GOBIERNO DE LA CIUDAD DE MÉXICO | SECRETARÍA DE LA CONTRALORÍA GENERAL

Sistemas de Datos Personales

y sus principales obligaciones

Objetivo General

Al finalizar el curso, el alumno conocerá las principales obligaciones que debe llevar a cabo el responsable de un sistema de datos personales, conforme a la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México.

Contenido del curso

1. DEFINICIONES

1.1 Dato Personal

1.2 Tipos y categorías de Datos Personales

1.3 Tratamiento de Datos Personales

1.4 Sistemas de Datos Personales

1.5 Principios de la Protección de Datos Personales

1.6 Personas involucradas en materia de Datos Personales

Contenido del curso

2. OBLIGACIONES DE LOS SISTEMAS DE DATOS PERSONALES

2.1 Publicación en Gaceta

2.2 Registro electrónico de Sistemas de Datos Personales

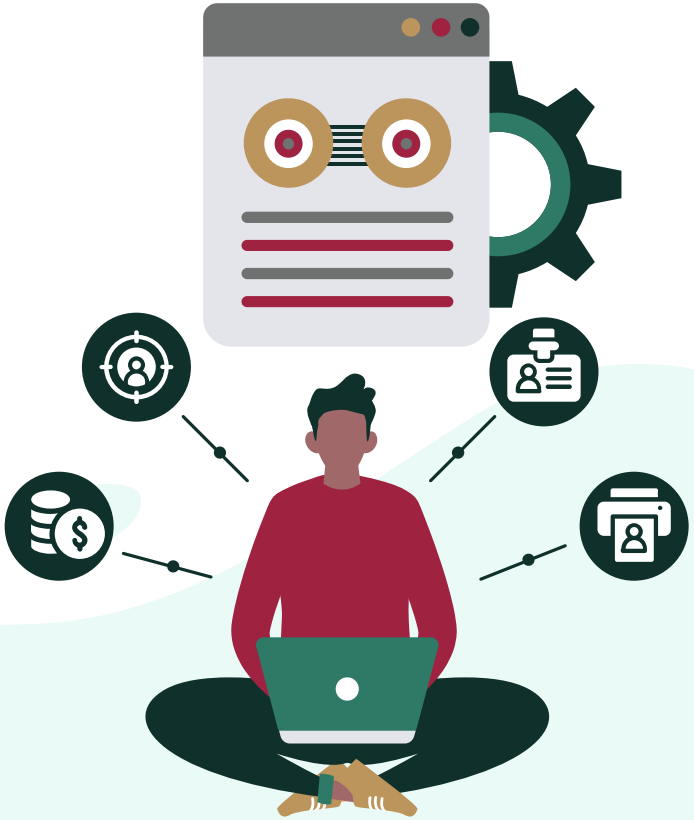
2.3 Aviso de privacidad

2.4 Documento de Seguridad

DEFINICIONES

Dato Personal

Cualquier **información relativa a una persona física identificada o identificable**, considerándose como identificable toda persona cuya identidad pueda determinarse, directa o indirectamente.



Tipos y Categorías de datos personales

Identificación

Nombre, edad, domicilio, estudios, etc.

Financieros

Bienes, cuentas bancarias, información fiscal, reporte de buró de crédito, declaraciones de impuestos

Laborales

Documentos de reclutamiento, nombramiento, incidencias, actividades extracurriculares, hoja de servicio etc.

Electrónicos

La dirección IP, correos electrónicos e incluso la geolocalización, etc.

Patrimoniales

Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, etc.

Procedimientos administrativos y/o jurisdiccionales

Información relativa a una persona que se encuentra sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional

Tipos y Categorías de datos personales

Académicos

Trayectoria educativa, calificaciones, títulos, certificados, etc.

Tránsito y movimientos migratorios

Viajes fuera y dentro del país, así como información migratoria.

Salud

Expediente clínico, referencias o descripción sintomatológicas, detección de enfermedades, etc.

Biométricos

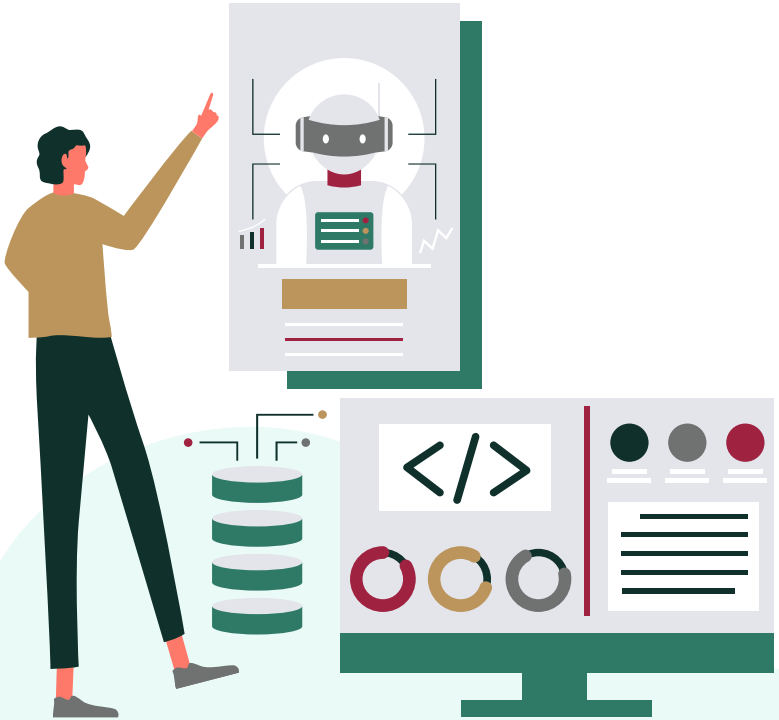
Huellas dactilares, ADN, geometría de la mano, características del iris, forma de caminar, etc.

De naturaleza pública

Aquellos que por mandato legal sean accesibles al público

Sensibles

Origen racial, estado de salud, creencias religiosas, preferencia sexual, datos biométricos.



Tratamiento
de datos personales

Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales.

Sistema de datos personales

Conjunto organizado de archivos, registros, ficheros, bases o bancos de datos personales en posesión de los sujetos obligados.

- **Físicos**: Para su tratamiento están contenidos en registros, documentos impresos, sonoros, magnéticos, visuales u holográficos;

- **Automatizados**: Estos permiten acceder a la información relativa a una persona física utilizando una herramienta tecnológica.

Principios de la Protección de Datos Personales

Calidad

Los datos personales deben ser ciertos, adecuados, pertinentes y proporcionales , no excesivos, en relación con el ámbito y la finalidad para la que fueron recabados.

Confidencialidad

Solo el titular, el Responsable y el usuario puedan acceder a los datos personales, para cumplir con las finalidades del tratamiento. Se deberá garantizar la secrecía y la no difusión de los mismos.

Consentimiento

Manifestación de la voluntad libre, específica e informada del titular de los datos personales para su tratamiento.

Finalidad

Los datos personales recabados y tratados tendrán fines determinados, explícitos y legítimos y no podrán ser tratados ulteriormente con fines distintos para los que fueron recabados

Información

El Responsable deberá informar al titular de los datos personales sobre las características principales del tratamiento, la finalidad y cualquier cambio del estado relacionados con sus datos personales.

Principios de la Protección de Datos Personales

Lealtad

El tratamiento de Datos Personales se realizará sin que medie dolo, engaño o medios fraudulentos, tengan un origen lícito, y no vulneren la confianza del titular.

Licitud

El tratamiento de Datos Personales será lícito cuando el titular los entregue, previo consentimiento o en cumplimiento de una obligación y no serán utilizados para otras finalidades.

Proporcionalidad

El Responsable tratará aquellos Datos Personales que resulten necesarios, adecuados y relevantes en relación con la finalidad, para la cual se obtuvieron.

Transparencia

La información relacionada con el tratamiento de Datos Personales será accesible, fácil de entender y siempre a disposición del titular.

Temporalidad

Los Datos Personales tendrán un ciclo de vida vinculado a la finalidad para la cual fueron recabados y tratados. Concluida su finalidad pueden ser destruidos.

Personas involucradas en materia de Datos Personales

Titular

La persona física a quien corresponden los datos personales.

Responsable

Persona servidora pública que decide sobre el tratamiento de los DP, su finalidad, la protección y las medidas de seguridad de los mismos.

Usuario

Persona autorizada por el responsable e integrante del sujeto obligado, que dé tratamiento y/o tenga acceso a los datos y/o sistema de datos personales.

Encargado

La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable.

Personas involucradas en materia de Datos Personales

Responsable de seguridad

Persona designada por el responsable del SDP a quien le asignan formalmente las funciones de coordinar y supervisar la implementación de las medidas de seguridad aplicables en función de las atribuciones en el tratamientos de los DP.

Oficial de PDP

Especialista en materia de protección de datos personales, adscrito a la Unidad de Transparencia con suficiente jerarquía para implementar las disposiciones de la Ley de Datos y los Lineamientos al interior del sujeto obligado.

Enlace

Persona servidora pública que fungirá como vínculo entre el sujeto obligado y el Instituto para atender los asuntos relativos a la ley en la materia.

Obligaciones de los Responsables de los Sistemas de Datos Personales

Publicación de acuerdos

Creación, Modificación y Supresión

Consentimiento y Aviso de privacidad

Simplificado e Integral

RESDP

Registro Electrónico de Sistemas de Datos Personales
http://datospersonales.infocdmx.org.mx/

Documento de seguridad

Sistema de gestión de seguridad de los datos personales

Publicación de acuerdos de creación modificación y supresión

- Cada sujeto obligado **publicará en la Gaceta Oficial** de la Ciudad de México la **creación, modificación o supresión** de sus sistemas de datos personales; (Artículo 37 Fr I, LPDPPSOCDMX)

- **Creación y modificación,** el acuerdo deberá dictarse y publicarse **previamente a la creación o modificación** del sistema de datos personales correspondientes, y

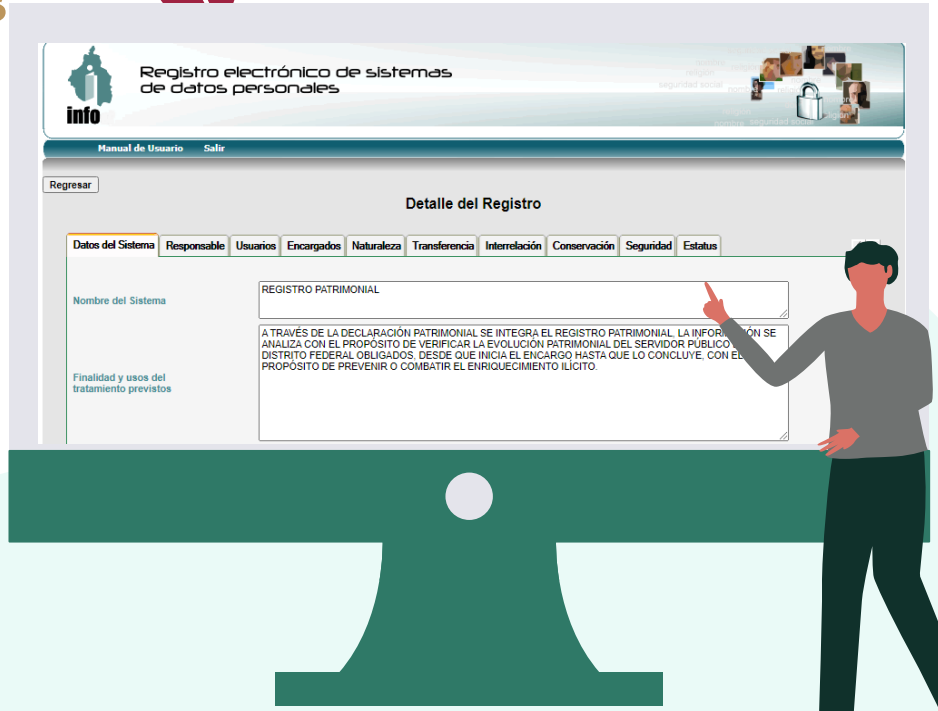
- **Supresión**, deberá publicarse al menos, **treinta días hábiles previos a la supresión** del sistema de que se trate. (Artículo 66, LGPDPPSOCDMX)

Elementos que se debe incluir en los acuerdos

a) La **finalidad o finalidades** de los sistemas de datos personales; así como los **usos** y **transferencias** previstos;
b) Las **personas físicas o grupos de personas** sobre las que se recaben o traten datos personales;
c) La estructura básica del sistema de datos personales y la descripción de los **tipos de datos** incluidos;
d) Las **instancias responsables** del tratamiento del sistema de datos personales: titular del sujeto obligado, usuarios y encargados, si los hubiera;
e) Las **áreas** ante las que podrán **ejercerse** los derechos **de acceso, rectificación, cancelación y oposición;**
f) El **procedimiento** a través del cual se podrán ejercerse los derechos de acceso, rectificación, cancelación y oposición; y
g) El **nivel de seguridad** y los **mecanismos de protección**.

RESDP
Registro Electrónico de Sistemas de Datos Personales

Todo acuerdo de modificación que afecte la integración y tratamiento de un sistema de datos personales también deberá ser inscrito por el Responsable en el Registro de Sistemas de Datos Personales, **dentro los diez días hábiles siguientes a su publicación.**



http://datospersonales.infocdmx.org.mx/

Elementos que podemos modificar sin necesidad de publicar en gaceta

NORMATIVIDAD

Denominación de la norma, la fecha de publicación, fecha de última reforma, artículos y fracciones.

Elementos que podemos modificar sin necesidad de publicar en gaceta

DATOS DEL RESPONSABLE

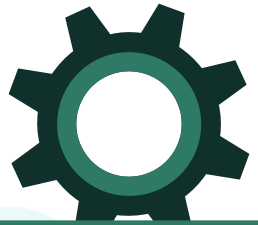
Nombre, domicilio, teléfono y correo electrónico

Elementos que podemos modificar sin necesidad de publicar en gaceta

DATOS DE LOS USUARIOS

Nombres

Elementos que podemos modificar sin necesidad de publicar en gaceta



INTERRELACIÓN

Sistemas del mismo Sujeto Obligado con los que comparte datos personales

Elementos que podemos modificar sin necesidad de publicar en gaceta

TIEMPO DE CONSERVACIÓN

Temporalidad de conservación en archivo de trámite y archivo de concentración.

Consentimiento

Manifestación de la voluntad **libre, específica e informada** del titular de los datos personales para su tratamiento.

Para la obtención del consentimiento, el responsable deberá facilitar al titular un medio sencillo y gratuito a través del cual pueda manifestar su voluntad, mismo que deberá permitir acreditar que de manera indubitable y, **documentar que el titular otorgó su consentimiento** ya sea a través de una declaración o una acción afirmativa clara.

El silencio, las casillas previamente marcadas, la inacción del titular o cualquier otra conducta o mecanismo similar a los mencionados **no podrán considerarse como consentimiento del titular.**

Aviso de privacidad

El responsable deberá informar al titular, a través del aviso de privacidad, la existencia y características principales del tratamiento previo a que sus datos personales sean recolectados

Aviso de privacidad

¿Cuándo y dónde se ponen a disposición del Titular de los datos personales?

Simplificado

- De manera **previa a la obtención** de los datos personales, cuando los mismos se obtengan directamente del titular, independientemente de los formatos o medios físicos y/o electrónicos utilizados para tal fin, o

- **Al primer contacto con el titular o previo al aprovechamiento** de los datos personales, cuando éstos se hubieren obtenido de manera indirecta del titular.

Integral

- Deberá estar **publicado, de manera permanente**, en el sitio o medio que se informe en el aviso de privacidad simplificado, a efecto de que el titular lo consulte en cualquier momento.

Aviso de Privacidad Simplificado

Artículo 21 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México

El aviso simplificado deberá contener la siguiente información:

Denominación del **responsable**

Finalidades

Transferencias

Mecanismos y medios para que el titular pueda **manifestar su negativa**

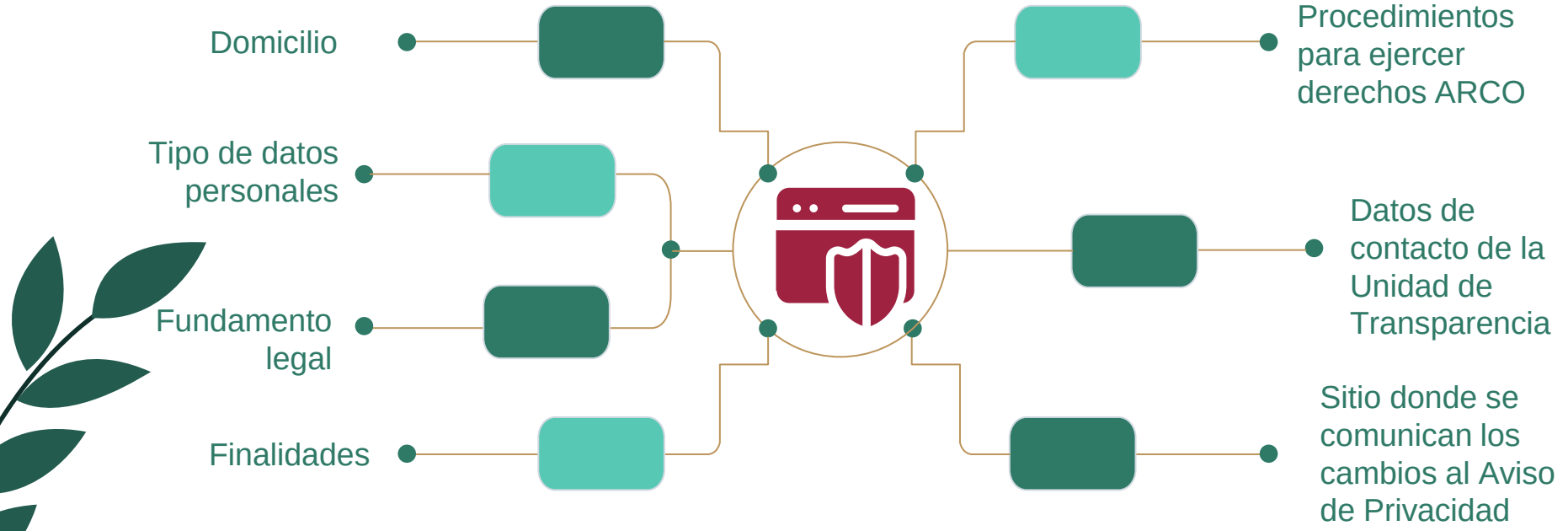
Sitio donde se podrá consultar el **aviso de privacidad integral**

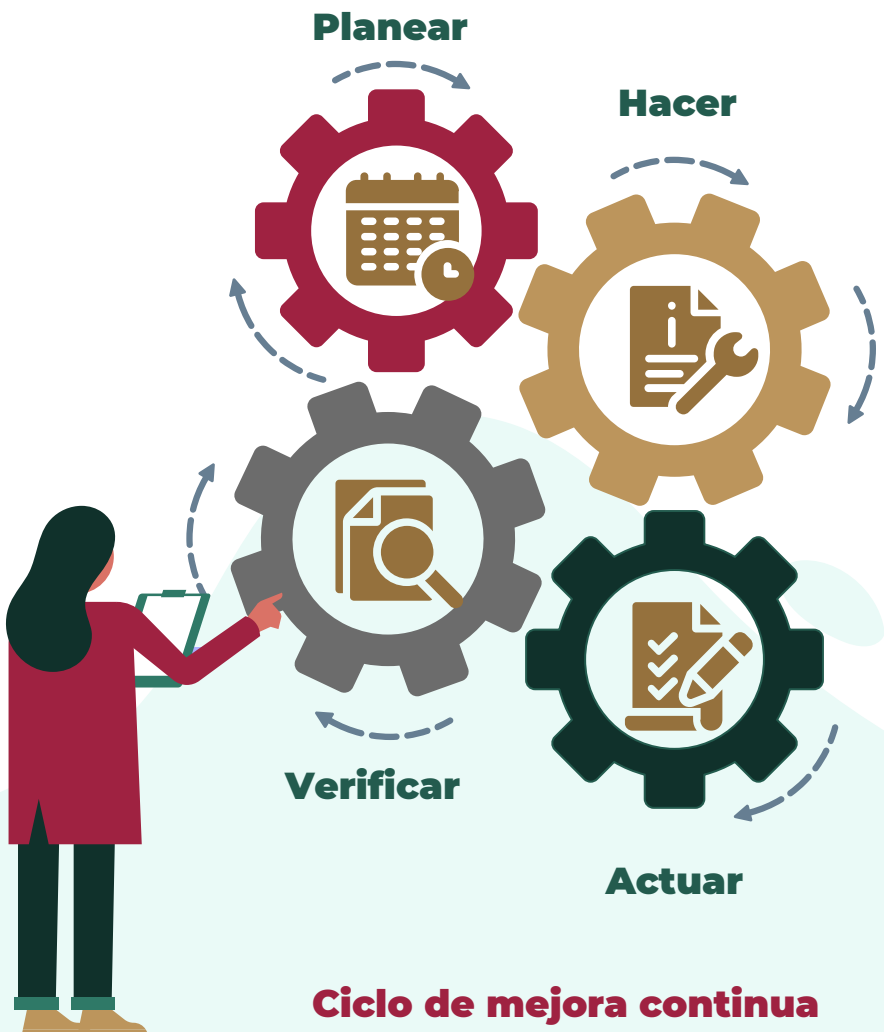
Consentimiento

Aviso de privacidad Integral

Artículo 21 Ter. de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México.

El aviso de privacidad integral además de lo dispuesto en el artículo 21, deberá contener al menos, la siguiente información:

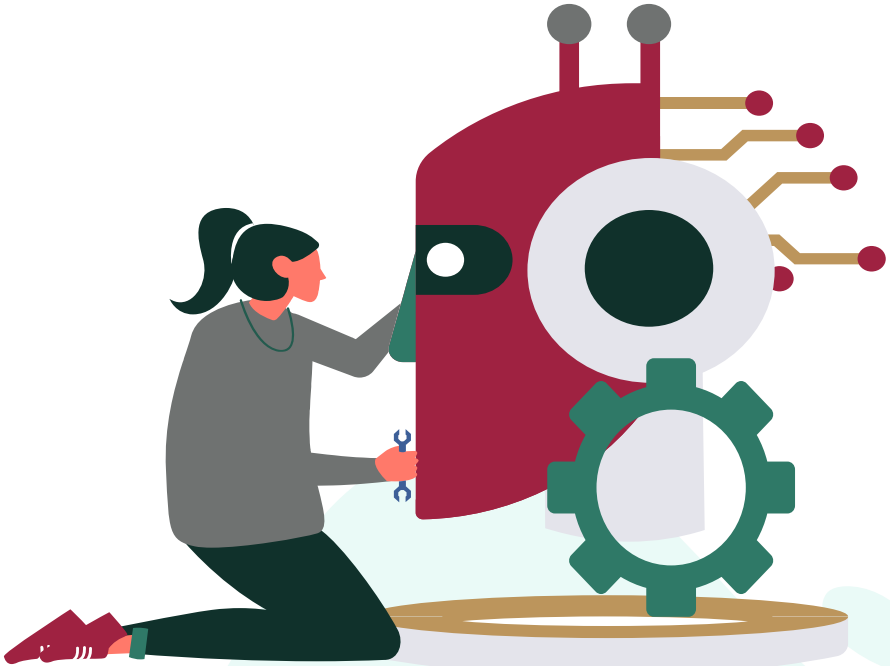




Ciclo de mejora continua

Sistema de Gestión de Seguridad de Datos Personales

Conjunto de elementos y actividades interrelacionadas para planificar, establecer, implementar, operar, monitorear, revisar, mantener y mejorar las medidas de seguridad de carácter administrativo, físico y técnico aplicados a los datos peronales.



Políticas y programas de protección de datos personales

- El responsable deberá **establecer los elementos y actividades de dirección, operación y control de todos los procesos que implique un tratamiento** de DP
- Deberán estar **sustentados en las atribuciones y funciones** explícitas del responsable a fin de proteger los DP de manera sistemática y continua
- Estas políticas deberán ser **aprobadas, coordinadas y supervisadas** por el Comité de Transparencia.
- Deberá **revisar las políticas y programas al menos cada dos años**

Elementos a considerar

Protección de los DP por diseño

Desde el diseño y desarrollo de un SDP, deberá considerarse los avances tecnológicos, los costos de implementación, la naturaleza, el ámbito, el contexto, los fines del tratamiento de los datos personales, los posibles riesgos.

Protección de los DP por defecto

El responsable deberá implementar **medidas técnicas y organizativas** necesarias orientadas a garantizar que por defecto, solo sean objeto de tratamiento los **DP estrictamente necesarios** para cumplir con la finalidad.

Deber de seguridad

El responsable deberá establecer y mantener las medidas de seguridad de carácter **administrativo, físico y técnico** a fin de garantizar su confidencialidad, integridad y disponibilidad.

Contenido de las políticas internas de gestión y tratamiento

Cumplimiento de los principios y deberes

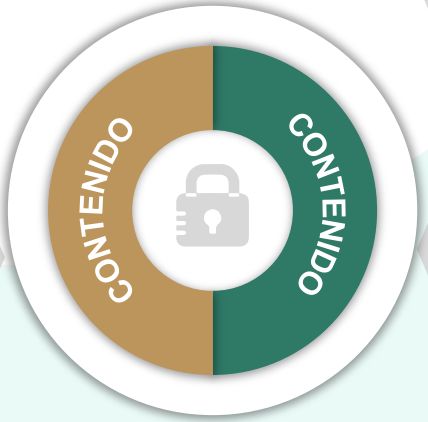
Implementar políticas y mecanismos para asegurar y acreditar el cumplimiento de los principios, deberes y demás obligaciones establecida en la Ley

Roles y responsabilidades

Establecer y documentar los roles y responsabilidades específicos de los involucrados internos y externos relacionados con el tratamiento de DP que efectúen

Sanciones

Especificar cuales son las sanciones en caso de incumplimiento.



Ciclo de vida

Identificar el ciclo de vida de los DP respecto de cada tratamiento que se efectúe; considerando cada parte del proceso, desde la obtención, hasta su destrucción en función de las finalidades.

Proceso general

Considerar el proceso general para el establecimiento, actualización, monitoreo y revisión de los mecanismos y medidas de seguridad considerando el análisis de riesgo.

Derechos ARCO

Establecer el proceso general de atención de los derechos ARCO


Aviso de privacidad
Procedimientos para atención de derechos ARCO
Designación de responsable o departamento al interior
Políticas de Seguridad y protección de datos
Convenios de confidencialidad y contratos
Acciones y procedimientos en caso de vulneración
Capacitar al personal involucrado
Inventario de Datos personales y sistemas de tratamiento
Identificación de personas que tratan los datos, privilegios, roles y responsabilidades
Análisis de riesgos
Análisis de brecha
Datos
Finalidades
Tratamientos
Consentimiento Tácito - Expreso
Privilegios de Acceso y transferencias
Identificar
¿Para qué?
¿Qué voy a hacer con ellos?
Evidencia
Internos
Externos
Medidas de seguridad Administrativas
Medidas de seguridad Físicas
Medidas de seguridad Técnicas

Documento de Seguridad

Instrumento que describe y da cuenta de las **medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable** para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

Actualización anual

Inventario de datos personales

Funciones y obligaciones

Registro incidencias

Identificación y autentificación

Control de acceso

Análisis de riesgos y de brecha

Responsable de seguridad

Registro de acceso y telecomunicaciones

Mecanismos para el monitoreo y revisión de medidas de seguridad

Plan de trabajo

Programa de capacitación

Inventario de datos personales

Medios de obtención

01

Catálogo de medios físicos y electrónicos mediante los cuales se obtienen los datos personales

Finalidades

02

Finalidades de cada tratamiento de datos personales

Tipos de datos personales

03

Catalogo de tipos de datos personales indicando si son sensibles o no.

Formato de almacenamiento

04

Catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales.

Listado de usuarios

05

La lista de las personas servidoras públicas que tienen acceso a los sistemas de tratamiento

Encargados

06

En su caso nombre completo o denominación social del encargado y el instrumento jurídico que formaliza la presentación de losservicios que brinda al responsable

Transferencias

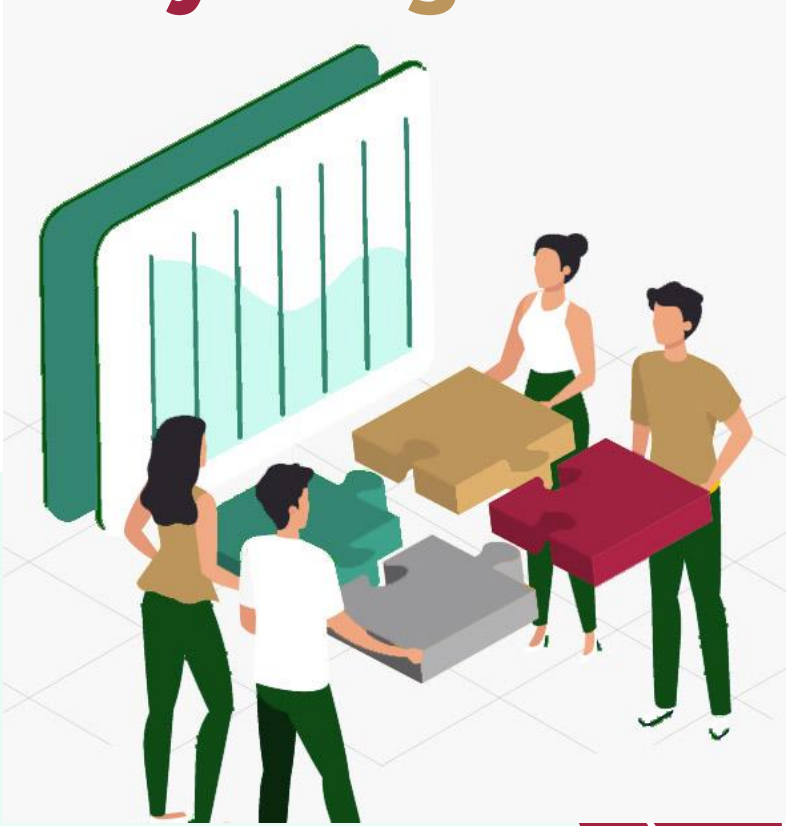
07

Listado de destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que justifican estas.

Funciones y obligaciones

El responsable deberá establecer y documentar:

- Los roles y responsabilidades de cada usuario
- La cadena de rendición de cuentas
- Mecanismos para que todos conozcan sus funciones y consecuencias de incumplimiento.



Registro de incidencias

Que hacer en caso de incidencias?

El responsable deberá implementar medidas de seguridad para prevenir que se presente un incidente, así como poder identificar una vulneración de seguridad

Manejo de incidentes:

- ❑ Preparación
- ❑ Respaldo
- ❑ Respuesta
- ❑ Identificación
- ❑ Contención
- ❑ Mitigación
- ❑ Recuperación
- ❑ Bitácora

Se deberá informar al titular y al Instituto dentro de un plazo máximo de 62 hrs en cuanto se confirme la vulneración y se comience con las acciones de mitigación

Manejo de incidencias

El responsable deberá implementar medidas de seguridad para prevenir que se presente un incidente, así como poder identificar una vulneración de seguridad para ello deberá considerar lo siguiente:

Preparación

- Designar una persona, equipo o área que deberá contar con políticas específicas, acceso a los activos y herramientas para el monitoreo y atención de las alertas de seguridad.

Respaldo

- Deberá crear respaldos o copias de seguridad, al menos mensualmente

Respuesta

- Deberá contar con hardware y software destinados a atender una alerta de seguridad, y comenzar la mitigación en caso de confirmar un incidente, como son antivirus portátiles, discos duros y/o dispositivos de memoria exclusivos para incidentes, herramientas, cables, software para analizar el trafico de red y listas de recisión de comandos, etc.

Identificación

- Una vez identificado el incidente, es necesario buscar alertas adicionales a la detonante y determinar su alcance total por al menos dos personas involucradas en la detección del incidente, una para evaluar los activos que pudieran ser afectados y otra para documentar y recabar evidencia

Manejo de incidencias

El responsable deberá implementar medidas de seguridad para prevenir que se presente un incidente, así como poder identificar una vulneración de seguridad para ello deberá considerar lo siguiente:

Contención

- Una vez identificado el incidente se debe proceder al aislamiento de los sistemas y la puesta en operación de respaldos en el corto plazo para reducir los efectos de un incidente. Posteriormente se debe proseguir con la contención del incidente a largo plazo y se deben identificar las vulnerabilidades explotadas en los activos, así como las medidas de seguridad que pudieron hacer falta, para su posterior implementación.

Mitigación:

- Para la mitigación del incidente es necesaria la implementación de medidas de seguridad y el tratamiento profundo del incidente para minimizar la posibilidad de que se vuelva a repetir, mediante la recolección de evidencia para el análisis forense digital, con herramientas especiales de hardware y software propio o subcontratado a fin de obtener más información para revertir sus efectos.

Recuperación:

- Se deberá dar seguimiento a las medidas implementadas en la mitigación y garantizar que los activos que fueron afectados se reintegran a los sistemas de datos personales, una vez que se encuentren funcionales o que cuenten con las medidas de seguridad que los soporten.

Bitácora:

- Finalmente es necesario completar la documentación respecto al incidente, y comunicar a las partes interesadas el estado de la seguridad de los activos después de lo sucedido mediante un reporte final dentro de los 15 días posteriores y generar un archivo histórico o bitácora que permita a los encargados de la respuesta a incidentes contar con una base de conocimiento, que pueda ser utilizada para entrenar a los usuarios, o a nuevos integrantes del equipo de respuesta a incidentes para la mejora continua.

Identificación y autentificación

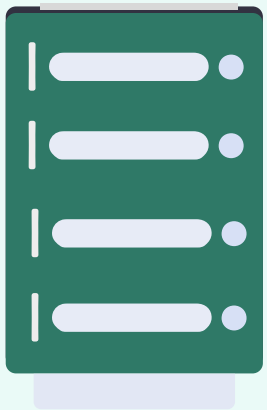
¿Qué personas están autorizadas para acceder a los datos personales del sistema?

¿De qué forma puedo comprobar la identidad de las personas autorizadas?

- Listado actualizado de usuarios
- Procedimiento de altas y bajas
- Mecanismo que permita la identificación de forma inequívoca y personalizada
- Asignación de claves y contraseñas al personal autorizado, debiendo indicar el procedimiento de creación y modificación de claves y contraseñas, señalando longitud, formato y contenido, así como inactivación de cuentas por baja de personal.

Control de accesos

El control de acceso implica llevar el **registro detallado de accesos al sistema**, el cual permita de forma eficaz, aprobar o negar el paso de personas o grupo de personas a zonas restringidas en función de ciertos parámetros de seguridad, es decir, que solo el personal autorizado pueda tener acceso al sistema.



Se deben describir las **medidas de seguridad implementadas para controlar** el acceso del personal autorizado al sistema de datos personales del que se trate, así como **la forma en que se llevará el registro** de accesos al mismo.

Registro de acceso y telecomunicaciones

El registro de acceso se llevará a cabo mediante la implementación de **bitácoras de acceso**, por lo cual, en el presente apartado se debe establecer el procedimiento para el uso de las bitácoras, considerando las acciones cotidianas llevadas a cabo en el sistema de datos personales.

Ejemplo:

Registro de acceso al Sistema de Datos….						
No.	*Nombre*	*Cargo*	*No. de expediente*	*Motivo de la consulta*	*Fecha y hora de la consulta*	*Fecha y hora término de la consulta*
1						
2						
3						

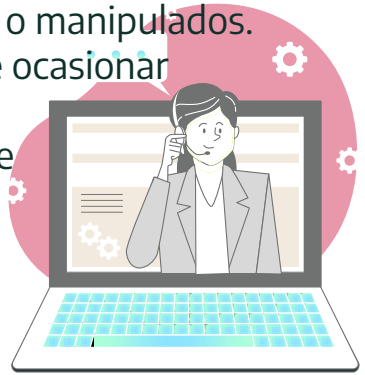
De igual manera se debe dejar constancia de envío, recepción o almacenamiento de los datos personales del sistema a través de dispositivos de telecomunicación.

Se debe tomar en cuenta:

➢ La manera en que se hará la transferencia de los datos, sin que puedan ser alterados o manipulados.

➢ El daño que puede ocasionar dicha transferencia.

➢ La información que va a transferirse



Análisis de riesgos

Amenaza

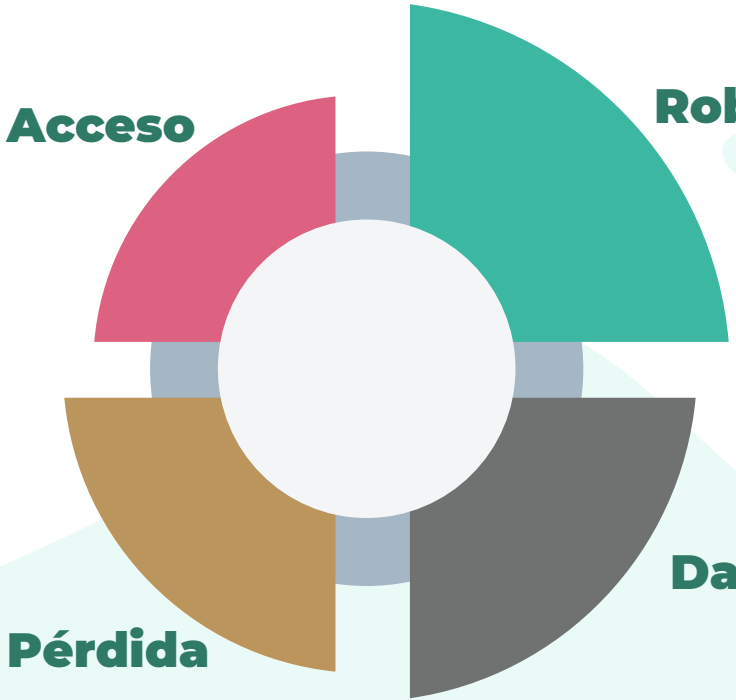
Es o genera

Acción o evento no deseado

Que trata de explotar

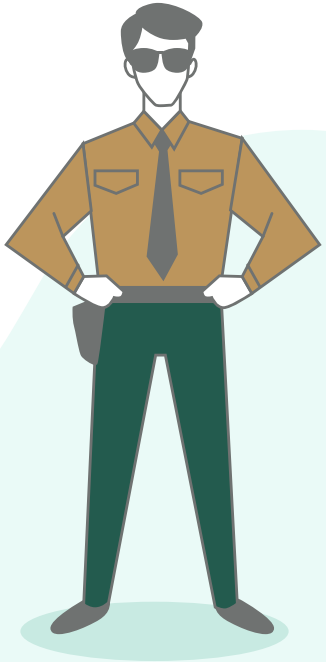
Vulnerabilidad de los archivos

Vulneraciones



Análisis de brecha

Responsable de seguridad



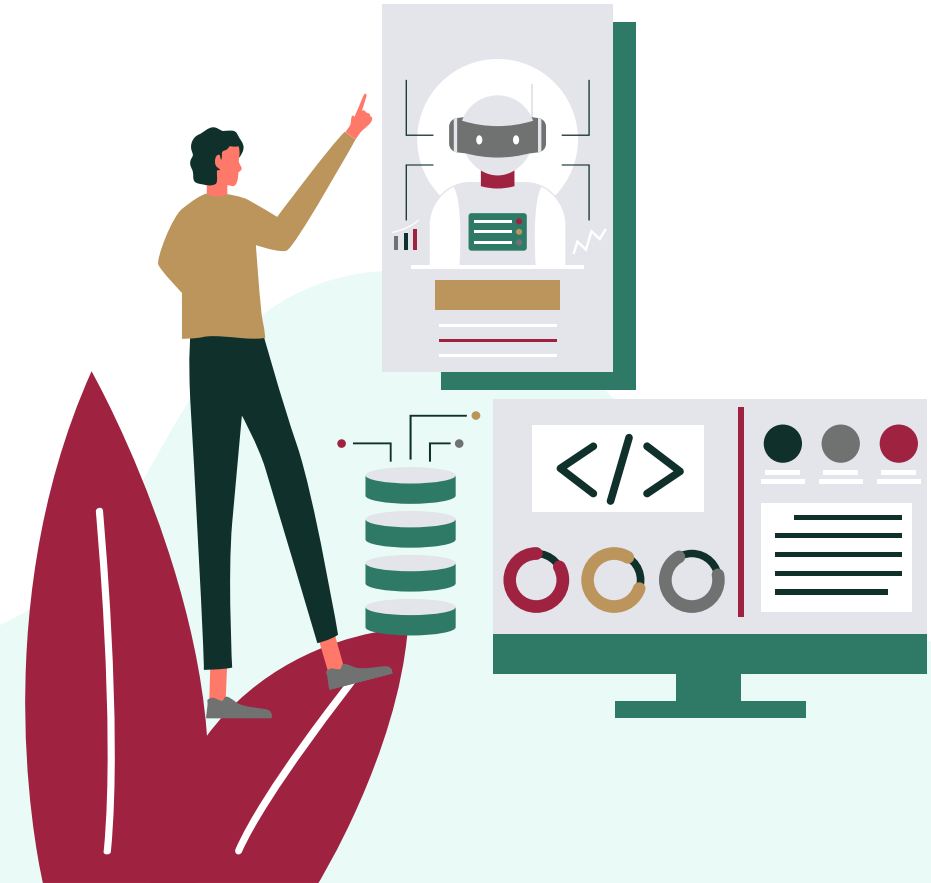
Se debe realizar la formalización mediante un oficio, signado por el responsable del sistema de datos personales, a través del cual se designará a la persona que será responsable de seguridad, en dicho documento se deberá hacer de conocimiento las funciones y obligaciones que tendrá.

Mecanismos para el monitoreo y revisión de medidas de seguridad

Deberá **evaluar y medir los resultados** de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales, a fin de verificar el cumplimiento de los objetivos propuestos y, en su caso, **implementar mejoras de manera continua.**

Plan de trabajo

Define las **acciones a implementar** de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, el cual debe dar prioridad a las medidas de seguridad más relevantes e inmediatas a establecer.



Programa general de capacitación

El responsable deberá establecer anualmente un programa de capacitación en materia de PDP dirigido a su personal y a encargados, el cual **deberá se aprobado, coordinado y supervisado por el Comité de Transparencia**

GOBIERNO DE LA CIUDAD DE MÉXICO | SECRETARÍA DE LA CONTRALORÍA GENERAL

Gracias

Instructora:
Lucero Quintero Olivier
Responsable de Capacitación

Contacto:
5556279700 Extensión 55802
lquintero@contraloriadf.gob.mx