RECOMENDACIONES PARA ORIENTAR EL DEBIDO

TRATAMIENTO DE DATOS PERSONALES EN EL REGISTRO DE CONTROL DE ACCESO

A EDIFICIOS E INSTALACIONES DE LOS SUJETOS OBLIGADOS

inai

Recomendaciones para orientar el debido tratamiento de datos personales en el registro de control de acceso a edificios e instalaciones de los sujetos obligados

OBJETIVO

Orientar a los responsables del sector público, para que brinden un tratamiento adecuado a los datos personales que recaban en los registros de control de acceso a sus instalaciones.

¿Quiénes son los responsables del tratamiento de datos personales que se recaban para llevar a cabo el registro de control de acceso a edificios e instalaciones de los sujetos obligados?

Los responsables en decidir sobre el tratamiento de los datos personales, que son solicitados a los titulares al pretender ingresar a un edificio o instalación pública, son cada uno de los sujetos obligados, Ejemplo: Secretaría de Educación Pública (SEP), Instituto Mexicano del Seguro Social (IMSS), Instituto del Fondo Nacional de la Vivienda para los Trabajadores (INFONAVIT), Instituto Nacional de Pediatría (INP), Cámara de Diputados, Consejo de la Judicatura Federal (CJF), Comisión Nacional de los Derechos Humanos (CNDH), Petróleos Mexicanos (PEMEX), entre otros.

Independientemente que, por conducto de un encargado, materialmente este, puede encargarse de la obtención, uso, registro, conservación, manejo y posesión de dichos datos personales.

¿Qué es el registro de control de acceso?

De conformidad con el artículo 3, fracciones XX y XXII de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), es una medida de seguridad física, mediante la cual, los responsables establecen un filtro de acceso a sus instalaciones, solicitando información específica de identificación a fin de prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información.

El control de acceso a edificios e instalaciones públicas más conocido, implica el registro de entrada y salida de personas, mismo que involucra un proceso de solicitud-entrega de datos personales.

¿Qué deben hacer los sujetos obligados respecto al tratamiento de datos personales en el registro de control de acceso a sus edificios e instalaciones?

En este caso, cuando se recaban datos personales, implica un tratamiento de los mismos, por lo que se deben observar los principios y deberes previstos en la legislación de protección de datos y garantizar el ejercicio de los derechos de los titulares en la materia.

¿En qué consiste el registro de control de acceso a edificios e instalaciones de los sujetos obligados?

En los edificios e instalaciones públicas,

generalmente se cuenta con un control de acceso, el cual, de manera regular, se presenta como un módulo de recepción con personal que brinda orientación sobre diversas actividades o funciones que realiza el sujeto obligado en el edificio que visita, adicionalmente, éste es el filtro básico de seguridad para el ingreso al inmueble, ya que, en este punto se lleva a cabo el registro de entrada y salida.

Así, se identifica que toda persona que accede a edificios e instalaciones públicas, registra de manera directa o indirecta su entrada y salida, proporcionando la información solicitada por el responsable para permitir el acceso al inmueble respectivo.

Ejemplos del registro:

Directo

El registro directo será cuando el titular (invitado), se registre de manera presencial o por algún medio que permita su entrega directa como podrían ser medios electrónicos, ópticos, sonoros, visuales, vía telefónica, Internet o cualquier otra tecnología y/o medio, independientemente de la forma en que el titular proporcione los datos, se deberá poner a su disposición el aviso de privacidad.

Indirecto

El registro indirecto, será cuando una tercera persona a quien el titular no se lo solicitó, sea quien proporciona los datos personales del titular. Por ejemplo: Cuando previo a su visita, un colaborador hace llegar los datos al control de vigilancia del edificio o en su caso del estacionamiento, situación que se hace presente de manera regular con invitados especiales o ponentes a eventos. En los casos en que se obtengan los datos de manera indirecta, el aviso de privacidad deberá ser puesto a disposición al primer contacto con el titular o previo al aprovechamiento de los datos personales.

De ahí, que el registro de entrada y salida es un mecanismo utilizado como medida de seguridad física, en donde involucra un tratamiento de datos personales por parte del sujeto obligado y que este en todo momento deberá cumplir con los principios y deberes establecidos en la normativa vigente en la materia.

¿Qué tipo de titulares acceden a edificios e instalaciones públicas?

Una adecuada identificación de los titulares de datos personales que se tratan a partir del registro de control de acceso, permite a los responsables agruparlos por tipo, generando diversas cédulas de registro, atendiendo a los datos que son estrictamente necesarios conocer de cada persona que pretende su ingreso al inmueble.

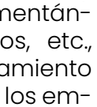
En principio, el registro de acceso se debe dividir en dos grupos:

Trabajadores

Titulares adscritos al sujeto obligado que acrediten que son trabajadores o prestadores de servicios en activo.

Visitantes o Usuarios

Titulares ajenos al sujeto obligado.



¿Qué es el registro de trabajadores?

Se trata de la base de datos del personal adscrito a la institución o dependencia, que tienen un sistema de registro específico. Usualmente, registra su acceso en sistemas digitales que incluyen el uso de credenciales, tarjetas, datos biométricos o cualquier elemento seleccionado por la institución para identificar al empleado y su hora de entrada y salida a las instalaciones.

Lo anterior, para acreditar el cumplimiento de las jornadas de trabajo reglamentarias.

El tratamiento de datos personales de trabajadores o empleados, es distinto al de visitantes ya que existe una relación jurídica laboral a través de un acuerdo de voluntades celebrado entre el patrón y el trabajador, acto jurídico que, da origen a la necesidad de registrar y monitorear constantemente los horarios de entradas y salidas de los empleados, fundamentándose en reglamentos, lineamientos, etc., asimismo, las finalidades del tratamiento de datos deben ser comunicadas a los empleados mediante el aviso de privacidad simplificado e integral, respectivamente.

Aunado a lo anterior, es importante destacar que, el tratamiento de datos personales de proveedores y personal de honorarios, es distinto al de trabajadores y de visitantes, ya que las relaciones existentes son variadas. Además, las finalidades del tratamiento de datos se comunican a estos titulares a través de los avisos de privacidad correspondientes.

Por otro lado, se pueden incluir a las personas prestadoras de servicio social o prácticas profesionales, mismos que cuentan con horario fijo y apegado a lo establecido en convenios de colaboración celebrados con instituciones de educación.

Como apoyo, se puede consultar la "Guía para la elaboración del aviso de privacidad en el área de recursos humanos (Sector Público)", disponible en el siguiente enlace: http://inicio.ifai.org.mx/DocumentosdeInteres/_GuiaAP-RRHH.pdf

¿Qué es el registro de visitantes y/o usuarios?

Base de datos referente a la categoría de visitantes, considerando como tales, a todas aquellas personas físicas ajenas al sujeto obligado, que acuden a las instituciones o dependencias para realizar diversas actividades en sus instalaciones.

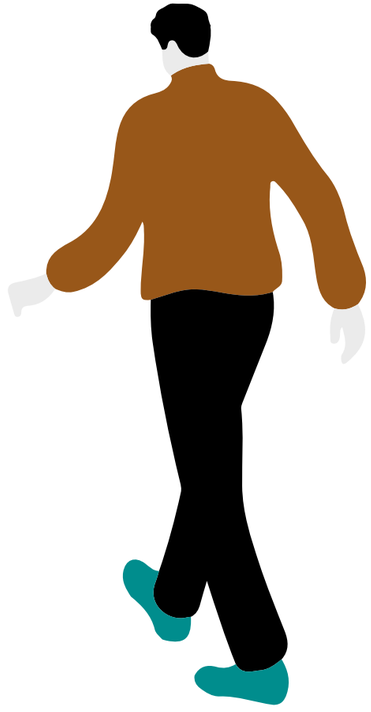
El tratamiento de datos personales de visitantes o del personal que no está adscrito al sujeto obligado, es un tratamiento con una temporalidad distinta al de un trabajador, pues se llevará a cabo durante la estadía de la persona en el edificio, y por el tiempo que se haya definido por el responsable del tratamiento para cumplir con la medida de seguridad que se implementó o en su caso con aquellas obligaciones legales que deriven del tratamiento.

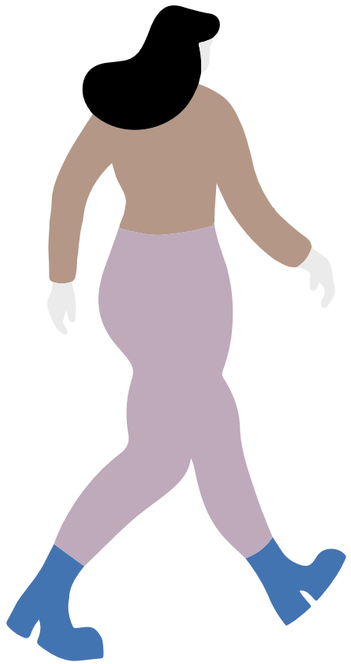
Ahora bien, para la categoría de visitantes, se sugiere hacer uso de subcategorías adicionales, lo anterior facilitará a los titulares que ingresan a las instalaciones, identificar rápidamente el tipo de registro que realizarán. Dentro de estas subcategorías, a manera de ejemplo se señalan las siguientes:

- Proveedores: Personal ajeno a la institución, acreditado por una entidad que cuente con al menos un contrato vigente para prestar servicios a la institución o dependencia.

- Asistentes a cursos, capacitaciones o eventos: Se refiere a todas aquellas personas que acuden de forma temporal, regularmente por solo un día a la institución o dependencia con motivo de un curso, capacitación o evento.

- Público en general: Se refiere a todas aquellas personas que acuden a las instalaciones de los Sujetos Obligados a realizar cualquier trámite o actividad distinta a la señalada en los puntos anteriores.





¿Qué medios se emplean para el registro de acceso?

Se emplean controles físicos o electrónicos, en los que se registran datos personales obtenidos de las identificaciones oficiales vigentes o biométricos, de los cuales, el titular respectivo, al plasmar su firma autógrafa en el control físico de registro, otorga su consentimiento expreso al momento de ingresar a las instalaciones del sujeto obligado.

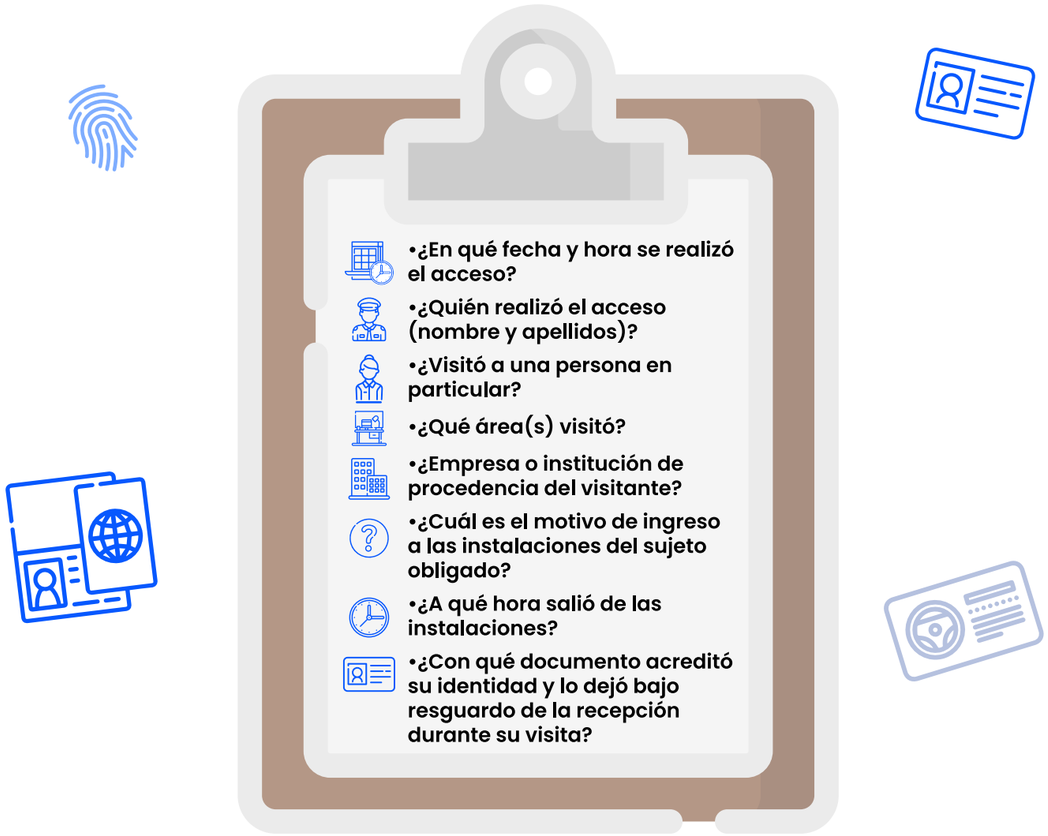
Como apoyo a este tema, se sugiere consultar la herramienta denominada "Guía para el tratamiento de datos biométricos", la cual, se encuentra disponible en la siguiente liga: http://inicio.ifai.org.mx/DocumentosdeInteres/GuiaDatosBiometricos_Web_Links.pdf

Por otra parte, la cédula o bitácora de registro, es una base de datos mediante la cual, los responsables recolectan los datos personales para llevar el control de acceso.

Es un documento físico o electrónico, generado a partir de preguntas que permiten obtener información respecto a la visita que realiza una persona a las instalaciones de los Sujetos Obligados.

Para elaborar una cédula o bitácora de registro, es importante que se tengan identificados los datos personales que se van a recabar de las personas que accedan a sus instalaciones, identificando la categoría de cada uno de estos y tomando en cuenta los principios de proporcionalidad y finalidad que rigen el tratamiento de datos personales.

Por lo anterior, no se recomienda contar con una cédula universal de registro, aunque es posible identificar preguntas básicas sobre el ingreso de una persona a las instalaciones, tales como:



En esta cédula, podrá incluir todas las preguntas que necesite para identificar el acceso a sus instalaciones por cada persona, apegándose al principio de proporcionalidad.

¿Qué tratamiento recibe comúnmente el documento de identificación solicitado al pretender el ingreso a un edificio o instalación del sujeto obligado?

Un documento de identidad es cualquier documento, expedido por una autoridad pública, que contiene datos de identificación personal que permite a las personas físicas identificarse en todos los escenarios o ámbitos de relacionamiento dentro de la sociedad.

En ocasiones, durante el proceso de registro, como medida de control adicional, después del registro de datos personales en la cédula, se realiza un resguardo temporal de un documento de identidad y a cambio se entrega, un elemento de identificación interno (gafete, tarjeta, identificador, etc.) que permite el acceso a las instalaciones, así como, facilitar al personal de seguridad la identificación de los visitantes.

La retención de documentos de identidad se puede presentar de dos maneras:

1. Mediante la **digitalización del documento**, mecanismo en donde se genera una copia digital de la identificación de quien ingresa a las instalaciones;

2. Mediante la **retención física del documento**, mecanismo en donde se resguarda el documento de identificación durante la estadía de la persona en las instalaciones.

Los responsables deberán considerar la conservación y digitalización de los documentos de identidad, en razón que ello constituye el tratamiento de los datos personales que están insertos en dichos documentos de identidad.

En México, el documento de identidad oficial mayormente solicitado es la credencial para votar expedida por el Instituto Nacional Electoral, por lo que puede servir de apoyo para su resguardo, las Recomendaciones sobre protección de datos personales contenidos en la Credencial para Votar disponibles en: http://inicio.inai.org.mx/DocumentosdeInteres/RecomendacionesCredencialV.pdf

¿Qué elementos se deben considerar para el registro de control de acceso de niñas, niños y adolescentes en las instalaciones de los sujetos obligados?

En el caso particular de las niñas, niños y adolescentes se debe tener especial cuidado ya que, de conformidad por lo dispuesto en el párrafo segundo del artículo 7 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, en el tratamiento de datos personales de menores de edad, se deberá privilegiar el interés superior de los menores, en términos de las disposiciones legales aplicables; por lo que, es recomendable que en caso de ser indispensable por parte del sujeto obligado el recabar datos de menores de edad, es necesario que esté presente su tutor o representante legal en atención de que el menor de edad no cuenta con capacidad de ejercicio como para otorgar el consentimiento respectivo.

¿Qué recomendaciones generales deben contemplarse para el registro de control de acceso a edificios e instalaciones de los sujetos obligados?

- PRINCIPIO DE INFORMACIÓN: El responsable deberá elaborar y poner a disposición de los titulares el aviso de privacidad en el cual se informen los términos, alcances y condiciones del tratamiento al que serán sometidos sus datos personales, en el caso específico del registro de control de acceso se sugiere que el aviso distinga claramente los datos personales que se recaben de cada una de las categorías de titulares que ingresa a la institución o dependencia.

  Al respecto, se sugiere consultar la siguiente herramienta de facilitación emitida por el INAI: "El ABC del Aviso de Privacidad (Sector Público)", misma que se encuentra disponible en el siguiente enlace: http://inicio.ifai.org.mx/DocumentosdeInteres/_ABC-AP-SPublico.pdf

- PRINCIPIO DE LICITUD: El responsable deberá en un primer término, contar con las atribuciones para tratar los datos personales según la normativa aplicable, por lo que se sugiere conocer la legislación que en lo específico regula y aplica a la actividad en la que son tratados los datos personales que se llegan a recabar por el proceso de registro de control de acceso a manera de ejemplo, los Reglamentos Internos o Estatutos Orgánicos de los Sujetos Obligados.

  Para la revisión sobre el cumplimiento del principio de licitud y acceder a un listado de comprobación relacionado con este principio, se recomienda consultar la página 17 del "Programa de Protección de Datos Documento Orientador", disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/DocumentoOrientadorPPDP.docx

- PRINCIPIO DE LEALTAD: El responsable deberá utilizar medios que estén permitidos por la ley para generar las cedulas de registro donde se recaben datos personales, contar con una cédula de registro de datos que permita identificar a los titulares qué datos se están solicitando. Asimismo, el responsable tiene las siguientes obligaciones en torno al principio de lealtad al generar las cédulas de registro:

  1) No hacer uso de medios engañosos o fraudulentos para la obtención de los datos personales.

  2) Respetar en todo momento la expectativa razonable de privacidad del titular.

  - Para la revisión sobre el cumplimiento del principio de lealtad y acceder a un listado de comprobación relacionado con este principio, se recomienda consultar las páginas 18 y 19 del "Programa de Protección de Datos Documento Orientador", disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/DocumentoOrientadorPPDP.docx

- PRINCIPIO DE CONSENTIMIENTO: Se sugiere identificar si los datos serán tratados dentro de alguno de los supuestos previstos por el artículo 22 de la LGPDPPSO. En caso de que así sea, su tratamiento no requerirá consentimiento.

  No obstante, si el sujeto obligado pretende utilizar los datos para finalidades que no encuadren en las excepciones anteriormente señaladas, o que no resulten compatibles o análogas con aquéllas para las cuales se recabaron los datos personales, será necesario que se obtenga el consentimiento del titular.

  - **Si el responsable recaba datos sensibles de los que se hace referencia en el artículo 3 fracción X de la LGPDPPSO, este deberá solicitar el consentimiento expreso y por escrito de los titulares de los datos, previo a que se recaben, o bien, en el momento en que lo indique la normativa aplicable.**

  Asimismo, para la revisión sobre el cumplimiento del principio de consentimiento y acceder a un listado de comprobación relacionado con este principio, se recomienda consultar las páginas 23 a 37 del "Programa de Protección de Datos Documento Orientador", disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/DocumentoOrientadorPPDP.docx

- PRINCIPIO DE CALIDAD: Los responsables deberán tomar todas las medidas razonables para garantizar que los datos en su poder sean exactos, completos, pertinentes y actualizados.

  Los datos personales deberán ser suprimidos cuando la o las finalidades para las cuales fueron recabadas hayan quedado obsoletas o sin efecto. De igual forma, deberán observar lo dispuesto por la normativa aplicable en materia de archivos, considerando así desde cuando fueron recabados los datos personales.

  No conservar los datos por un plazo superior al necesario para cumplir con la finalidad para la que se han recolectado. Asimismo, para la revisión sobre el cumplimiento del principio de calidad y acceder a un listado de comprobación relacionado con este principio, se recomienda consultar las páginas 43 al 45 del "Programa de Protección de Datos Documento Orientador", disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/DocumentoOrientadorPPDP.docx

  Así también, se sugiere al sujeto obligado revisar la siguiente herramienta de facilitación emitida por el INAI: "Guía para el Borrado Seguro de Datos Personales", misma que puede ser consultada en el siguiente enlace: http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_Borrado_Seguro_DP.pdf

- PRINCIPIO DE FINALIDAD: Se deberán señalar claramente la finalidad o finalidades específicas del tratamiento de datos personales del registro de entradas y salidas de instalaciones del sujeto obligado.

  Por lo que respecta a la revisión sobre el cumplimiento del principio de finalidad y acceder a un listado de comprobación relacionado con este principio, se recomienda revisar las páginas 40 a 43 del "Programa de Protección de Datos Documento Orientador", disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/DocumentoOrientadorPPDP.docx

- PRINCIPIO DE PROPORCIONALIDAD: Los responsables solo deberán solicitar los datos personales estrictamente necesarios para controlar el acceso y cumplir con las medidas de seguridad que se hayan adoptado. En este sentido, se recomienda evitar conservar cualquier tipo de copias respecto de las identificaciones oficiales presentadas por quienes pretenden acceder al espacio público.

  Para acceder a una revisión sobre el cumplimiento del principio de proporcionalidad y acceder a un listado de comprobación relacionado con este principio, se recomienda revisar las páginas 38 y 39 del "Programa de Protección de Datos Documento Orientador", disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/DocumentoOrientadorPPDP.docx

- PRINCIPIO DE RESPONSABILIDAD: Los responsables deberán velar por el cumplimiento de los principios y responder por el tratamiento de los datos personales, adoptando medidas para garantizar el debido tratamiento en el registro de control de acceso a instalaciones del sujeto obligado, debiendo en todo momento privilegiar los intereses del titular y su expectativa razonable de privacidad. Para llevar a cabo la revisión sobre el cumplimiento del principio de responsabilidad y acceder a un listado de comprobación relacionado con este principio, se recomienda revisar las páginas 69 a 73 del "Programa de Protección de Datos Documento Orientador", disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/DocumentoOrientadorPPDP.docx

- DEBER DE SEGURIDAD: En el tratamiento de datos por el registro de control de acceso a instalaciones del sujeto obligado, los responsables deberán implementar las medidas (I) **administrativas** (controles que ayuden a evitar prácticas inadecuadas del personal que pongan en riesgo los datos personales, como por ejemplo dejar bitácoras o cédulas de registro al alcance de todos o compartir contraseñas de las computadoras en dónde se encuentren los registros electrónicos), (II) **físicas** (controles aplicados en los espacios físicos e infraestructura que minimicen el robo o acceso no autorizado, como por ejemplo, mantener las áreas de trabajo, mobiliario y equipos debidamente cerrados con los controles y candados suficientes), y (III) **técnicas** (controles para proteger equipos de cómputo y dispositivos de almacenamiento de virus, malware, entre otros) necesarias para garantizar que los datos personales que intervienen en el proceso de registro de entradas y salidas a instalaciones se encuentren protegidos del acceso, procesamiento, eliminación, pérdida o uso no autorizados.

Para el registro de entradas y salidas, se pueden identificar dos tipos de sistemas de registro, uno donde se utilizan bitácoras físicas y otro donde se implementa un sistema de gestión de visitantes. Dependiendo del sistema de registro que identifique, deberá adoptar medidas muy específicas para el resguardo de la información que recaba.

Independientemente del sistema que se utilice, deberá identificar perfectamente los siguientes elementos:

- Los actores que intervienen en el proceso de registro de entradas y salidas.
- El listado de datos personales que serán recabados por cada actor identificado.
- Los tiempos en que se realiza el intercambio de los datos personales.
- Los mecanismos y elementos (equipos, dispositivos, materiales, etc.) implementados para recabar y procesar los datos personales.

Asimismo, respecto al deber de seguridad, se recomienda consultar el siguiente hipervínculo: http://inicio.ifai.org.mx/DocumentosdeInteres/Anexos-DocumentoOrientador.zip
y consultar específicamente los documentos:
ANEXO6-MedidasdeSeguridad.docx (Paginas 20 a 22).
ANEXO6-1-Vulneraciones.DOCX (Página 11).

Por cuanto hace al análisis de riesgo, análisis de brecha, plan de trabajo, monitoreo y revisión de las medidas de seguridad, no se desarrollaron listas de comprobación, en razón de que se consideran elementos técnicos específicos.

Por otro lado, con respecto al control de acceso a instalaciones del sujeto obligado, para mayor información sobre las medidas administrativas, físicas y técnicas consulte el Anexo III de la presente guía.

- DEBER DE CONFIDENCIALIDAD: En el tratamiento de datos personales, se sugiere al responsable que tanto él como en el caso que se contrate un proveedor del servicio para estos fines, se celebre un instrumento jurídico que respalde el deber de confidencialidad, donde se detallen, al menos, los alcances técnicos del sistema, las medidas de seguridad técnicas aplicadas a la información al ser resguardada y consultada, el formato de la información, el espacio físico o virtual donde se almacene la información, los datos personales a recabar y las transferencias que serán habilitadas.

  Definir claramente al personal autorizado para tener acceso y tratar datos, o bien, por terceros que actúen a nombre y por cuenta del responsable. Al respecto, se considera pertinente que delimiten las obligaciones de los empleados dentro de la organización del sujeto obligado, así como del encargado. Lo anterior, toda vez que en las instituciones o dependencias se hace uso de personal de seguridad quienes son los encargados de controlar el acceso y salida de las instalaciones.

  De manera adicional, se recomienda al responsable que, para el cumplimiento del deber de confidencialidad, consulte las páginas 15 y 16 del Documento orientador para la elaboración del Programa de Protección de Datos Personales, disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/DocumentoOrientadorPPDP.docx

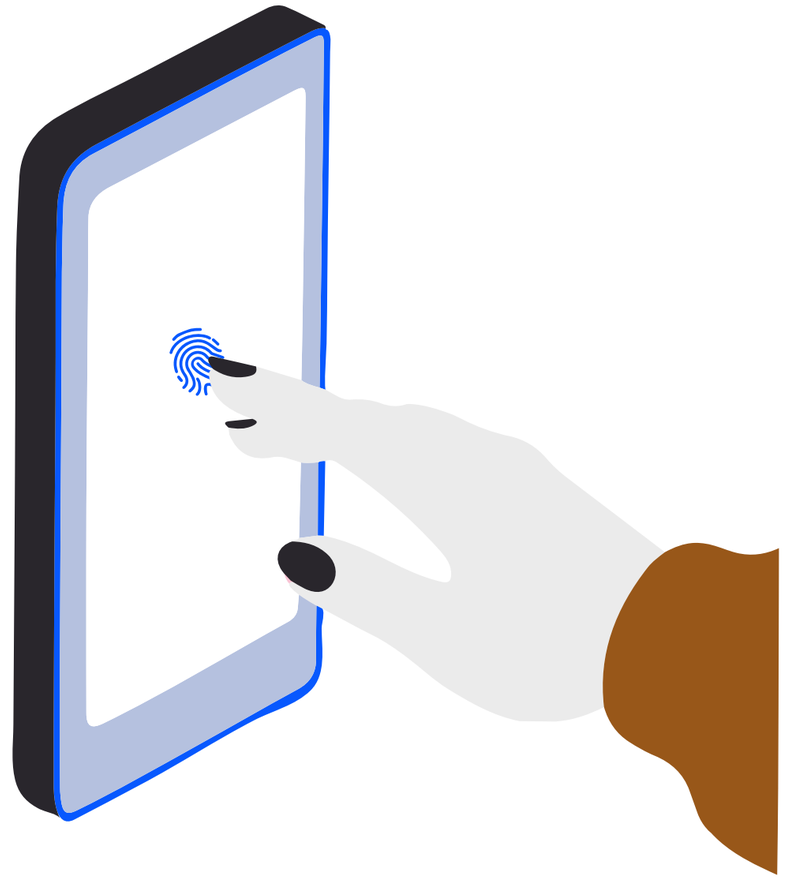
  Por lo que respecta al cumplimiento específico de deberes y principios de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, se les recomienda a los sujetos obligados, consultar la "Guía para cumplir con los principios y deberes de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados", misma que se encuentra disponible en el siguiente enlace: http://inicio.ifai.org.mx/DocumentosdeInteres/_GuiaPrincipiosDeberes.pdf

ANEXO I
Identificaciones oficiales y datos personales

A continuación, se presenta un listado de los documentos oficiales más comunes y los datos que se incluyen en éstos:

Tipo de Documento	Datos personales	
Credencial para votar	•Fotografía •Nombre completo •Domicilio •Fecha de nacimiento •Sexo •CURP •Clave de elector	•Número identificador (OCR) •Firma •Huella dactilar •Datos electorales •Código de barras y QR •Año de registro y vigencia
Pasaporte	•Fotografía •Nombre completo •Nacionalidad •Fecha de nacimiento •Lugar de nacimiento	•Sexo •Fecha de expedición y caducidad •Número identificador (OCR) •Número de pasaporte •Firma
Cédula profesional vigente	•Fotografía •Nombre completo •Número de Cédula profesional	•Grado de estudios •Firma •CURP
Cartilla del Servicio Militar Nacional	•Fotografía •Nombre completo •Fecha de nacimiento •Lugar de nacimiento •Datos de padres •Estado civil	•Ocupación •Sabe leer y escribir •Grado de estudios •Domicilio •Matrícula •Firma
Credencial emitida por instituciones de educación pública o privada con fotografía	•Fotografía •Nombre completo •CURP •Especialidad	•Grado y grupo •Folio •Turno •Firma
Licencia de conducir	•Fotografía •Nombre completo •CURP •Expedición •Vencimiento •Folio	•Firma •Nacionalidad •Firma •Huella dactilar •Código QR
Credencial del INAPAM	•Fotografía •Nombre completo •Fecha de nacimiento •Folio	•Domicilio •Huella dactilar •Firma •Contacto de confianza

Por otro lado, algunos sujetos obligados, en su carácter de patrón hacía sus trabajadores, implementan medidas de control para registro de entradas y salidas de manera electrónica, recabando así datos biométricos, como ejemplo, la huella dactilar, a través del denominado “sistema electrónico para el registro de entradas y salidas”.



ANEXO II

Ciclo de vida de los datos personales

El registro de control de acceso implica el tratamiento de datos personales que se establecen como necesarios para tener un control sobre el acceso a cualquier instalación del sujeto obligado, mismos que tienen un ciclo de vida que se presenta de la siguiente manera:

01 REGISTRO DE ENTRADA

- Se registran diversos datos de la persona que ingresa al edificio.
- Se registran datos de los motivos de la visita.
- Se registra la hora de entrada.
- En caso de ser necesario, se registran datos de los objetos, dispositivos, materiales, etc. que lleva la persona que va a ingresar.
- Puede ocurrir una retención de identificación oficial.

02 ESTANCIA EN EL INMUEBLE

- Se resguardan los datos del visitante. *(SE considera que los datos, no solo se resguardan durante la estancia)*
- Se monitorea si la persona que accedió continúa dentro de las instalaciones.

03 REGISTRO DE SALIDA

- Se registra la hora de salida de la persona.
- En caso de que haya registrado objetos, dispositivos, materiales, etc. se verifican los datos de éstas pertenencias.
- En caso de que hubiera una retención de identificaciones, se devuelve la identificación oficial a su dueño.

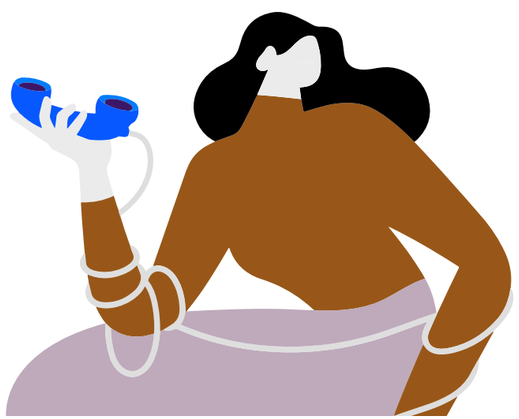
04 RETENCIÓN DE REGISTROS

- Los datos obtenidos del registro de entradas y salidas se resguardan por un tiempo que debe ser definido de acuerdo con la finalidad y lo dispuesto en la normatividad de archivos.

05 ELIMINACIÓN DE REGISTROS

(Revisar la supresión y cancelación, tema de archivos)

- Una vez que concluya el tiempo definido para su resguardo por uso, se deben eliminar los datos y generar una evidencia de su borrado.



ANEXO III

Medidas de seguridad para sistemas de registro físico y electrónico de control de acceso

Debe considerarse que los sistemas físicos y electrónicos de control de acceso para las personas que pretenden el ingreso a un edificio o instalación pública son más recomendados por las medidas de seguridad y control de información que incorporan, aunque su implementación, operación y mantenimiento conlleva un costo adicional que debe considerarse. A continuación, se presenta un comparativo para advertir las ventajas de este tipo de sistemas frente a los de carácter físico:

Sistema de registro en bitácoras físicas

Se trata de bitácoras o libretas de registro ubicadas en los puntos de acceso a los edificios, donde el titular registra sus datos.

En ocasiones, se complementa este sistema con el intercambio de un documento de identidad por una credencial, identificador o tarjeta de acceso a las instalaciones de la institución o dependencia.

Sistema electrónico de gestión de visitantes

Sistema que incluye software y hardware con el fin de digitalizar el procedimiento de registro de visitantes, este sistema sustituye al tradicional al omitir el registro físico.

Para poder conocer los diferentes sistemas que se ofrecen en el mercado, le recomendamos utilizar un comparador de software, donde podrá encontrar descripciones, comentarios e información sobre los sistemas que ofrecen el servicio que está buscando.

Medidas de seguridad administrativas

Sistema de registro en bitácoras físicas

- Implementar reglas de uso sobre las bitácoras de registro.
- Contar con una bitácora por actor identificado que pueda ingresar a las instalaciones.
- Tener un sistema de recolección de identificaciones que minimice el riesgo de extraviarlas o intercambiarlas.

Sistema electrónico de gestión de visitantes

- Implementar reglas de operación al sistema.
- Darle acceso únicamente al personal que intervenga en el proceso de registro de visitantes.
- Revisar los contratos y medidas de seguridad que implementa la aplicación.
- Celebrar un contrato de confidencialidad con el proveedor de servicio.

Medidas de seguridad físicas

Sistema de registro en bitácoras físicas

- Contar con aditamentos que no permitan a los visitantes ver otros registros.
- Contar con aditamentos que no permitan sustraer hojas o las bitácoras completas.
- Contar con espacios de resguardo para bitácoras en caso de no ser utilizadas.
- No permitir la reproducción total o parcial del contenido de las bitácoras por ningún medio.

Sistema electrónico de gestión de visitantes

- Habilitar dispositivos dedicados al uso del sistema en los puntos de acceso a las instalaciones, es decir, no tener otros programas o aplicaciones en los dispositivos para acceso.
- Fijar los dispositivos a los puntos de acceso para visitantes.

Medidas de seguridad técnicas

Sistema de registro en bitácoras físicas

- En atención a que los elementos que componen una bitácora son documentos físicos, a estos no se les puede aplicar una medida de seguridad técnica.

Sistema electrónico de gestión de visitantes

- Es importante resaltar que la capacidad y la seguridad de estos sistemas depende de la inversión que se quiera hacer, ya que, además de encontrar con una gran cantidad de proveedores de dicho servicio, encontrará herramientas complementarias para mejorar la seguridad del sistema.
- Se debe contar con una base de datos única que incluya cifrado sobre los registros de datos que se realizan.
- Implementar funciones criptográficas para la información intercambiada entre los dispositivos y el espacio de almacenamiento de la información.
- No replicar la base de datos en otros dispositivos.
- Bloquear la conexión de dispositivos de almacenamiento a los dispositivos destinados para el registro.

inai

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales