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

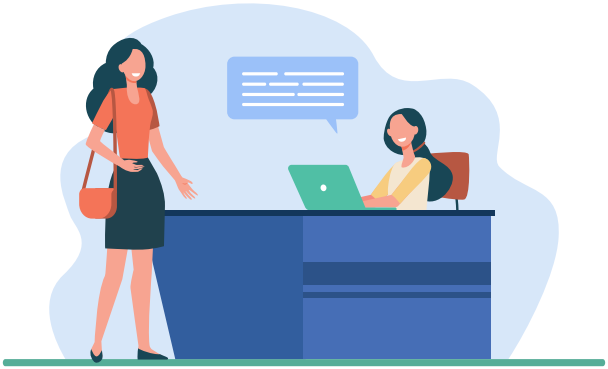
Recomendaciones para orientar el debido tratamiento de datos personales en el registro de control de acceso a edificios e instalaciones de los sujetos obligados del Estado de Chihuahua

Chihuahua, Chih. Julio de 2021

Recomendaciones para orientar el debido tratamiento de datos personales en el registro de control de acceso a edificios e instalaciones de los Sujetos Obligados del Estado de Chihuahua

Objetivo

Orientar a los responsables de las Instituciones Públicas, para que brinden un tratamiento adecuado a los datos personales que recaban en los registros de control de acceso a sus instalaciones, esto en cumplimiento al deber de seguridad previsto en los diversos incisos de las fracción I del artículo 73 de la Ley de Protección de Datos Personales del Estado de Chihuahua, ya que los responsables recaban datos personales y cuentan con el deber de establecer medidas de seguridad.



¿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 previo a ingresar a un edificio o instalación pública, son cada uno de los sujetos obligados, que enuncian el art 6 de la Ley de Protección de Datos Personales del Estado de Chihuahua. Ejemplo: Tribunal Superior de Justicia del Estado, H. Congreso del Estado, Instituto Estatal Electoral (IEE), Junta Central de Agua y Saneamiento (JCAS), Policía Amigo, Ayuntamiento de Delicias, DIF Juárez, Partido Acción Nacional (PAN), Centro Estatal de Trasplantes, entre otros.

Con independencia de que sea por conducto de un encargado que, materialmente opere 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 11, fracción XXII de la Ley de Protección de Datos Personales del Estado de Chihuahua y el artículo 55, fracción I de los Lineamientos de la Ley de Protección de Datos Personales del Estado de Chihuahua, 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, y así mismo, para cuestiones estadísticas o de seguridad.

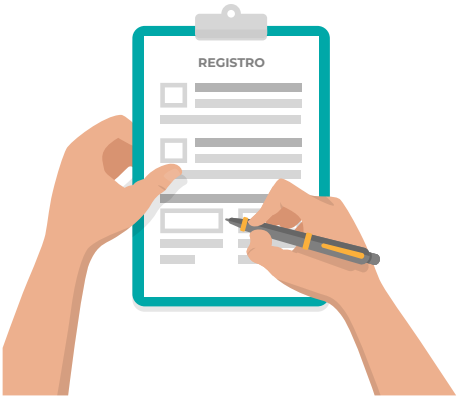
El control de acceso a edificios e instalaciones públicas más conocido, implica el registro de entrada y salida de personas, mismo que involucra un proceso de solicitud-entrega de datos personales consintiendo a través de la puesta a disposición del aviso de privacidad por parte del responsable.

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

El recabar 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 en la materia de los titulares.

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

Los Sujetos Obligados en los edificios e instalaciones públicas, generalmente cuentan con un control de acceso, el cual, de manera regular, se presenta como un módulo de recepción con personal que en ocasiones, brinda orientación sobre diversas actividades o funciones que realiza el sujeto obligado en el edificio que visita, no obstante, la función consiste en ser, 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 se actualiza cuando el titular (visitante), se registre de manera presencial o por algún medio que permita la entrega directa de datos personales tales como 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, se actualiza cuando una tercera persona a quien el titular no se lo solicitó, sea quien proporcione 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, que involucra un tratamiento de datos personales por parte del sujeto obligado que en todo momento deberá cumplir con los principios y deberes establecidos en la normativa vigente en la materia.

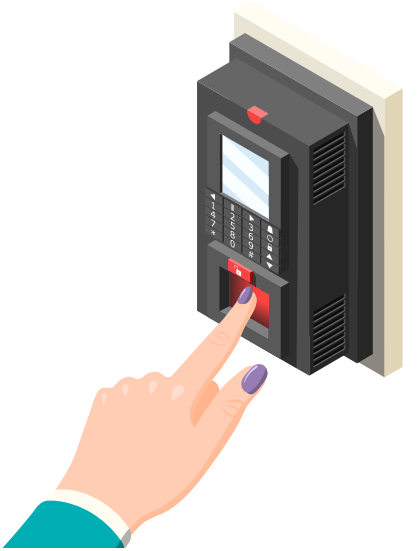
¿Qué tipo de titulares de datos personales acceden a edificios e instalaciones públicas?

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:

- **Empleados:** Titulares adscritos al sujeto obligado que acrediten que son empleados o prestadores de servicios en activo.
- **Visitantes o Usuarios:** Titulares ajenos a la plantilla laboral del sujeto obligado.

¿Qué es el registro de empleados?



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 o establecidas y otros registros de tipo administrativo.

El tratamiento de datos personales de empleados, es distinto al de visitantes ya que en este 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.

Es importante destacar que, el tratamiento de datos personales de proveedores y personal contratado por honorarios, es distinto al de empleados y de visitantes, ya que las relaciones que generan la necesidad de tratamiento son variadas. Además, en caso dado las finalidades del tratamiento de datos se comunican a los 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, que cuenten con horario fijo, apegado a lo establecido en convenios de colaboración celebrados con instituciones educativas.

Como apoyo para elaborar los Avisos de Privacidad en el caso de los Sujetos Obligados, se puede consultar los artículos 66 y 67 de la Ley de Protección de Datos Personales del Estado de Chihuahua y los artículos 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41 y 42 de los Lineamientos de la Ley de Protección de Datos Personales del Estado de Chihuahua.

¿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 empleado, 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?

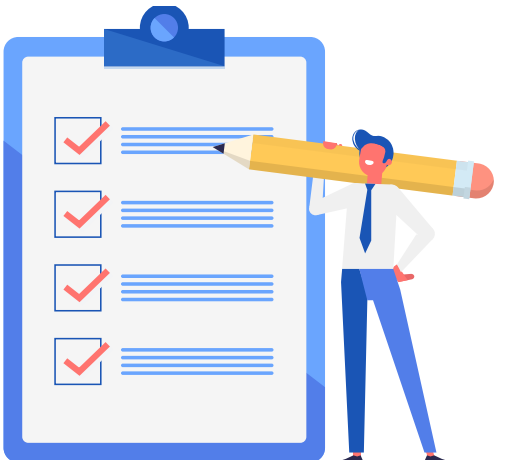
Se emplean controles físicos o electrónicos, en los que se registran datos personales obtenidos de las identificaciones oficiales vigentes o biométricos, de los cuales, el titular respectivo, al plasmar su firma autógrafa en el control físico de registro, otorga su consentimiento expreso al momento de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

Para mayor conocimiento de los datos biométricos se considera que estos son propiedades físicas, fisiológicas, de comportamiento o rasgos de la personalidad, atribuibles a una sola persona y que son medibles. Los datos biométricos que refieren a características físicas y fisiológicas entre los más comunes se encuentran la huella digital, el rostro (reconocimiento facial), la retina, el iris, la geometría de la mano o de los dedos, entre otros. Por otro lado, entre los datos biométricos que refieren a las características del comportamiento y los rasgos de la personalidad, entre los más comunes se encuentran la firma autógrafa, la escritura, la voz, entre otros.

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:

1. ¿En qué fecha y hora se realizó el acceso?
2. ¿Quién realizo el acceso (nombre y apellidos)?
3. ¿Visito a alguna persona en particular?
4. ¿Qué áreas visitó?
5. ¿Empresa o institución de procedencia del visitante?
6. ¿Cuál es el motivo de ingreso a las instalaciones del Sujeto Obligado?
7. ¿A qué hora salió de las instalaciones?
8. ¿Con que documento acreditó su identidad y si lo dejó bajo resguardo de la recepción durante su visita?

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 identificación 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, además de cumplir con su principal finalidad que es ejercer el derecho al voto, es utilizada como documento de identidad, ya que contiene, entre otros, los siguientes datos personales: nombre completo, sexo, fecha de nacimiento, en algunos casos domicilio, entidad federativa, municipio y localidad, firma, fotografía, huella dactilar, Clave Única de Registro de Población, clave de elector, OCR. En ese sentido, el uso de la Credencial para Votar o de los datos contenidos en ella implica un tratamiento de datos personales y, por tanto, la generación de responsabilidades en cuanto a su protección.

Es por ello, que damos cinco recomendaciones básicas para evitar un mal tratamiento de los datos personales contenidos en la Credencial para Votar.

1. No la pidas si no es necesaria.
2. Si la tienes que pedir, no te quedes con fotocopia.
3. Si la tienes que fotocopiar o reproducir, resguárdala con medidas de seguridad y confidencialidad adecuadas.
4. Si ya no es necesaria, suprime los datos personales.
5. Mide el riesgo: entre más datos personales trates más obligaciones tendrás que cumplir.
6. En su caso fijar temporalidad de conservación breve.

¿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 17 de la Ley de Protección de Datos Personales del Estado de Chihuahua y el artículo 5 de los Lineamientos de la Ley de Protección de Datos Personales del Estado, 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.

  El artículo 26, párrafo II dispone que por regla general, todo responsable está obligado a cumplir con el principio de información y poner a disposición del titular el aviso de privacidad de conformidad con lo dispuesto en los artículos 11 fracción II, 63, 64 y 65 de la Ley Estatal, con independencia de que no se requiera el consentimiento del titular para el tratamiento de sus datos personales.

- **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 mayor entendimiento y dar cumplimento con el principio de licitud el Sujeto Obligado deberá, Identificar el marco normativo (leyes, tratados o acuerdos internacionales, reglamentos, lineamientos, entre otros, con sus respectivos artículos) que faculta a la unidad administrativa a tratar los datos personales para cada una de las finalidades, y aquél que regula el tratamiento respectivo, a manera de ejemplo son, los Reglamentos Internos o Estatutos Orgánicos de los Sujetos Obligados.

- **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.

  Como recomendación, el Sujeto Obligado deberá verificar que los datos personales no se obtengan con dolo, mala fe o negligencia y debe verificar los tratamientos que realiza el sujeto obligado, a fin de confirmar que los mismos no den lugar a discriminación o trato injusto o arbitrario en contra del titular.

- **PRINCIPIO DE CONSENTIMIENTO:** Se sugiere identificar si los datos serán tratados dentro de alguno de los supuestos previstos por el artículo 20 de la Ley de Protección de Datos Personales del Estado de Chihuahua. 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 11 fracción IX de la Ley de Protección de Datos Personales del Estado de Chihuahua, este deberá solicitar el consentimiento expreso y por escrito de los titulares de los datos, previo a que se recaben, o bien, revisar que se actualice alguno de los supuestos del artículo 20 de la Ley Estatal. Adicionalmente deberá revisar la necesidad y legalidad

del tratamiento de datos personales sensibles para cumplir con la finalidad de que se trate, a fin de que quede debidamente justificada su obtención y uso y verificar que el tratamiento de datos personales no tenga como consecuencia discriminación de los titulares.

Para que el Sujeto Obligado cumpla con el deber de consentimiento deberá en primera instancia solicitar el consentimiento después de que se ponga a disposición del titular el aviso de privacidad y redactar las solicitudes de consentimiento de forma tal que éste sea libre, específico e informado, y que las solicitudes sean concisas e inteligibles, estén en un lenguaje claro y sencillo acorde con el perfil del titular, y se distingan de asuntos ajenos a la protección de datos personales, cuando ello sea necesario.

Así mismo, Definir el tipo de consentimiento que se requiere, según las categorías de datos personales que se vayan a tratar o las disposiciones normativas que regulen el tratamiento, habilitar los mecanismos necesarios para solicitar el consentimiento expreso, en los términos señalados en párrafo anterior, así como documentar su obtención y documentar la puesta a disposición del aviso de privacidad para la obtención del consentimiento tácito.

De la misma forma el Sujeto Obligado deberá solicitar el consentimiento previo a la obtención de los datos personales y después de la puesta a disposición del aviso de privacidad, cuando los datos personales se obtengan directamente de su titular o representante y cuando los datos personales no los proporcione personal o directamente el titular o su representante, el sujeto obligado deberá enviar a los titulares el aviso de privacidad correspondiente al medio de contacto que tenga registrado. Asimismo, deberá informarles que cuentan con un plazo de 5 días hábiles para en su caso manifestar su negativa para el tratamiento de sus datos personales para aquellas finalidades que requieran su consentimiento.

Si el titular no manifiesta su negativa en el plazo de cinco días antes señalado, el sujeto obligado podrá suponer que cuenta con el consentimiento tácito o en el caso del consentimiento expreso, es necesario que el mismo se solicite, ya sea en el cuerpo del aviso de privacidad o en un instrumento aparte. El sujeto obligado no podrá tratar los datos personales si no cuenta con el consentimiento expreso del titular y deberá prever en el procedimiento interno para la atención de solicitudes de derechos ARCO lo relativo a la revocación del consentimiento, según los plazos, requisitos y procedimiento que se establecen para el ejercicio de los derechos de cancelación y oposición.

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, para esto los Sujetos Obligados deberán implementar medidas para que los datos personales se actualicen y, en su caso, corrijan o completen, en las distintas bases de datos que estén a cargo de la unidad administrativa y estas medidas deberán permitir que la modificación de los datos personales sea inmediata, una vez que la unidad administrativa tenga conocimiento de la actualización o corrección a que haya lugar.

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 y deberán establecer los plazos de conservación de los datos personales, para cada uno de los tratamientos, lo cual deberá ser congruente con los plazos de conservación establecidos en los instrumentos de clasificación archivística.

PRINCIPIO DE FINALIDAD: Se deberán señalar claramente la finalidad o finalidades de los datos personales, en finalidades concretas, lícitas, explícitas y legítimas, esto para el tratamiento de datos personales del registro de entradas y salidas de instalaciones del sujeto obligado.

1. **Concretas:** cuando el tratamiento de los datos personales atiende a la consecución de fines específicos o determinados, sin que admitan errores, distintas interpretaciones o provoquen incertidumbre, dudas o confusión en el titular;
2. **Explícitas:** cuando las finalidades se expresan y dan a conocer de manera clara en el aviso de privacidad;
3. **Lícitas:** cuando las finalidades que justifican el tratamiento de los datos personales son acordes con las atribuciones o facultades del responsable, conforme a lo previsto en la legislación mexicana y el derecho internacional que le resulte aplicable, y

4. **Legítimas:** cuando las finalidades que motivan el tratamiento de los datos personales se encuentran habilitadas por el consentimiento del titular, salvo que se actualice alguna de las causales de excepción previstas en el artículo 20 de la Ley de Protección de Datos Personales del Estado de Chihuahua.

- **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.

- **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 se agrega un listado de comprobación y recomendaciones relacionado con este principio:

  1. Prever presupuesto para la instrumentación de programas y políticas de protección de datos personales.
  2. Elaborar un programa de protección de datos personales que contemple el cumplimiento obligatorio al interior de la organización del responsable.
  3. Elaborar y aplicar un programa de capacitación y actualización de los servidores públicos en materia de protección de datos personales, de conformidad con el apartado de Capacitación de este Programa.

4. Establecer un sistema de supervisión y vigilancia interna y/o externa para comprobar el cumplimiento de este programa, incluyendo las medidas de seguridad, que prevea una revisión cada dos años o antes si es necesario por un cambio sustancial en el tratamiento.
5. Establecer procedimientos para recibir y responder dudas y quejas de los titulares, que sea de fácil acceso y con la mayor cobertura posible.
6. Diseñar, desarrollar e implementar las políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales.

- **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.
» En lo concerniente al sistema de gestión de visitantes, se hace el análisis de riesgo, el análisis de brecha, el plan de trabajo, monitoreo y revisión de las medidas de seguridad, en el caso de bitácoras físicas no se desarrollan listas de comprobación, en razón de que se consideran elementos técnicos específicos.

- **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.

ANEXO I
Identificaciones oficiales y datos personales

Para mayor conocimiento se agrega un listado de los documentos oficiales más comunes y el contenido de los datos que se incluyen en estos:

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
- Huella Dactilar
- Código QR

Credencial de 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 hacia 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:

1. 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.

2. Estancia en el inmueble

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

3. 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 a estas pertenecías.
- En caso de que hubiera una retención de identificaciones, se devuelve la identificación oficial a su dueño.

4. 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.

5. 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 y libretas de registro ubicadas en los puntos de acceso a los edificios, donde el titular registra sus datos.
- En ocasiones se complementa un 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.

Sistema electrónico de gestión de visitantes

- No permitir la reproducción total o parcial del contenido de las bitácoras por ningún medio.
- 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 encontrara 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.

Instituto Chihuahuense para la Transparencia y Acceso a la Información Pública

Av. Teofilo Borunda Ortíz No. 2009
Col. Los Arquitos C.P. 31025
Tel. 614 201 33 00

www.ichitaip.org