datos personales.

Solamente el responsable podrá conceder, alterar o anular la autorización para el acceso a los sistemas de datos personales.

F) Gestión de soportes

Al almacenar los soportes físicos y electrónicos que contengan datos de carácter personal se deberá cuidar que estén etiquetados para permitir el tipo de información que contienen, ser inventariados y sólo podrán ser accesibles por el personal autorizado para ello en el documento de seguridad.

La salida de soportes y documentos que contengan datos de carácter personal, fuera de las instalaciones u oficinas bajo el control de responsable, deberá ser autorizada en el documento de seguridad.

G) Copias de respaldo y recuperación

Deberán establecerse procedimientos para la realización de copias de respaldo y su periodicidad. En caso de que los datos personales se encuentren en soporte físico, se procurará que el respaldo se efectúe mediante la digitalización de los documentos.

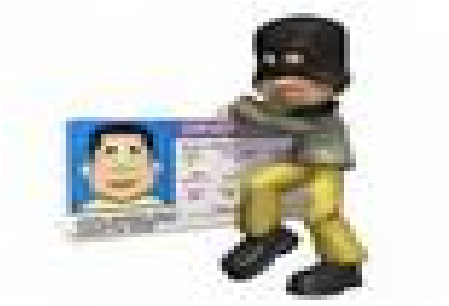
Para soportes electrónicos se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida involuntaria o destrucción accidental.

DE LOS SISTEMAS DE DATOS PERSONALES NIVELES DE SEGURIDAD

NIVEL MEDIO

Nivel Medio.- El nivel de seguridad medio es aplicable a los sistemas de datos personales relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, datos patrimoniales, así como a los sistemas que contengan datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo.

Este nivel de seguridad, de manera adicional a las medidas calificadas como básicas, considera los siguientes aspectos :



DE LOS SISTEMAS DE DATOS PERSONALES NIVELES DE SEGURIDAD

NIVEL MEDIO

a) Responsable de seguridad.

El responsable designará uno o varios responsables de seguridad para coordinar y controlar las medidas definidas en el documento de seguridad. Esta designación podrá ser única para todos los sistemas de datos en posesión del ente público, o diferenciada, dependiendo de los métodos de organización y tratamiento de los mismos. En todo caso dicha circunstancia deberá especificarse en el documento de seguridad.

b) Auditoría

Las medidas de seguridad implementadas para la protección de los sistemas de datos personales se someterán a una auditoría interna o externa, mediante la que se verifique el cumplimiento de la Ley, de los presentes lineamientos y demás procedimientos vigentes en materia de seguridad de datos al menos, cada dos años.

El informe de resultados de la auditoría deberá dictaminar sobre la adecuación de las medidas de seguridad previstas en los Lineamientos, así como en las recomendaciones, que en su caso haya emitido el Instituto, además, deberá identificar sus deficiencia y proponer las medidas preventivas, correctivas o complementarias necesarias.

El informe de auditoría deberá ser comunicado por el responsable al Instituto dentro de los 20 días siguientes a su emisión. Asimismo, se deberá informar al instituto de la adopción de las medidas correctivas derivadas de la auditoría en el plazo referido, a partir de que estas hayan sido atendidas.

c) Control de acceso físico

El acceso a las instalaciones donde se encuentren los sistemas de datos personales, ya sea en soporte físico o electrónico, deberá permitirse exclusivamente a quienes están expresamente autorizados en el documento de seguridad.

d) Pruebas con datos reales.

Las pruebas que se lleven a cabo con efecto de verificar la correcta aplicación y funcionamiento de los procedimientos para la obtención de copias de respaldo y de recuperación de los datos, anteriores a la implantación modificación de los sistemas informáticos que traten sistemas de datos personales, no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tipo de datos tratados. Si se realizan pruebas con datos reales, se elaborará con anterioridad una copia de respaldo.

DE LOS SISTEMAS DE DATOS PERSONALES NIVELES DE SEGURIDAD

Nivel Alto.- Es aplicable a los sistemas de datos de carácter personal se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su traslado o transmisión.

El nivel de seguridad alto, además de incorporar las medidas de nivel básico y medio, deberán completar las que se detallan a continuación:

DE LOS SISTEMAS DE DATOS PERSONALES NIVELES DE SEGURIDAD

a)Distribución de soportes:

La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos, o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulable por terceros.

b)Registro de acceso:

El acceso a los sistemas de datos personales se limitará exclusivamente al personal autorizado, estableciendo mecanismos que permitan identificar los accesos realizados en el caso en que los sistemas puedan ser utilizados por múltiples autorizados.

Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad correspondiente, si que se permita la desactivación o manipulación de los mismos.

De cada acceso se guardarán, al menos, la identificación del usuario, la fecha y hora en que se realizó, el sistema accedido, el tipo de acceso y si éste fue autorizado o denegado.

El periodo de conservación de los datos consignados en el registro de acceso será de, al menos, dos años.

c)Telecomunicaciones

La transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulable por terceros.

GRACIAS POR SU ATENCIÓN

MARÍA CRISTINA PINEDA ARZOLA
SALVADOR CORREA PÉREZ
VÍCTOR MANUEL SASPE SIQUEIROS