Instituto Veracruzano
de acceso a la información
y protección de datos personales

Medidas de seguridad en Protección de Datos Personales

¿Qué son los datos personales?

- La información numérica, alfabética, gráfica, acústica o de cualquier otro tipo concerniente a una persona **física**, **identificada o identificable.**

Regulación

Protección de Datos Personales

En posesión de entes públicos

En posesión de entes privados

Ley General de Protección de Datos Personales en posesión de Sujetos Obligados

Leyes estatales de Protección de Datos (11) (mientras no armonicen)

Ley Federal de Protección de Datos Personales en Posesión Particulares

Tratamiento de Datos Personales

Instrumentos de protección

1) Acuerdo de creación, modificación y supresión de Sistemas de datos personales

2) Declarativa de Privacidad

3) Documento de Seguridad

Su creación es obligatoria aún cuando ya exista la Ley General de datos personales, únicamente cambiaran algunos requisitos.

Deber de seguridad

Aplicación de medidas de seguridad encaminadas a garantizar la confidencialidad, integridad y disponibilidad de éstos, bajo los niveles de protección básico, medio y alto.

Disposiciones Generales

Artículo 6. Para los efectos de la presente Ley, se entiende por:

Sistema de Datos Personales: 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;

Roles

Titular de la Unidad de Transparencia

Responsable del Sistema de Datos Personales

Responsable del Área de Informática

CAPÍTULO VII
Medidas de Seguridad

Artículo 29. Los entes públicos establecerán las medidas de seguridad técnica y organizativa para garantizar la confidencialidad e integridad de cada sistema de datos personales que posean…

… Las medidas serán adoptadas en relación con el menor o mayor grado de protección que ameriten los datos personales, deberán constar por escrito y ser comunicadas al Instituto para su registro…

CAPÍTULO VI
Boletines Judiciales, Listas de Acuerdos y Estrados

Artículo 28. Si la publicación de los datos personales lleva por fin la notificación al titular de un determinado acto, y la notificación se realiza por medios informáticos, digitales o de internet, una vez efectuada aquélla y transcurridos los plazos de ejercicio de los posibles recursos, no se mantendrán dichos datos para su localización a través de los buscadores electrónicos. Al efecto, se dictarán las órdenes oportunas para limitar la indexación del nombre y apellidos de las personas en los mencionados documentos mediante la incorporación de un código **norobot.txt**, con objeto de que los motores de búsqueda de internet no puedan asociarlo al titular.

CAPÍTULO VI
Artículo 28

El archivo robots.txt más simple utiliza dos reglas:

User-Agent: el robot al que se aplica la siguiente regla
Disallow: la URL que quieres bloquear

Ejemplo:

User-Agent:*
Disallow /

- Se trata de un archivo con capacidad técnica para ocultar determinadas páginas de un sitio web, a fin de impedir el acceso automático de los buscadores en Internet.

CAPÍTULO VII
Medidas de Seguridad

Artículo 30. El ente público responsable de la tutela y tratamiento del sistema de datos personales adoptará las medidas de seguridad conforme a lo siguiente:

I. Tipos de seguridad:

a) Física.
b) Lógica.
c) De desarrollo
d) De cifrado.
e) De comunicac

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

CAPÍTULO VII
Medidas de Seguridad

Artículo 30. El ente público responsable de la tutela y tratamiento del sistema de datos personales adoptará las medidas de seguridad conforme a lo siguiente:

I. Tipos de seguridad:

a) Física.
b) Lógica
c) De desarrollo
d) De cifrado.
e) De comunicaci

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

CAPÍTULO VII
Medidas de Seguridad

Artículo 30. El ente público responsable de la tutela y tratamiento del sistema de datos personales adoptará las medidas de seguridad conforme a lo siguiente:

I. Tipos de seguridad:

a) Física.
b) Lógica.
c) De desarrollo y aplicacione
d) De cifrado.
e) De comunicaciones y rec

Autorizaciones con las que deberá contar la creación o tratamiento de sistemas de datos personales 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, así como las consideraciones especiales respecto de aplicaciones y pruebas;

CAPÍTULO VII
Medidas de Seguridad

Artículo 30. El ente público responsable de la tutela y tratamiento del sistema de datos personales adoptará las medidas de seguridad conforme a lo siguiente:

I. Tipos de seguridad:

a) Física.
b) Lógica.
c) De desarrollo y aplic
d) De cifrado
e) De comunicaciones y

Es implementación de algoritmos, claves, contraseñas, así como dispositivos concretos de protección que garanticen la integralidad y confidencialidad de la información

CAPÍTULO VII
Medidas de Seguridad

Artículo 30. El ente público responsable de la tutela y tratamiento del sistema de datos personales adoptará las medidas de seguridad conforme a lo siguiente:

I. Tipos de seguridad:

a) Física.
b) Lógica.
c) De desarrollo y aplicacion
d) De cifrado.
e) De comunicaciones y red

Se refiere a las restricciones preventivas 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.

CAPÍTULO VII
Medidas de Seguridad
ARTÍCULO 30
LDP 5

NIVELES

Básico

Todos los sistemas de datos personales

Medio

Comisión de infracciones administrativas o penales, hacienda pública, servicios financieros, datos patrimoniales

Alto

- Ideología
- Religión
- Creencias
- Afiliación política
- Origen étnico
- Salud
- Biométricos
- Genéticos o vida sexual
- Datos recabados para fines policiales
- De seguridad, Prevención, investigación y persecución de delitos.

CAPÍTULO VII

Medidas de Seguridad

ARTÍCULO 30

LDP-16

NIVELES	MEDIDAS
Básico Todos los sistemas de datos personales	1. Documento de seguridad; 2. Funciones y obligaciones del personal que intervenga en el tratamiento de los sistemas de datos personales; 3. Registro de incidencias; 4. Identificación y autentificación; 5. Control de acceso; 6. Gestión de soportes; 7. Copias de respaldo y recuperación.

CAPÍTULO VII
Medidas de Seguridad
ARTÍCULO 30

NIVELES

Las **funciones y obligaciones** de todos los que intervengan en el tratamiento de datos personales **deben estar claramente definidas en el documento de seguridad**.

El responsable del sistema de datos personales **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.

MEDIDAS

1. Documento de seguridad;
2. Funciones y obligaciones del personal que intervenga en el tratamiento de los sistemas de datos personales;
3. Registro de incidencias;
4. Identificación y autentificación;
5. Control de acceso;
6. Gestión de soportes;
7. Copias de respaldo y recuperación.

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

Nombre	Cargo	Funciones	Obligaciones

CAPÍTULO VII
Medidas de Seguridad
ARTÍCULO 30

NIVELES	MEDIDAS
Básico	1. Documento de seguridad; 2. Funciones y obligaciones del personal que intervenga en el tratamiento de los sistemas de datos personales; 3. Registro de incidencias; 4. Identificación y autentificación; 5. Control de acceso; 6. Gestión de soportes; 7. Copias de respaldo y recuperación.

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 quién se le comunica.
- Los efectos que se hubieran derivado de la misma.
- Las acciones implementadas.

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

Ante cualquier incidente que pudiera suscitarse se debe realizar el siguiente registro:

Descripción de la incidencia	Fecha y hora	Persona que realiza la notificación	Persona que recibe la notificación	Efectos derivados de la incidencia	Acciones implementadas

NIVELES

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

Establecerá un mecanismo que permita la **identificación**, de forma inequívoca y personalizada, de **toda aquella persona que intente acceder al sistema** y la verificación de que está autorizada.

Cuando el mecanismo de autenticación se base en la existencia de contraseñas **se establecerá un procedimiento de asignación, distribución y almacenamiento** que garantice su confidencialidad e integridad.

Las contraseñas se cambiarán con la periodicidad que se determine en el documento de seguridad y se conservarán cifradas.

Se establecerá un **procedimiento de creación** y modificación de contraseñas (longitud, formato, contenido).

MEDIDAS

1. Documento de seguridad;
2. Funciones y obligaciones del personal que intervenga en el tratamiento de los sistemas de datos personales;
3. Registro de incidencias;
4. Identificación y autentificación;
5. Control de acceso;
6. Gestión de soportes;
7. Copias de respaldo y recuperación.

CAPÍTULO VII
Medidas de Seguridad
ARTÍCULO 30

NIVELES	MEDIDAS
Básico	1. Documento de seguridad; 2. Funciones y obligaciones del personal que intervenga en el tratamiento de los sistemas de datos personales; 3. Registro de incidencias; 4. Identificación y autentificación; 5. Control de acceso; 6. Gestión de soportes; 7. Copias de respaldo y recuperación.

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

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

CAPÍTULO VII
Medidas de Seguridad
ARTÍCULO 30

NIVELES

Al almacenar los soportes físicos y electrónicos que contengan datos de carácter personal se deberá cuidar que **estén etiquetados** para permitir identificar 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 del responsable del sistema de datos personales, **deberá ser autorizada** por éste, o encontrarse debidamente autorizada en el documento de seguridad. En **el traslado de soportes físicos y electrónicos** se adoptarán medidas dirigidas **a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.**

Siempre que vaya a desecharse cualquier soporte que contenga datos de carácter personal **deberá procederse a su destrucción o borrado**, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.

MEDIDAS

1. Documento de seguridad;
2. Funciones y obligaciones del personal que intervenga en el tratamiento de los sistemas de datos personales;
3. Registro de incidencias;
4. Identificación y autentificación;
5. Control de acceso;
6. Gestión de soportes;
7. Copias de respaldo y recuperación.

CAPÍTULO VII
Medidas de Seguridad
ARTÍCULO 30

NIVELES

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.

Asimismo, 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.

El responsable del sistema de datos personales se encargará de verificar, al menos, cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

MEDIDAS

1. Documento de seguridad;
2. Funciones y obligaciones del personal que intervenga en el tratamiento de los sistemas de datos personales;
3. Registro de incidencias;
4. Identificación y autentificación;
5. Control de acceso;
6. Gestión de soportes;
7. Copias de respaldo y recuperación.

CAPÍTULO VII
de Seguridad
CULO 30
DP-16

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

Deberá contener, como mínimo:

I. Nombre del sistema;
II. Cargo y adscripción del responsable del sistema de datos personales;
III. Ámbito de aplicación;
IV. Estructura y descripción del sistema de datos personales;
V. Especificación detallada de la categoría de datos 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.
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 automatizados;
X. Procedimientos para la realización de auditorías, en su caso.

El documento de seguridad deberá **actualizarse anualmente** o cuando se produzcan cambios relevantes en el tratamiento, que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas.

MEDIDAS

1. Documento de seguridad;
2. Funciones y obligaciones del personal que intervenga en el tratamiento de los sistemas de datos personales;
3. Registro de incidencias;
4. Identificación y autentificación;
5. Control de acceso;
6. Gestión de soportes;
7. Copias de respaldo y recuperación.

CAPÍTULO VII
Medidas de Seguridad
ARTÍCULO 30

NIVELES	MEDIDAS
Básico Todos los sistemas de datos personales	1. Documento de seguridad; 2. Funciones y obligaciones del personal que intervenga en el tratamiento de los sistemas de datos personales; 3. Registro de incidencias; 4. Identificación y autentificación; 5. Control de acceso; 6. Gestión de soportes; 7. Copias de respaldo y recuperación.
	8. Responsable de seguridad; 9. Auditoría; 10. Control de acceso físico; 11. Pruebas con datos reales.

El responsable del sistema de datos personales **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.

En ningún caso esta designación supone una delegación de las facultades y atribuciones que corresponden al responsable del sistema de datos personales de acuerdo con la Ley y los Lineamientos.

CAPÍTULO VII
Medidas de Seguridad
ARTÍCULO 30

NIVELES

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 Lineamientos** y demás procedimientos vigentes en materia de seguridad de datos, al menos, cada dos años. La auditoría interna podrá realizarse a través del órgano de control interno del ente público.

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 deficiencias y proponer las medidas preventivas, correctivas o complementarias necesarias.

El informe de auditoría deberá ser comunicado por el responsable del sistema de datos personales al Instituto dentro de los veinte días hábiles 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 éstas hayan sido atendidas.

MEDIDAS

1. Documento de seguridad;
2. Funciones y obligaciones del personal que intervenga en el tratamiento de los sistemas de datos personales;
3. Registro de incidencias;
4. Identificación y autentificación;
5. Control de acceso;
6. Gestión de soportes;
7. Copias de respaldo y recuperación.
8. Responsable de seguridad;
9. Auditoría;
10. Control de acceso físico;
11. Pruebas con datos reales.

CAPÍTULO VII
Medidas de Seguridad
ARTÍCULO 30

NIVELES	MEDIDAS
Básico Todos los sistemas de datos personales	1. Documento de seguridad; 2. Funciones y obligaciones del personal que intervenga en el tratamiento de los sistemas de datos personales; 3. Registro de incidencias; 4. Identificación y autentificación; 5. Control de acceso; 6. Gestión de soportes; 7. Copias de respaldo y recuperación.
Medio	8. Responsable de seguridad; 9. Auditoría; 10. Control de acceso físico; 11. Pruebas con datos reales.

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 estén expresamente autorizados en el documento de seguridad.**

CAPÍTULO VII
Medidas de Seguridad
ARTÍCULO 30

NIVELES	MEDIDAS
Básico Todos los sistemas de datos personales	1. Documento de seguridad; 2. Funciones y obligaciones del personal que intervenga en el tratamiento de los sistemas de datos personales; 3. Registro de incidencias; 4. Identificación y autentificación; 5. Control de acceso; 6. Gestión de soportes; 7. Copias de respaldo y recuperación.
Medio	8. Responsable de seguridad; 9. Auditoría; 10. Control de acceso físico; 11. 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 o 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.

CAPÍTULO VII

Medidas de Seguridad

ARTÍCULO 30

NIVELES	MEDIDAS
Básico Todos los sistemas de datos personales	1. Documento de seguridad; 2. Funciones y obligaciones del personal que intervenga en el tratamiento de los sistemas de datos personales; 3. Registro de incidencias; 4. Identificación y autentificación; 5. Control de acceso; 6. Gestión de soportes; 7. Copias de respaldo y recuperación.
Medio Datos relativos a la comisión de infracciones administrativas o penales, hacienda pública, servicios financieros, datos patrimoniales	8. Responsable de seguridad; 9. Auditoría; 10. Control de acceso físico; 11. Pruebas con datos reales.
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 manipulada durante su traslado o transmisión. prevención, investigación y persecución de delitos.	12. Distribución de soportes; 13. Registro de acceso; y 14. Telecomunicaciones.

CAPÍTULO VII
Medidas de Seguridad
ARTÍCULO 30

NIVELES

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

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

De cada acceso se guardarán:

- 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.

MEDIDAS

1. Documento de seguridad;
2. Funciones y obligaciones del personal que intervenga en el tratamiento de los sistemas de datos personales;
3. Registro de incidencias;
4. Identificación y autentificación;
5. Control de acceso;
6. Gestión de soportes;
7. Copias de respaldo y recuperación.
8. Responsable de seguridad;
9. Auditoría;
10. Control de acceso físico;
11. Pruebas con datos reales.
12. Distribución de soportes;
13. Registro de acceso; y
14. Telecomunicaciones.

CAPÍTULO VII
Medidas de Seguridad
ARTÍCULO 30

NIVELES	MEDIDAS
Básico Todos los sistemas de datos personales	1. Documento de seguridad; 2. Funciones y obligaciones del personal que intervenga en el tratamiento de los sistemas de datos personales; 3. Registro de incidencias; 4. Identificación y autentificación; 5. Control de acceso; 6. Gestión de soportes; 7. Copias de respaldo y recuperación.
Medio Datos relativos a la comisión de infracciones administrativas o penales, hacienda pública, servicios financieros, datos patrimoniales	8. Responsable de seguridad; 9. Auditoría; 10. Control de acceso físico; 11. Pruebas con datos reales.
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.	12. Distribución de soportes; 13. Registro de acceso; y 14. Telecomunicaciones.

CAPÍTULO VII

Medidas de Seguridad

ARTÍCULO 30

NIVELES	MEDIDAS
Básico Todos los sistemas de datos personales	1. Documento de seguridad; 2. Funciones y obligaciones del personal que intervenga en el tratamiento de los sistemas de datos personales; 3. Registro de incidencias; 4. Identificación y autentificación; 5. Control de acceso; 6. Gestión de soportes; 7. Copias de respaldo y recuperación.
Medio Datos relativos a la comisión de infracciones administrativas o penales, hacienda pública, servicios financieros, datos patrimoniales	8. Responsable de seguridad; 9. Auditoría; 10. Control de acceso físico; 11. Pruebas con datos reales.
Alto Datos concernientes a la ideología, religión, creencias, afiliación política, origen étnico, salud, biométricos, genéticos o vida sexual, así como los que contengan datos recabados para fines policiales, de seguridad, prevención, investigación y persecución de delitos.	12. Distribución de soportes; 13. Registro de acceso; y 14. Telecomunicaciones.

CAPÍTULO VII
Medidas de Seguridad

Artículo 31. Las medidas de seguridad de los datos personales tratados en bases de datos almacenadas o soportadas en sistemas informáticos deberán ser analizadas y establecidas por medio del Comité de Transparencia a que se refiere el artículo 130 de la Ley de Transparencia y Acceso a la Información Pública para el Estado, que se constituirá como el Comité para la Seguridad Informática de los Datos Personales.

CAPÍTULO VII
Medidas de Seguridad

Artículo 32. El responsable del área informática de cada ente público deberá integrarse de manera obligatoria al Comité para la Seguridad Informática de los Datos Personales, el que deberá:

Artículo 32

Plan de Contingencia Informático para la preservación de la Información

Sistema de Gestión de la Seguridad de la Información

Elaborar análisis de riesgos de TICs

Desarrollar metodologías y procesos específicos relativos a la seguridad y privacidad de la información

Desarrollar proceso de Admon. de la continuidad de las operaciones de las TICs ante la presencia de incidentes relativos a la seguridad de la información

Proponer al Comité, la política de seguridad de la información y sus objetivos, así como observar el cumplimiento de los mismos

Establecer, operar, monitorear, mantener y mejorar un sistema de administración de seguridad de la información

Monitorear cambios significativos en los riesgos que afectan a los recursos de información

Garantizar que la seguridad sea parte del proceso de planificación de la información

Conformar grupos de trabajo que permitan garantizar la seguridad y privacidad de los entes públicos

Promover la difusión de la cultura de seguridad y privacidad de la información dentro del EP

CAPÍTULO VII
Medidas de Seguridad
Artículo 33

Manual Administrativo de Aplicación General en las materias de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información

ISO/IEC 27001

ISO/IEC 27005

CAPÍTULO VII
Medidas de Seguridad

Artículo 33. Las medidas de seguridad a las que se refiere el presente Capítulo constituyen mínimos exigibles, por lo que el ente público adoptará las medidas adicionales que estime necesarias…

Por la naturaleza de la información, las medidas de seguridad que se adopten serán consideradas confidenciales y únicamente se comunicará al Instituto, para su registro, el nivel de seguridad aplicable.

Los entes públicos podrán hacer referencia a estándares, normas, marcos de referencia y buenas prácticas estatales, nacionales e internacionales…

Ley General de Protección de Datos Personales en posesión de Sujetos Obligados

- Publicada en el Diario Oficial de la Federación del 26 de enero de 2017, con lo que se establece reglas comunes en toda la republica mexicana.

- Las leyes estatales deberán ajustarse en un plazo de 6 meses

Innovaciones en la Ley General

Tipos de medidas

- Administrativas
- Físicas
- Técnicas

Materialización

- Documento de seguridad
- Sistema de gestión
- Notificación de vulneraciones

Garantizar

- ✓Integridad
- ✓Confidencialidad
- ✓Disponibilidad

Derecho de Portabilidad

El titular puede ejercer ante un responsable (sujeto obligado) el derecho a **obtener sus datos personales en un formato estructurado comúnmente utilizado** (formato electrónico) para su uso posterior.

Empoderamiento del Titular de los Datos Personales

Elección de servicios

Cómputo en la Nube

Posibilidad de que el **RESPONSABLE** haga uso de **servicios externos de cómputo** y de infraestructura (plataformas o programas informáticos) **generalmente disponibles por medio de Internet**, para el almacenamiento, resguardo y tratamiento de datos personales.

Vulneraciones en la Nube

El **responsable** podrá hacer uso de servicios en la nube

Solo si se **garantiza que el proveedor externo cuenta con políticas de protección de datos personales** equivalentes a los principios y deberes establecidos en la Ley.

Esquema de acciones preventivas

Esquemas de **mejores prácticas** previstos en la Ley

Evaluaciones de Impacto ante un **tratamiento intensivo** o relevante de datos personales

Los organismos garantes podrán emitir recomendaciones no vinculantes especializadas en la materia.

Figura del **Oficial de Protección de Datos**

Privacidad por diseño = *Cumplimiento*

Mtra. Ivonne Flores Olivos
Responsable de la Oficina de Desarrollo de Sistemas
iflores.ivai@Outlook.com ext. 211
Mtra. Irma Rodríguez Ángel
Directora de Datos Personales
irodriguez@verivai.org.mx ext. 406

Cirilo Celis Pastrana s/n. esq. Av. Lázaro Cárdenas, col. Rafael Lucio
C.P. 91110, Xalapa, Ver. Tel: 01 (228) 8420270
www.ivai.org.mx

Ivai Veracruz
@VERIVAI
Ivai Veracruz