Anexo al Periódico Oficial

Gobierno del Estado
Libre y Soberano de Chihuahua

Registrado como
Artículo
de segunda Clase de
fecha 2 de Noviembre
de 1927

Todas las leyes y demás disposiciones supremas son obligatorias por el sólo hecho de publicarse en este Periódico.

Responsable: La Secretaría General de Gobierno. Se publica los Miércoles y Sábados.

Chihuahua, Chih., sábado 30 de agosto del 2014. **No. 70**

Folleto Anexo

ACUERDO No. 062

LINEAMIENTOS PARA LA LEY DE PROTECCION DE DATOS PERSONALES DEL ESTADO DE CHIHUAHUA

LIC. CÉSAR HORACIO DUARTE JÁQUEZ, Gobernador Constitucional del Estado Libre y Soberano de Chihuahua, en ejercicio de la facultad que me concede el Artículo 93, Fracción XLI de la Constitución Política del Estado, y con fundamento en el Artículo 1, Fracción VI y 25 Fracción VII de la Ley Orgánica del Poder Ejecutivo del Estado, he tenido a bien emitir el siguiente:

A C U E R D O 062

ARTÍCULO PRIMERO: Publíquese en el Periódico Oficial del Estado el Acuerdo aprobado por el Consejo General del Instituto Chihuahuense para la Transparencia y Acceso a la Información Pública, tomado en sesión extraordinaria celebrada el día 26 de junio de 2014, mediante el cual se aprobaron por unanimidad los Lineamientos para la Ley de Protección de Datos Personales del Estado de Chihuahua.

ARTÍCULO SEGUNDO: Este Acuerdo entrará en vigor al día siguiente de su Publicación en el Periódico Oficial del Estado.

D A D O en el Palacio del Poder Ejecutivo, en la Ciudad de Chihuahua, Chihuahua, a los trece días del mes de agosto del año dos mil catorce.

Sufragio Efectivo: No Reelección

EL GOBERNADOR CONSTITUCIONAL DEL ESTADO

LIC. CÉSAR HORACIO DUARTE JÁQUEZ

EL SECRETARIO GENERAL DE GOBIERNO

RAYMUNDO ROMERO MALDONADO

LINEAMIENTOS PARA LA LEY DE PROTECCIÓN DE DATOS PERSONALES DEL ESTADO DE CHIHUAHUA

EL CONSEJO GENERAL DEL INSTITUTO CHIHUAHUENSE PARA LA TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA, CON FUNDAMENTO EN EL ARTÍCULO 37 FRACCIÓN I, DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES DEL ESTADO DE CHIHUAHUA; Y

CONSIDERANDO

Que el Instituto Chihuahuense para la Transparencia y Acceso a la Información Pública, es un organismo público autónomo, con personalidad jurídica, patrimonio y competencia propios, creado por disposición expresa de la Constitución Política del Estado Libre y Soberano de Chihuahua de conformidad con su artículo 4 Fracción II párrafo IV, para garantizar y hacer efectivo el ejercicio de los derechos de Acceso a la Información Pública y de Protección de Datos Personales.

Que el veintiséis de junio del año dos mil trece, fue publicado por el Ejecutivo del Estado Libre y Soberano de Chihuahua, en el Periódico Oficial del Estado el Decreto 1208/2013 X P.E., por el cual la Sexagésima Tercera Legislatura del Honorable Congreso del Estado de Chihuahua, expide la Ley de Protección de Datos Personales del Estado de Chihuahua.

Que las disposiciones contenidas en la Ley de Protección de Datos Personales del Estado de Chihuahua, son de orden público, interés social y de observancia general en el Estado de Chihuahua y tienen por objeto garantizar la protección de datos personales en posesión de los sujetos obligados, así como establecer los principios, derechos, excepciones, obligaciones y procedimientos que rigen en la materia.

Que de acuerdo con el artículo 37 de la Ley de Protección de Datos Personales del Estado de Chihuahua, Instituto Chihuahuense para la Transparencia y Acceso a la Información Pública, es el órgano encargado de dirigir y vigilar el cumplimiento de la Ley en mención, así como de las normas que de ella deriven; y la autoridad encargada de garantizar la protección y el correcto tratamiento de los datos personales y tiene como atribución, entre otras, la de establecer, en el ámbito de su competencia, políticas y lineamientos de observancia general para el manejo, tratamiento, seguridad y protección de los datos personales en posesión de los sujetos obligados, así como expedir normas que resulten necesarias para el cumplimiento de la Ley.

Que existen en posesión de los sujetos obligados bases de datos personales, que han sido obtenidos en el marco de sus respectivas atribuciones y competencias, para determinados fines, integrados en sus sistemas de información, cuyo manejo, tratamiento y seguridad deben ser garantizados.

Que todo dato personal en posesión de los sujetos obligados debe de ser protegido conforme a la Ley de Protección de Datos Personales del Estado de Chihuahua, motivo por el cual, estos deberán implementar las medidas de seguridad para la protección de los sistemas de datos personales que poseen y

los que en lo sucesivo sean creados, debiendo para ello conducirse conforme a procedimientos y normas que faculten a las personas el ejercicio de los derechos de acceso, rectificación, cancelación y oposición de datos personales (ARCO).

Que atendiendo a las atribuciones con que cuenta el Instituto Chihuahuense para la Transparencia y Acceso a la Información Pública y a fin de fortalecer el marco normativo en materia de protección de datos personales, es necesaria la emisión de Lineamientos para la Protección de Datos Personales en el Estado de Chihuahua, con el objeto de establecer los criterios que normen los procedimientos para atender la recepción, procesamiento, resolución y notificación de las solicitudes de acceso, rectificación, cancelación u oposición de datos personales que formulen los particulares, así como las condiciones y requisitos mínimos para el debido manejo y custodia de los sistemas de datos personales que se encuentren en posesión de los sujetos obligados derivado del ejercicio de sus funciones, a fin de garantizar la protección y el adecuado tratamiento de los mismos, en términos de lo dispuesto por la Ley.

Por lo que en consecuencia de conformidad con el artículo 37, fracción I de la Ley de Protección de Datos Personales del Estado de Chihuahua, se emiten los siguientes:

LINEAMIENTOS PARA LA LEY DE PROTECCIÓN DE DATOS PERSONALES DEL ESTADO DE CHIHUAHUA

TÍTULO PRIMERO DISPOSICIONES GENERALES

CAPÍTULO I DISPOSICIONES GENERALES

Objeto de los Lineamientos.

PRIMERO.- Los presentes lineamientos son de observancia obligatoria para los sujetos obligados a que se refiere el artículo 3 de la Ley de Protección de Datos Personales del Estado de Chihuahua y tienen por objeto establecer las directrices y criterios para la aplicación e implementación de dicha Ley, a fin de garantizar la protección de datos personales y el adecuado tratamiento de los mismos.

Glosario.

SEGUNDO.- Además de las definiciones contenidas en el artículo 3 de la Ley de Protección de Datos Personales para el Estado de Chihuahua, para los efectos de los presentes Lineamientos se entenderá por:

I. **Archivos:** A manera enunciativa, mas no limitativa, los expedientes, reportes, estudios, actas, resoluciones, oficios, correspondencia, acuerdos, directivas, directrices, circulares, contratos, convenios, instructivos, notas, memorandos, estadísticas, o bien cualquier conjunto de documentos en cualquier soporte, impreso, sonoro, visual, electrónico, informático u holográfico, etc., que son producidos o recibidos, por los sujetos obligados en el ejercicio de sus atribuciones.

II. **Autentificación:** Comprobación de la identidad de la persona autorizada por el sujeto obligado para el tratamiento de datos personales.

III. **Bloqueo:** Identificación y conservación de datos personales con el propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo, legal o contractual, de prescripción de éstas o, en su caso, la procedencia de la eliminación de éstos de un sistema de datos personales a petición del titular. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación del sistema a que correspondan.

IV. **Cancelación:** Eliminación de determinados datos de un sistema de datos personales previo bloqueo de los mismos; como consecuencia del ejercicio de los derechos de cancelación u oposición.

V. **Cesionario:** persona física o moral, pública o privada, a la que un sujeto obligado realice una cesión de datos personales. El cesionario puede ser usuario o destinatario de datos personales.

VI. **Costos de reproducción:** El monto de los derechos que deban cubrir los particulares en caso de reproducción de la información, derivada del costo de materiales utilizados; en los términos de la Ley o normatividad respectiva.

VII. **Derechos ARCO:** Son los derechos de acceso, rectificación, cancelación y oposición de los datos personales.

VIII. **Derecho de acceso a datos personales:** Es la Prerrogativa del interesado a que se le informe si sus datos personales están siendo objeto de tratamiento, la finalidad del tratamiento que, en su caso, se esté realizando, así como la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de los mismos.

IX. **Derecho de cancelación de datos personales:** Prerrogativa del interesado a solicitar que se eliminen los datos que resulten inadecuados o excesivos en el sistema de datos personales de que se trate, sin perjuicio de la obligación de bloquear los datos conforme a la Ley y a los presentes Lineamientos.

X. **Derecho de oposición al tratamiento de datos personales:** Prerrogativa del interesado a solicitar que no se lleve a cabo el tratamiento de sus datos personales para un fin determinado o cese el mismo.

XI. **Derecho de rectificación de datos personales:** Prerrogativa del interesado a solicitar que se modifiquen los datos que resulten inexactos o incompletos, con respecto a la finalidad para la cual fueron obtenidos. Los datos serán considerados exactos si corresponden a la situación actual del interesado.

XII. **Destinatario:** Ente Público al que un sujeto obligado realice una cesión o transmisión de datos personales, en virtud de una disposición legal.

XIII. **Disociación de datos:** Tratamiento o procedimiento mediante el cual los datos personales contenidos en un sistema de datos no pueden asociarse a sus Titulares, ni permitir por su estructura, contenido o grado de desagregación, obtener la identificación individual de los mismos.

XIV. **Documento de seguridad:** Instrumento que establece las medidas y procedimientos administrativos, físicos y técnicos de seguridad aplicables a los sistemas de datos personales necesarios para garantizar la protección, confidencialidad, integridad y disponibilidad de los datos contenidos en dichos sistemas.

XV. **Encargado:** Servidor Público que labora para el ente público y que al interior de éste, en ejercicio de sus atribuciones mediante procedimiento establecido realiza tratamiento de datos personales de forma cotidiana y por cuenta del responsable.

XVI. **Enlace:** Servidor público designado por el titular del ente, que fungirá como vínculo entre el sujeto obligado y el Instituto para atender los asuntos relativos a la Ley de la materia, con función coordinadora de los esfuerzos de aquel en materia de protección de datos.

XVII. **Fuente de acceso público:** Aquella cuya consulta pueda ser realizada por cualquier persona, y no impedida por una norma limitativa, sin más exigencia que, en su caso, el pago que genere el acceso a determinado medio de información. Tendrán el carácter de fuente de acceso público los Registros Públicos, los diarios, periódicos y boletines gubernamentales, así como todo otro medio oficial de difusión.

XVIII. **Incidencia:** Cualquier acontecimiento o anomalía que afecte o pudiera afectar la seguridad de los sistemas de datos personales.

XIX. **Interesado:** Persona física titular de los datos personales objeto de tratamiento.

XX. **Instituto:** Instituto Chihuahuense para la Transparencia y acceso a la Información Pública.

XXI. **Ley:** Ley de Protección de Datos Personales del Estado de Chihuahua.

XXII. **Lineamientos:** Lineamientos para la Ley de Protección de Datos Personales del Estado de Chihuahua.

XXIII. **Medio o Sistema Electrónico:** Sistema electrónico establecido por el Instituto mediante el cual las personas podrán presentar sus solicitudes de acceso, rectificación, cancelación y oposición de datos personales y sistema único para el registro y captura de todas las solicitudes recibidas por los sujetos obligados a través de los medios señalados en la Ley de Protección De Datos Personales del Estado de Chihuahua, así como para la recepción de los recursos de revisión que en su caso se interpongan contra las resoluciones a tales solicitudes.

XXIV. **Protección de datos:** La salvaguarda debida a las personas contra la posible utilización, en forma no autorizada, de sus datos; también es la protección de los derechos fundamentales y libertades de los ciudadanos contra el almacenamiento y posterior cesión de sus datos personales que afecte su intimidad.

XXV. **Registro Electrónico de Sistemas de Datos Personales:** Aplicación informática desarrollada por el Instituto para la inscripción de los Sistemas de Datos Personales en posesión de los sujetos obligados, registro del cual se obtiene una identificación alfanumérica.

XXVI. **Responsable de seguridad:** El servidor público al que el responsable del sistema de datos personales asigna formalmente la función de coordinar y controlar las medidas de seguridad aplicables al mismo.

XXVII. **Sistema de Datos Personales:** conjunto organizado de datos que estén en posesión de los sujetos obligados, contenidos en archivos, registros, ficheros, bases o bancos de datos, que permita el acceso con arreglo a criterios determinados, cualquiera que fuere la modalidad de su creación, almacenamiento, organización o acceso.

XXVIII. **Solicitud de datos personales:** Escrito libre o en formato emitido por el Instituto mediante el cual se ejerce el derecho de protección de datos personales por los interesados o sus representantes legales, debidamente acreditados.

XXIX. **Soporte electrónico:** Medio de almacenamiento al que se pueda acceder sólo mediante el uso de algún aparato con circuitos electrónicos que procese su contenido para examinar, modificar o almacenar los datos personales, incluidos los microfilms.

XXX. **Soporte físico:** Medio de almacenamiento inteligible a simple vista, es decir, que no requiere de ningún aparato que procese su contenido para examinar, modificar o almacenar los datos personales.

XXXI. **Supresión:** Actividad consistente en eliminar, borrar o destruir de un sistema de datos personales, una vez concluido el periodo de bloqueo y bajo las medidas de seguridad previamente establecidas por el responsable, el o los datos personales a que se refiera una solicitud de datos personales o respecto de los que se haya cumplido su temporalidad con arreglo a su finalidad específica.

XXXII. **Suspensión y Bloqueo o Inmovilización de los sistemas:** Medida cautelar ordenada por el Instituto consistente en la interrupción temporal del tratamiento de determinados datos personales contenidos en un sistema de datos personales.

XXXIII. **Transmisión:** Toda entrega total o parcial de sistemas de datos personales realizada por las dependencias y entidades a cualquier persona distinta al Titular de los datos, mediante el uso de medios físicos o electrónicos tales como la interconexión de computadoras, interconexión de bases de datos, acceso a redes de telecomunicación, así como a través de la utilización de cualquier otra tecnología que lo permita.

XXXIV. **Usuario:** Persona física, moral de derecho privado o negociación comercial externa al sujeto obligado, que facultado por un instrumento jurídico o expresamente autorizado por el Responsable y por cuenta de éste, le presta servicios para tratar datos personales y en función del cual accede a los sistemas de datos personales, para su tratamiento, sin posibilidad de agregar o modificar su contenido.

CAPÍTULO II
DE LOS PRINCIPIOS RECTORES
DE LA PROTECCIÓN DE DATOS PERSONALES

Principios.

TERCERO.- En los términos del artículo 7 de la Ley, los sujetos obligados en el tratamiento de los datos personales conforme a los principios establecidos en aquel, estarán igualmente a lo siguiente:

En cuanto al **Principio de Calidad de datos:** que se refiere a que para su tratamiento, los datos personales deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido. Los datos recabados deberán de responder con veracidad a la situación actual del interesado.

Para su tratamiento, se entenderá que los datos contenidos en el sistema de datos personales son:

a) **Ciertos:** Cuando los datos personales que lo integran se mantienen actualizados, de tal manera que no se altere la veracidad de la información de forma que traiga como consecuencia una afectación a su titular.
b) **Adecuados:** Cuando se observa una relación proporcional entre los datos recabados y la finalidad del tratamiento.
c) **Pertinentes:** Cuando su tratamiento es realizado por el personal autorizado para el cumplimiento de las atribuciones de los sujetos obligados que los hayan recabado;
d) **No excesivos:** Cuando la información solicitada al titular de los datos es la estrictamente necesaria para cumplir con los fines para los cuales se hubieran recabado.

Respecto al **Principio de Licitud:**Para garantizar un tratamiento, leal de los datos personales, se considera tratamiento lícito de los sistemas de datos personales, aquel que cuente con el consentimiento inequívoco, expreso y por escrito del interesado al que se refiere el artículo 29 de la Ley, así como a que la posesión de dichos sistemas debe obedecer exclusivamente al ejercicio de las atribuciones legales y/o reglamentarias de cada sujeto obligado debiendo obtenerse a través de los medios previstos al efecto por las disposiciones atinentes.

Los sistemas de datos no podrán tener finalidades contrarias a las leyes o a la moral pública y en ningún caso los datos que contengan podrán ser utilizados con finalidades distintas o incompatibles con aquellas que motivaron su obtención, misma que debe ser explícita, determinada y legal. No se considerará incompatible el tratamiento posterior de los datos personales con fines históricos, estadísticos o científicos.

En relación con el **Principio de Consentimiento:** éste se refiere a la necesaria manifestación de la voluntad, mediante el cual el interesado consiente en cada caso de manera independiente, tanto el tratamiento como la transmisión de sus datos personales, los cuales deben otorgarse de forma libre, inequívoca, específica e informada; salvo los casos y excepciones previstas por la Ley, considerados conforme a lo siguiente:

a) Libre: Cuando es obtenido sin coacción alguna, dolo, engaño ni mediante la intervención de vicio alguno de la voluntad.
b) Inequívoco: Cuando existe expresamente una acción que implique sin lugar a dudas su otorgamiento y los alcances del mismo.
c) Específico: Cuando se otorga referido a una finalidad determinada pudiendo referirse únicamente al acopio de datos o además para su transmisión.
d) Informado: Cuando se otorga con conocimiento de las finalidades para las que el mismo se concedió, en función de la información que se proporcione al interesado.

Por lo que hace al **Principio de Información:** Bajo este principio se ampara el derecho de los titulares a conocer los tratamientos que sobre sus datos se hacen, aún y cuando el consentimiento se excepcione en términos de la Ley, y

corresponde a la obligación del responsable del tratamiento de hacer del conocimiento del interesado, mediante la pertinente cláusula o leyenda informativa, aquellos extremos dispuestos por la fracción IV del artículo 7 de la Ley.

Tocante al **Principio de Disponibilidad:** El cual se desprende de la fracción V del artículo 7 de la Ley, e implica que los datos personales deben ser almacenados y organizados de forma tal que, durante el tiempo que permanezcan en posesión de los sujetos obligados, permitan en todo momento el ejercicio de los derechos de acceso, rectificación, cancelación u oposición, conforme a lo previsto por la Ley y los presentes Lineamientos.

Con referencia al **Principio de Confidencialidad:** Consiste en el deber a cargo de toda persona que intervenga en cualquier fase del tratamiento de datos personales, que implica la obligación de guardar absoluta secrecía respecto de los mismos, deber que subsistirá aún después de finalizada la relación que haya generado el tratamiento.

Con relación al principio de confidencialidad, se entenderá que los datos personales son:

a) **Irrenunciables:** Esto es que el interesado está imposibilitado de privarse voluntariamente de las garantías que le otorga la legislación en materia de protección de datos personales.
b) **Intransferibles:** El interesado es el único titular de los datos y éstos no pueden ser transferidos a otra persona, salvo lo dispuesto por la Ley y previo consentimiento de éste.
c) **Indelegables:** Sólo el interesado tiene la facultad de decidir a quién transmite sus datos personales.

El deber de secrecía y el principio de confidencialidad se considerarán equiparables, por lo que el responsable y toda persona que intervenga en cualquier fase del tratamiento de los datos personales en posesión de los sujetos obligados, están constreñidos a guardar absoluta secrecía respecto de los mismos, obligación que subsistirá aun después de finalizada la relación que dio origen al tratamiento de datos.

Únicamente en los casos que se justifiquen ya sea por resolución judicial, por una situación prevista en la Ley, por razones de seguridad pública, seguridad nacional o salud pública, se podrá relevar a responsables, encargados, usuarios, destinatarios o toda persona que intervenga en cualquier fase del tratamiento de tal deber.

En lo que concierne al **Principio de Seguridad:** Deberán establecer procesos específicos tendientes a garantizar que únicamente el responsable del sistema de datos personales, o en su caso, los encargados y usuarios autorizados puedan llevar a cabo el tratamiento de los datos personales, además de adoptar las medidas de seguridad necesarias que a su vez garanticen la integridad, confiabilidad, confidencialidad y disponibilidad de los mismos, mediante acciones que eviten su alteración, pérdida, transmisión o acceso no autorizado, que prevengan su utilización indebida.

En cuanto al **Principio de Proporcionalidad:** Se refiere a un atributo que debe revestir al proceso de obtención de datos, que implica una necesaria relación entre las atribuciones del sujeto obligado, su ámbito de aplicación y las finalidades expresas a ellas afectas con la cantidad de datos personales que para su cumplimiento sea necesario obtener de los titulares en la creación de un sistema de datos personales determinado.

Respecto al **Principio de Temporalidad:** Se refiere a que los datos personales deberán ser destruidos o cancelados cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales fueron recolectados; no obstante, dichos datos podrán conservarse durante el tiempo en que pueda exigirse algún tipo de responsabilidad derivada de una relación u obligación jurídica o de la ejecución de un contrato.

Se exceptúa el tratamiento que con posterioridad se les dé con objetivos estadísticos o científicos, previo procedimiento de disociación en términos de lo previsto por la Ley; y únicamente podrán ser conservados de manera íntegra, permanente y sujetos a tratamiento los datos personales con fines históricos observando para tales efectos la normatividad estatal vigente en materia de Archivos y el correspondiente catálogo de disposición documental.

TÍTULO SEGUNDO
DE LOS SISTEMAS DE DATOS PERSONALES

CAPÍTULO I
DISPOSICIONES GENERALES

Tipos de sistemas.

CUARTO.- Conforme a lo dispuesto en el artículo 6 fracción XIII de la Ley, y Lineamiento segundo fracción XXVII de los presentes Lineamientos, los sistemas de datos personales se distinguen por su forma de creación o almacenamiento en:

I. **Físicos:** Conjunto ordenado de datos de carácter personal relativos a personas físicas que para su tratamiento están contenidos en soporte físico, sean manuales, impresos, sonoros, magnéticos, visuales u holográficos, estructurado conforme a criterios específicos que permitan acceder sin esfuerzos desproporcionados a su contenido; y

II. **Automatizados:** Conjunto ordenado de datos de carácter personal que permita acceder a su contenido mediante el uso de alguna herramienta o dispositivo tecnológico.

Categorías de los datos personales

QUINTO.- De manera enunciativa, más no limitativa, se clasifican los datos personales contenidos en los sistemas, conforme a las siguientes categorías:

I. Datos identificativos: que corresponde a toda aquella información o dato que haga identificable a una persona como: el nombre, domicilio, número telefónico particular, número telefónico celular particular, firma, clave del Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP), Matrícula del Servicio Militar Nacional, Número de pasaporte, lugar y fecha de nacimiento, nacionalidad, edad, fotografía, media filiación y demás datos de similar naturaleza.

II. Datos electrónicos: que corresponde a aquella información asociada a una persona física que sea utilizada para su identificación en internet u otra red de comunicaciones electrónicas; como lo son: el correo electrónico no oficial, dirección IP (Protocolo de Internet), dirección MAC (dirección Media Access Control o dirección de control de acceso al medio), así como el nombre del usuario, contraseñas, firma electrónica; o cualquier otra información empleada por cualquier persona, para su identificación en ambientes virtuales.

III. Datos laborales: es toda aquella información que pertenezca a una persona, asociada a sus actividades y desarrollo laboral o profesional, entre otros: datos sobre su reclutamiento y selección, nombramiento, incidencia, capacitación, actividades extracurriculares, datos sobre la experiencia, desarrollo profesional, referencias laborales, referencias personales, solicitud de empleo, hoja de servicio, y demás datos de similar naturaleza.

IV. Datos patrimoniales: corresponde a toda aquella información de las personas, referente a los bienes, derechos y obligaciones de contenido patrimonial, entre otros, la correspondiente a bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, fianzas, servicios contratados, referencias personales crediticias o patrimoniales y demás datos de similar naturaleza.

V. Datos sobre procedimientos administrativos y/o jurisdiccionales: la información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal, fiscal, administrativa o de cualquier otra rama del Derecho.

VI. Datos académicos: Toda aquella información de las personas, referente a su trayectoria educativa entre otra la que se incluya en el currículum vitae, evaluaciones, calificaciones, títulos, cédula profesional, certificados, constancias, reconocimientos y demás datos de similar naturaleza.

VII. Datos de tránsito y movimientos migratorios: información relativa al tránsito de las personas dentro y fuera del país, así como información migratoria.

VIII. Datos sobre la salud: el expediente clínico de cualquier atención médica, referencias o descripción de sintomatologías, detección de enfermedades, incapacidades médicas, discapacidades, intervenciones quirúrgicas, vacunas, consumo de medicamentos, consumo de estupefacientes, uso de aparatos oftalmológicos, ortopédicos, auditivos, prótesis, así como el estado mental o físico de la persona y demás datos de similar naturaleza.

IX. Datos biométricos: es toda aquella información que se obtenga por medio de la aplicación de técnicas para la identificación de una persona a través de sus características fisiológicas y de comportamiento, como lo son: huellas dactilares, ADN, geometría de la mano, características de iris y retina y demás datos de similar naturaleza.

X. Datos especialmente protegidos (sensibles): aquellos que su conocimiento pueda traducirse en prácticas o acciones discriminatorias en perjuicio de su titular, tales como: origen étnico o racial, características morales o emocionales, ideología, opiniones políticas, creencias, convicciones religiosas y filosóficas, sexualidad, hábitos sexuales de las personas y demás datos de similar naturaleza.

XI. Datos afectivos y familiares: es toda aquella información de una persona referente a sus sentimientos y emociones, así como la relativa a su entorno familiar, como son: estado civil, número de hijos, dependientes económicos, beneficiarios, referencias familiares y demás datos de similar naturaleza.

XII. Datos personales de naturaleza pública: aquellos que por mandato legal expreso sean accesibles al público, entre otros aquella que esté comprendida dentro de la información pública de oficio, en los términos de la Ley de Transparencia y Acceso a la Información Pública y su Reglamento ambos del estado de Chihuahua, por ejemplo, las percepciones de servidores públicos, correo electrónico institucional, nombre de beneficiarios de programas sociales, entre otra.

Contenido de los acuerdos de creación, modificación y supresión de sistemas.

SEXTO.- Para la creación, modificación o supresión de sistemas de datos personales conforme a su ámbito de competencia, los sujetos obligados, a través de su titular u órgano competente, deberá emitir el correspondiente acuerdo, el cual, a efecto de cumplir con lo dispuesto por el artículo 11 de la Ley, deberá contener:

I. En lo referente a la fracción I del artículo 11 de la Ley deberá señalarse: La identificación del sistema de datos personales, indicando su denominación y normativa aplicable en función de su ámbito competencial, así como la descripción de la finalidad y usos previstos. Se deberá fundar y motivar las razones de la recolección de datos que justifique su tratamiento.

II. En lo referente a las fracciones II y III del artículo 11 de la Ley deberá señalarse: El origen de los datos, indicando el conjunto de personas sobre las que se pretende obtener datos de carácter personal, o que resulten obligados a suministrarlos; su procedencia (propio interesado, representante, sujeto obligado, etc.).

III. En lo referente a la fracción IV del artículo 11 de la Ley deberá precisarse: El procedimiento de recolección de los datos personales, tales como, método, formularios, interfaces de Internet, transmisión electrónica, o cualquiera otro que lo permita.

IV. En lo referente a la fracción V del artículo 11 de la Ley deberá precisarse: La estructura básica del sistema de datos personales mediante la descripción detallada de los datos identificativos que contiene y, en su caso, de los datos especialmente protegidos, así como las restantes categorías de datos de carácter personal incluidas en el mismo y la modalidad de tratamiento previsto para su explotación (manual o automatizado). En su caso, señalar los datos de carácter obligatorio y facultativo.

V. En lo referente a la fracción VI del artículo 11 de la Ley deberán precisarse: Las cesiones de datos que en ejercicio de sus atribuciones se tengan previstas, indicando, en su caso, los destinatarios o usuarios.

VI. En lo referente a la fracción VII del artículo 11 de la Ley deberá precisarse: La identificación de la unidad administrativa a la que corresponde el sistema de datos personales, así como el cargo del responsable de los datos personales.

VII. En cuanto al contenido de la fracción VIII del artículo 11 de la Ley, deberá señalar domicilio oficial y dirección electrónica de la Unidad de Información ante la cual se presentarán las solicitudes para ejercer los derechos de acceso, rectificación, cancelación y oposición, así como la revocación del consentimiento.

VIII. En lo tocante al plazo de conservación, establecido en la fracción IX del artículo 11 de la Ley, se indicará el periodo o lapso de preservación de los datos personales con base en las disposiciones archivísticas aplicables, y vigencia documental en los archivos de trámite, concentración e histórico según su soporte (manual o automatizado);

IX. Indicación del nivel de seguridad que resulte aplicable conforme al tipo y categoría de datos personales que contenga, y que puede ser: básico, medio o alto.

Además, en los casos de tratamiento de datos personales sensibles, deberán publicarse las razones de interés general que justifiquen dicho tratamiento, las cuales deberán obedecer a situaciones reales, debidamente fundadas y motivadas por los sujetos obligados.

En el caso de sistemas de datos personales relacionados con programas o proyectos que se renuevan periódicamente, se considerará como el mismo sistema y sólo se registrarán las modificaciones respecto del programa anterior.

Todos los acuerdos de creación de sistemas de datos personales emitidos por los sujetos obligados deberán registrarse ante el Instituto Chihuahuense para la Transparencia y Acceso a la Información Pública, dentro de los diez días siguientes a la fecha de su creación.

SÉPTIMO.- El acuerdo mediante el cual se determine modificar un sistema de datos personales, deberá indicar las modificaciones producidas en cualquiera de las fracciones a que se hace referencia en el numeral 11 de la Ley, y conforme al sexto de los presentes Lineamientos.

Dicha modificación también deberá ser notificada al Instituto, dentro de los diez días hábiles siguientes a su emisión, a efecto de que este se pronuncie al respecto en un plazo similar. Vencido el plazo anterior y de no existir pronunciamiento por parte del Instituto, el responsable deberá inscribir la modificación acordada dentro del plazo de cinco días hábiles en el Registro Electrónico de Sistemas de Datos Personales.

La reorganización de los sistemas de datos personales, será considerada una modificación siempre y cuando los documentos permanezcan en posesión del mismo sujeto obligado y no implique dar de baja documentos en términos de la normatividad archivística correspondiente.

OCTAVO.- En caso de que el titular de la Unidad de Información del sujeto obligado o, en su defecto, el responsable del sistema de datos personales determine la supresión de un sistema mediante la publicación del acuerdo respectivo en su correspondiente página de internet, dicha supresión deberá ser notificada al Instituto dentro de los diez días hábiles siguientes, a efecto de que se proceda a la cancelación de la inscripción en el registro correspondiente.

En los acuerdos que se emitan para la supresión de sistemas de datos personales, se establecerá el destino que vaya a darse a los datos contenidos en los mismos o, en su caso, las previsiones que se adopten para su destrucción, de conformidad con la Ley de Archivos del Estado de Chihuahua y demás normatividad que resulte aplicable.

No procederá la supresión de los sistemas de datos personales cuando exista una disposición expresa en una Ley que exija su conservación. O cuando pueda exigirse algún tipo de responsabilidad derivada de una relación u obligación jurídica o de la ejecución de un contrato.

En los casos de transferencia de sistemas de datos personales contenidos en archivos a consecuencia de la extinción de la naturaleza y facultades de sujetos obligados, o en virtud de la creación de algún sujeto obligado al cual se transfieran aquellas, procederá la supresión de dichos sistemas en términos de la Ley y de los presentes Lineamientos, a fin de dar paso a su transferencia e integración al ente público creado, bajo la modalidad de creación de sistemas de datos personales a los que se dará tratamiento en lo sucesivo.

CAPÍTULO II
DEL REGISTRO DE SISTEMAS DE DATOS PERSONALES

Del Órgano técnico.

NOVENO.- Para el registro de Sistemas de Protección de Datos Personales, el Instituto contará con un órgano técnico, cuyo objeto primordial es llevar el registro sobre la creación, modificación, existencia, supresión, reorganización y finalidad de sistemas de datos personales en poder de sujetos obligados, en términos de la Ley.

DÉCIMO.- Será objeto de registro lo siguiente:

I. Los sistemas de datos personales existentes en posesión de los sujetos obligados, previo a la entrada en vigor de la Ley.

II. Los acuerdos de creación de sistemas de datos personales.
III. Los acuerdos de modificación o actualizaciones que realicen los sujetos obligados a los sistemas de datos personales, así como la reorganización de dichos sistemas.
IV. Los datos relativos a los sistemas de datos que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición.
V. Los acuerdos de supresión de sistemas de datos personales.

DÉCIMO PRIMERO.- Para el registro de Sistemas de Datos Personales, el Instituto habilitará en su página web una plataforma denominada Registro Estatal de Sistemas de Datos Personales RESDAP, a través de la cual los sujetos obligados tendrán posibilidad de llevar a cabo el registro de los Sistemas de Datos Personales y los informes que deban rendir en los términos de los presentes Lineamientos.

De los campos del registro de Sistemas de Datos Personales

DÉCIMO SEGUNDO.- Sin perjuicio de lo establecido en el artículo 14 de la Ley, el registro de cada Sistema de Datos Personales contendrá los siguientes campos:

I. Identificación y naturaleza jurídica del sujeto obligado a cuyo cargo se encuentre la base de datos, nombre del Sistema y fecha de creación.
II. Naturaleza de la información. Se refiere al origen de los datos personales, el grupo de interesados sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, así como los datos personales de cada categoría de datos personales a que se refiere el Lineamiento Quinto.
III. Objetivos para los cuales se utiliza la información. Se refiere al fin, propósito o intención con la que se recaban los datos personales.
IV. Medidas que deben tomarse si se desea tener acceso al expediente. Se refiere a las normas y/o procedimientos establecidos por el sujeto obligado.
V. Finalidad y periodo para el que se mantiene cada tipo de registro. Se refiere al lapso durante el cual se conservará cada tipo de registro del sistema de datos personales y la finalidad es el cumplimiento de la norma que obliga a la conservación temporal o permanente de la información.
VI. Personas facultadas para acceder a los datos personales contenidos en los registros y las condiciones para ello. Se refiere al personal autorizado del sujeto obligado –Responsable, enlace, usuario o destinatario, encargado- y a los requisitos o requerimientos para el manejo o tratamiento de los datos personales.
VII. Nombre, correo electrónico, dirección, teléfono y cargo del responsable, así como nombre de los usuarios. Se refiere a los datos institucionales específicos del responsable del Sistema de Datos Personales y de los usuarios.
VIII. Forma de recopilación y actualización de datos. Se refiere al procedimiento de obtención de los mismos ya sea mediante formulario, internet, transmisión electrónica, vía telefónica o directa y los mecanismos implementados para su actualización.

IX. Destino de los datos y personas físicas o morales a las que pueden ser transmitidos. Se refiere a la utilidad, interés u objeto para el que se requiere la información y los nombres de las personas, dependencias o entidades públicas a las que pueden ser transmitidos.

X. Modo de interrelacionar la información registrada. Se refiere a las distintas áreas o departamentos del sujeto obligado que se comunican o participan entre sí la misma información, para su utilización y aprovechamiento.

XI. Normatividad aplicable al sistema. Se refiere a las diversas disposiciones normativas que regulan de manera específica la actividad atinente del sujeto obligado que sirven de fundamento para el tratamiento de los datos personales, la creación, modificación o supresión del sistema de datos personales, así como para su posible cesión.

XII. Medidas de seguridad. Se refiere a indicar el nivel de seguridad aplicable al sistema de datos personales: básico, medio o alto.

DÉCIMO TERCERO.- Los responsables de los sistemas de datos personales en posesión de los sujetos obligados a través de su enlace en su caso, deberán inscribir dichos sistemas en el Registro Electrónico de Sistemas de Datos Personales habilitado por el Instituto, en un plazo no mayor a diez días hábiles siguientes a la publicación de su creación en su página de internet.

CAPÍTULO III
DEL DEBER DE INFORMACIÓN

Del aviso de privacidad.

DÉCIMO CUARTO.- A efecto de cumplir con lo previsto en el artículo 15 de la Ley, el sujeto obligado en el momento en que recabe los datos personales, deberá hacer del conocimiento del interesado las advertencias a las que se refieren las fracciones de dicho artículo, lo cual hará constar en el aviso de privacidad.

Contenido del aviso de privacidad

DÉCIMO QUINTO.- El aviso de privacidad debe ser redactado de forma tal que su lectura sea clara y de fácil comprensión y contendrá, además de lo establecido en las fracciones del artículo 15 de la Ley, la siguiente información:

a) Nombre y domicilio oficial del sujeto obligado, así como el nombre del Responsable.

b) Nombre, área de adscripción del Responsable y denominación de los Sistemas de Datos Personales.

c) Señalar el medio por el cual se están obteniendo los datos personales, es decir, físico o electrónico.

d) Las finalidades del tratamiento de los datos personales.

e) Indicar la o las categorías en las que se encuentran los datos personales recabados.

f) Los procedimientos o mecanismos que el Responsable ofrezca a los Titulares para limitar el uso o divulgación de los datos;

g) Los medios para ejercer los derechos de acceso, rectificación, cancelación u oposición, de conformidad con lo dispuestos en la Ley y en estos Lineamientos.

h) Indicar a los Titulares, en su caso, las transferencias a las que pueda ser susceptible la información, para que en su caso manifieste su consentimiento expreso. Sin perjuicio de la posibilidad de solicitar la revocación de su consentimiento respecto del tratamiento de sus datos personales, mediante escrito que presente ante la Unidad de Información.

i) El procedimiento y medio por el cual el Responsable comunicará a los Titulares de cambios que pudiesen hacer al Aviso de Privacidad, de conformidad con lo previsto en estos Lineamientos; y

j) La facultad que tiene el Titular para interponer recurso de revisión.

DÉCIMO SEXTO.- El Aviso de Privacidad deberá estar a disposición de los Titulares de datos personales, en la Página Principal del sujeto obligado, quien puede adoptar adicionalmente otras medidas para la difusión del aviso.

DÉCIMO SÉPTIMO.- En el caso de datos personales que no hayan sido obtenidos del titular y resulte material o jurídicamente imposible cumplir con el deber de información o bien su cumplimiento requiera de esfuerzos desproporcionados o implique un costo excesivo, ya sea porque se carezca de datos de contacto con los titulares, porque los mismos se encuentren desactualizados, incorrectos, incompletos o inexactos o de la antigüedad de los datos, los sujetos obligados podrán implementar mecanismos alternos para cumplir con dicho deber de información a través de medios masivos de comunicación u otros medios de amplio alcance, tales como diarios de circulación local, página de Internet del sujeto obligado e informar de ello al Instituto.

Modelo de aviso de privacidad.

DÉCIMO OCTAVO.- Sin perjuicio de la modalidad mediante la cual los sujetos obligados recaben datos personales, éstos deberán utilizar el siguiente modelo de aviso de privacidad para informar al interesado de las advertencias a que se refiere el artículo 15 de la Ley.

"Aviso de privacidad

Los datos personales recabados serán protegidos, incorporados y tratados en el Sistema de datos personales *(nombre del sistema de datos personales),* ***con fundamento en*** *(fundamento legal que faculta al sujeto obligado para recabar los datos personales),* ***cuya finalidad es*** *(describir la finalidad del sistema)* ***y podrán ser transmitidos a*** *(destinatario) con la finalidad de (finalidad de la transmisión),* ***además de otras transmisiones previstas en la Ley de Protección de Datos Personales del Estado de Chihuahua.***

Los datos marcados con un asterisco (*) son obligatorios y sin ellos no podrá acceder al servicio o completar el trámite *(indicar el servicio o trámite de que se trate)*

Asimismo, se le informa que sus datos no podrán ser difundidos sin su consentimiento expreso, salvo las excepciones previstas en la Ley.

El responsable del Sistema de Datos Personales es *(nombre y cargo del responsable),* ***y la dirección donde podrá ejercer sus derechos de acceso, rectificación, cancelación y oposición, así como la revocación del consentimiento es*** *(indicar el domicilio de la Unidad de Información correspondiente).*

El interesado podrá dirigirse al Instituto Chihuahuense para la Transparencia y Acceso a la Información Pública, donde recibirá asesoría sobre los derechos que ampara la Ley de Protección de Datos Personales del Estado de Chihuahua, al teléfono: (01) (614) 201-3300 y (01) (614) 201-3301 o www.ichitaip.org.mx"

DÉCIMO NOVENO. Los sujetos obligados que recaben datos personales a través de un servicio de orientación telefónica, u otros medios o sistemas, deberán establecer un mecanismo por el que se informe previamente a los particulares que sus datos personales serán recabados, la finalidad de dicho acto así como el tratamiento al cual serán sometidos, cumpliendo con lo establecido en el Décimo Cuarto de los presentes Lineamientos. Salvo lo dispuesto en el artículo 21 de la Ley y en aquellos supuestos que impliquen la movilización, acción o respuesta inmediata de cuerpos de emergencias, sin perjuicio de cumplir posteriormente con el deber de información.

CAPÍTULO IV
DE LAS MEDIDAS DE SEGURIDAD

VIGÉSIMO.- Las medidas de seguridad aplicables a los sistemas de datos personales responderán a los niveles establecidos en la Ley para cada tipo de datos. Dichas medidas deberán tomar en consideración las recomendaciones, que en su caso, emita el Instituto para este fin, con el objeto de garantizar la confidencialidad, integridad y disponibilidad de los datos personales durante su tratamiento, para lo cual los sujetos obligados deberán:

a) Adoptar las medidas para el resguardo de los sistemas de datos personales cualquiera que sea el soporte en que se encuentren, de manera que se evite su alteración, pérdida o acceso no autorizado.
b) Autorizar expresamente, en los casos en que no esté previsto por un instrumento jurídico, a Encargados y Usuarios, y llevar una relación actualizada de las personas que tengan acceso a los sistemas de datos personales que se encuentran en soporte físico.

VIGÉSIMO PRIMERO.- Conforme a lo dispuesto en el Lineamiento Vigésimo Segundo, las medidas de seguridad se distinguen en:

I. **Medidas de seguridad administrativas:** que se refieren a acciones y mecanismos cuyo objeto es establecer la gestión, soporte y revisión de la

seguridad de la información a nivel organizacional, la identificación y clasificación de la información, así como la concienciación, formación y capacitación del personal, en materia de protección de datos personales;

II. **Las Medidas de seguridad físicas:** Se refieren a acciones y mecanismos, ya sea que empleen o no la tecnología, destinados a:
   a) Prevenir el acceso no autorizado, el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, equipo e información.
   b) Proteger de su sustracción los equipos móviles (equipo de cómputo, u ordenadores portátiles o de fácil remoción), situados dentro o fuera de las instalaciones.
   c) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento que asegure su disponibilidad, funcionalidad e integridad, y
   d) Garantizar la eliminación de datos de forma segura.

III. **Medidas de seguridad técnicas:** se refiere a aquellas actividades, controles o mecanismos con resultado medible, que se valen de la tecnología para asegurar que:
   a) El acceso a las bases de datos lógicas o a la información en formato lógico sea por usuarios identificados y autorizados;
   b) El acceso referido en el inciso anterior sea únicamente para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
   c) Se incluyan acciones para la adquisición, operación, desarrollo y mantenimiento de sistemas seguros, y
   d) Se lleve a cabo la gestión de comunicaciones y operaciones de los recursos informáticos que se utilicen en el tratamiento de datos personales.

VIGÉSIMO SEGUNDO.- Conforme a lo dispuesto por la Ley en el artículo 27 fracción I, en sus diversos incisos, respecto a los tipos de seguridad que en aquel se especifican, los sujetos obligados atenderán a lo siguiente:

I.- De los tipos de seguridad:

a) En cuanto al **tipo de seguridad física** a que se refiere el inciso a), podrán al menos establecer algunas de las siguientes medidas: Control de acceso físico del personal autorizado; puertas de seguridad blindadas, candados, gavetas con cerradura de llaves, extinguidores, croquis de localización, cajas libres de ácido, fundas transparentes de polipropileno o poliéster, todo tipo de hardware de seguridad, dispositivos de radiofrecuencia (Near Field Communication), tarjeta inteligente, etc.
b) En cuanto al tipo de **seguridad lógica** a que se refiere el inciso b), podrán al menos establecer alguna de las siguientes medidas: Bitácoras de acceso, sistemas de control por medio del uso y portación de credenciales de identificación con fotografía, control de acceso biométrico, reloj checador por medio de huella digital para acreditar la pertenencia o estancia en las instalaciones respectivas.
c) En cuanto al tipo de **seguridad desarrollo y aplicaciones** a que se refiere el inciso c), podrán al menos establecer alguna de las siguientes medidas:

La administración de cuentas de usuarios; acceso remoto (acceso desde una computadora a un recurso ubicado físicamente en otra computadora que se encuentra geográficamente en otro lugar, a través de una red local o externa, como Internet); la autenticidad de documentos por medio del uso de la firma digital; el uso del Certificado Digital (declaración firmada de manera digital que enlaza el valor de una clave pública con la identidad de una persona, un dispositivo o un servicio que posee la clave privada correspondiente); sistemas de detección de intrusos; sistema de protección de correo electrónico; antivirus, etc.

d) En cuanto al tipo de **seguridad de cifrado** a que se refiere el inciso d), podrán al menos establecer alguna de las siguientes medidas: Cifrado simétrico: (crear una misma clave para cifrar y descifrar mensajes) Claves y contraseñas de acceso al Registro de Sistemas de Datos Personales, INFOMEX, correo electrónico oficial, etc. Cifrado asimétrico (cuando ambas claves son distintas).
e) En cuanto al tipo de **seguridad de comunicaciones y redes** a que se refiere el inciso e), podrán al menos establecer alguna de las siguientes medidas: Firewall (software), sistemas de detección de intrusos, sistemas de protección de correo electrónico, control de acceso de derechos, etc.

Respecto a los niveles de seguridad que la Ley establece en el artículo 27 fracción II, en sus diversos incisos, dichas medidas son acumulativas y los sujetos obligados atenderán a lo siguiente:

II.- De los niveles de seguridad:

a. **En cuanto al Nivel Básico.-** Comprende los siguientes aspectos:

1. **Documento de seguridad.-**

El responsable elaborará, difundirá e implementará la normativa de seguridad que será de observancia obligatoria para todos los servidores públicos del sujeto obligado, así como para toda aquella persona que debido a la prestación de un servicio tenga acceso a los sistemas de datos personales y/o al sitio donde se ubican los mismos, tomando en cuenta lo dispuesto en la Ley y en los presentes Lineamientos.

El documento de seguridad deberá contener, como mínimo, los siguientes aspectos:

1.1 Nombre del sistema.
1.2 Cargo y adscripción del responsable.
1.3 Ámbito de aplicación.
1.4 Estructura y descripción del sistema de datos personales.
1.5 Especificación detallada de la categoría de datos personales contenidos en el sistema.
1.6 Funciones y obligaciones del personal que intervenga en el tratamiento de los sistemas de datos personales.
1.7 Medidas, normas, procedimientos y criterios enfocados a garantizar el nivel de seguridad exigido por el artículo 27 de la Ley y los presentes Lineamientos.

1.8 Procedimientos de notificación, gestión y respuesta ante incidencias.
1.9 Procedimientos para la realización de copias de respaldo y recuperación de los datos, para los sistemas de datos personales automatizados; y
1.10 Procedimientos para la realización de auditorías, en su caso.

El contenido del documento de seguridad se considera información de acceso restringido solo será del conocimiento de las personas en función a su encargo o servicio, debiendo clasificarse de conformidad con la Ley de Transparencia y Acceso a la Información Pública del Estado de Chihuahua.

El documento de seguridad deberá actualizarse anualmente o cuando se produzcan cambios relevantes en el tratamiento, que puedan repercutir en el cumplimiento de las medidas de seguridad implementadas; así como, la fecha en la cual se realizó la actualización del documento de seguridad en un plazo no mayor a los diez días hábiles siguientes.

2. Funciones y obligaciones del responsable, operario y de toda persona que intervenga en el tratamiento de los sistemas de datos personales.

Las funciones y obligaciones de todos los que intervengan en el tratamiento de datos personales deben estar claramente definidas en el documento de seguridad. El responsable adoptará las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones, así como las responsabilidades y consecuencias en que pudiera incurrir en caso de incumplimiento.

3. Registro de incidencias.

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

Cuando se registre una incidencia que involucre datos de tipo sensible o de menores, deberá notificarse al Instituto el acta de hechos levantada de acuerdo al procedimiento establecido en el documento de seguridad.

4. Identificación y autentificación.

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

El responsable establecerá un mecanismo que permita la identificación, de forma inequívoca y personalizada, de toda aquella persona que intente acceder al sistema de datos personales y la verificación de que está autorizada.

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

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

Asimismo, se establecerá un procedimiento de creación y modificación de contraseñas (longitud, formato, contenido).

5. Control de acceso.

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

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

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

6. Gestión de soportes.

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

La salida de soportes y documentos que contengan datos de carácter personal, fuera de las instalaciones u oficinas bajo el control del responsable del sistema de datos personales, deberá ser autorizada por éste, o encontrarse debidamente autorizada en el documento de seguridad. En el traslado de soportes físicos y electrónicos se adoptarán medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.

Siempre que vaya a eliminarse cualquier soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado de la información, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior, previo proceso de valoración documental avalado mediante dictamen emitido por el órgano facultado para ello, del sujeto obligado que se trate, en los términos de la Ley de Archivos del Estado de Chihuahua.

7. Copias de respaldo y recuperación.

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

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

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

b. **Nivel Medio.** El nivel de seguridad medio es aplicable a los sistemas de datos personales en los términos del artículo 27 fracción II inciso a); debiendo observarse lo siguiente:

1. **En cuanto al Responsable de seguridad.**

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

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

2. **Respecto a la Auditoría.**

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

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

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

3. **En cuanto al Control de acceso físico.**

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

4. **En relación con la Pruebas que se realicen con datos reales.**

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

c. **Nivel Alto.** El nivel de seguridad alto es aplicable a los sistemas de datos personales en los términos del artículo 27 fracción II inciso c); debiendo observarse lo siguiente:

1. **En cuanto a distribución de soportes.**

La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos, o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su traslado o transmisión.

2. **Registro de acceso.**

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

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

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

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

3. Telecomunicaciones.

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

Legalidad de las medidas de seguridad adicionales.

VIGÉSIMO TERCERO.- Las medidas de seguridad que en su caso se adopten en forma adicional a las establecidas en los artículos 26 y 27 de la Ley de Protección de Datos Perscnales del Estado de Chihuahua y los presentes Lineamientos, para establecer mayores garantías en la protección y resguardo de los sistemas de datos personales, no deberán ser contrarias a las disposiciones legales.

Deber de actualización del registro de nivel de seguridad.

VIGÉSIMO CUARTO.- Los responsables sólo deberán comunicar al Instituto el nivel de seguridad aplicable a los sistemas de datos personales para su registro, además de la fecha de elaboración del documento de seguridad, así como las fechas de elaboración y/o actualización del mismo.

CAPÍTULO V
DEL TRATAMIENTO DE DATOS PERSONALES

VIGÉSIMO QUINTO.- En el tratamiento de los datos personales, además de lo dispuesto en el artículo 7 de la Ley, se observará lo dispuesto en el Título Primero, Capítulo II, De los Principios de la Protección de Datos Personales de los presentes Lineamientos.

Del consentimiento

VIGÉSIMO SEXTO.- El responsable deberá obtener el consentimiento del interesado para el tratamiento de sus datos personales, salvo en aquellos supuestos en que el mismo no sea exigible en términos de lo dispuesto en el artículo 29 de la Ley.

El consentimiento del interesado deberá ir referido a un tratamiento específico, con delimitaciones de temporalidad y finalidad.

Cuando se solicite el consentimiento del interesado para la cesión de sus datos, éste deberá ser informado de forma que conozca inequívocamente la finalidad a la que se destinarán los datos respecto de cuya comunicación se solicita el consentimiento, así como el tipo de actividad desarrollada por el cesionario. En caso contrario, el consentimiento será nulo.

Menores o incapaces.

VIGÉSIMO SÉPTIMO.- En caso de que el sujeto obligado requiera obtener datos personales de menores de edad o incapaces, el responsable del sistema de datos personales, deberá cerciorarse de que quien otorga el consentimiento es la persona que ejerce la patria potestad, tutela o la representación legal del menor o incapaz de que se trate en términos del Código Civil del Estado de Chihuahua.

Forma de recabar el consentimiento.

VIGÉSIMO OCTAVO.- El responsable del sistema de datos personales, deberá comunicar por escrito al interesado los aspectos a que se refiere el artículo 15 de la Ley y Décimo Sexto de los presentes Lineamientos, concediéndole un plazo de quince días hábiles para manifestar su negativa al tratamiento, bajo la advertencia de que en caso de no pronunciarse al respecto, se entenderá que no consiente el tratamiento de sus datos personales, excepto los supuestos contemplados en la Ley.

Para efectos de cumplir con el deber de información, el responsable deberá incorporar al escrito de declarativa el Aviso de Privacidad a que se hace referencia en el numeral Décimo Octavo de estos Lineamientos.

En el caso de los sistemas de datos creados con anterioridad a la entrada en vigor de la Ley, así como en los casos y excepciones señalados en el artículo 29 de la misma, no se requerirá la notificación a la que se hace referencia en el párrafo anterior, salvo que los datos reciban un tratamiento distinto a aquel para el que fueron recabados inicialmente.

La comunicación a que se refiere el primer párrafo del presente numeral, podrá realizarse en el domicilio del sujeto obligado; por correo electrónico o por correo certificado.

Revocación del Consentimiento.

VIGÉSIMO NOVENO.- En el caso de cesión de datos personales a terceros, de conformidad con lo dispuesto en el artículo 31 de la Ley, el interesado podrá revocar su consentimiento mediante solicitud dirigida al sujeto obligado, que será presentada ante la Unidad de Información, a través del formato que para tal efecto emita el Instituto o mediante escrito libre, en el cual deberá especificar la causa o motivo por la que solicita se revoque el consentimiento para tratar sus datos personales.

Únicamente el titular o su representante legal, podrá solicitar al sujeto obligado la revocación de su consentimiento, respecto de los datos personales que fueron objeto de cesión.

Requisitos de la solicitud.

TRIGÉSIMO.- La solicitud de revocación del consentimiento deberá ir acompañada de un medio de identificación oficial, reuniendo, al menos, los requisitos siguientes:

I. Nombre del sujeto obligado a quien se dirija.

II. Nombre completo del titular y, en su caso, el de su representante legal.

III. Descripción clara y precisa de los datos personales respecto de los que se busca revocar el consentimiento.

IV. Cualquier otro elemento que facilite su localización.

V. Ofrecer y aportar, en su caso, las pruebas que guarden relación directa con los hechos del escrito.

VI. Domicilio, para oír y recibir notificaciones o medio electrónico para recibirlas.

En el caso de que el solicitante no señale domicilio o algún medio para oír y recibir notificaciones, incluso las de carácter personal, se harán por estrados de la Unidad de Información del sujeto obligado.

La persona interesada deberá identificarse plena e indubitablemente, dejando constancia de ello en el expediente, mediante documento suficiente para tal efecto, mientras que quien ostente, en su caso, la representación legal, deberá acreditarla en los términos de la legislación civil.

Del procedimiento.

TRIGÉSIMO PRIMERO.- El procedimiento ante el sujeto obligado para dar trámite a las solicitudes de revocación del consentimiento, se desahogará en el plazo máximo de diez hábiles y se ajustará a lo siguiente:

I. Recibida la solicitud, la Unidad de Información verificará el cumplimiento de lo dispuesto en el Lineamiento Trigésimo y, en su caso, prevendrá al interesado dentro de los dos días hábiles siguientes a la recepción de la solicitud para que un término igual la complemente.
La notificación de la prevención tendrá por efecto interrumpir el plazo de diez días hábiles para resolver la solicitud.
Una vez notificado y transcurrido el plazo otorgado sin que el interesado cumpla con la prevención; en el caso de las fracciones I y II del Lineamiento Trigésimo, la solicitud se tendrá por no interpuesta; en el caso de las fracciones III y IV, se abordará el estudio de la solicitud con los hechos y elementos que obren en el expediente; en el caso de la fracción V, las pruebas se tendrán por no ofrecidas y, en caso, de no haberse señalado domicilio como lo establece la fracción VI, aún las de carácter personal se harán por medio de estrados.
II. Atendida la(s) prevención(es) La Unidad de Información, de conformidad con los artículos 3 fracción XII y 36 de la Ley, dará vista al(los) responsable(es) del(los) Sistema(as) de Datos Personales, quien(es) deberán resolver sobre la procedencia o improcedencia de la revocación del consentimiento.

Toda solicitud de revocación del consentimiento, deberá ser resuelta en un término no mayor a diez días hábiles contados a partir del día siguiente a la recepción de la solicitud. La Unidad de Información notificará la resolución al interesado, en un plazo no mayor a tres días hábiles de la fecha de resolución.

Efectos de la Revocación.

TRIGÉSIMO SEGUNDO.- En caso de que el responsable del sistema de datos personales, determine que la solicitud de revocación del consentimiento es procedente, éste deberá cesar en el tratamiento de los mismos, sin perjuicio de la

obligación de bloquear los datos personales conforme a la Ley y estos Lineamientos, circunstancias que deberán indicarse en la resolución.

En el caso de que los datos hubieren sido cedidos previamente, el responsable del sistema de datos personales, una vez revocado el consentimiento, deberá comunicarlo a los cesionarios dentro del plazo de diez días hábiles para que procedan de conformidad con el primer párrafo de este numeral.

Ante la improcedencia de la revocación del consentimiento, el interesado podrá ejercer su derecho de cancelación, conforme a la Ley y los presentes Lineamientos.

Tratamiento ilícito de datos personales.

TRIGÉSIMO TERCERO.- Requerimiento de suspensión. El Instituto podrá ordenar en los supuestos a que hace referencia el artículo 32 de la Ley, mediante resolución fundada y motivada del Consejo General, que los responsables de sistemas de datos personales suspendan la utilización o cesión de determinados datos, sin perjuicio de las responsabilidades que en su caso se generen.

El requerimiento deberá ser atendido dentro del plazo improrrogable de cinco días hábiles al término del cual, el sujeto obligado a través del responsable del sistema de datos personales deberá rendir un informe en el cual señale las medidas adoptadas para la suspensión y en el que alegue lo que a su derecho convenga.

Transcurrido el plazo, el Instituto deberá emitir una resolución, dentro del término de quince días hábiles, en la que podrá:

I. Emitir recomendaciones mediante las que requiera al sujeto obligado se subsanen las irregularidades detectadas, mismas que tendrán que ser solventadas dentro del plazo y condiciones que al efecto se establezcan;
II. Requerir al responsable la cancelación o rectificación de determinados datos contenidos en el sistema que corresponda;
III. Requerir que el responsable modifique el sistema a efecto de que se ajuste a lo establecido en la Ley y demás normativa aplicable; y
V. Determinar que no hay elementos que permitan establecer que se actualizan los supuestos a que hace referencia el artículo 32 de la Ley.

No podrá archivarse ningún expediente sin que se haya cumplido la resolución correspondiente o se hubiere extinguido la materia de la ejecución.

Requerimiento de inmovilización.

TRIGÉSIMO CUARTO.- En caso de que el requerimiento de suspensión fuera desatendido, el Instituto, mediante resolución fundada y motivada del Consejo, podrá requerir la inmovilización del sistema correspondiente, con el único fin de restaurar los derechos de las personas afectadas, lo que se hará en conformidad con el Lineamiento anterior.

Si el requerimiento de inmovilización del sistema fuera desatendido, el Instituto iniciará el procedimiento previsto en el Lineamiento correspondiente a que se

refiere el Título Quinto, de la Ley; lo anterior, con independencia de lo establecido en los artículos 50 último párrafo y 60 de la Ley.

El Instituto podrá evaluar el cumplimiento de la actuación del sujeto obligado mediante la realización de visitas de inspección en los términos de la Ley y demás normatividad aplicable. Si el Instituto advierte alguna presunta infracción a la Ley, dará vista al sujeto obligado, para que determine lo que en derecho corresponda, con independencia de iniciar el procedimiento previsto en el Lineamiento correspondiente.

Cancelación de datos personales por los sujetos obligados.

TRIGÉSIMO QUINTO.- Los datos de carácter personal serán suprimidos de oficio por los sujetos obligados o cancelados, a petición del interesado, una vez que hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hayan sido recabados. Sin embargo, deberán conservarse durante el tiempo en que pueda exigirse algún tipo de responsabilidad derivada de una relación u obligación jurídica, o de la ejecución de un contrato, siendo el plazo de conservación el que se establezca dentro del catálogo de disposición documental, de conformidad con la Ley de Archivos del Estado de Chihuahua.

Una vez cumplido el plazo a que se refiere el párrafo anterior, los datos sólo podrán conservarse con fines estadísticos o históricos, previa disociación de los mismos, sin perjuicio de la obligación de bloqueo prevista en la Ley y estos Lineamientos.

TRIGÉSIMO SEXTO.- Los datos personales que hayan sido objeto de tratamiento y que no contengan valores históricos, científicos o estadísticos, deberán ser suprimidos o cancelados, del sistema de datos personales, según sea el caso, teniendo en cuenta los plazos establecidos:

I. En el formato físico o electrónico por medio del cual se recabaron;
II. Por las disposiciones aplicables; y
III. En el instrumento jurídico formalizado entre un tercero y el sujeto obligado.

Cesión de datos personales.

TRIGÉSIMO SÉPTIMO.- La cesión de datos personales sólo podrá realizarse cuando el cesionario garantice por escrito un nivel de protección similar al empleado en el sistema de datos personales, y que se haya consignado en el documento de seguridad. El cesionario de los datos personales quedará sujeto a las mismas obligaciones que corresponden al responsable que los transfiera.

El acceso a los sistemas de datos personales por parte de la persona encargada del tratamiento, no se considerará una cesión o delegación de responsabilidades por parte del responsable del sistema.

Seguridad en la cesión.

TRIGÉSIMO OCTAVO.- El carácter adecuado de las medidas de seguridad que ofrezca el cesionario se evaluará atendiendo a las circunstancias que concurran en la transferencia, y en especifico se tomará en consideración la naturaleza de los datos personales, la finalidad y la duración del tratamiento.

CAPÍTULO VI
DE LAS OBLIGACIONES DE LOS SUJETOS OBLIGADOS

TRIGÉSIMO NOVENO.- El titular del sujeto obligado es el responsable de los sistemas de datos personales, y tiene la obligación de designar al servidor público responsable de cada sistema de datos personales, mismo que deberá estar adscrito a la unidad administrativa en la que se concrete la competencia material del sistema, quien tendrá la atribución de decidir sobre el contenido y finalidad de los sistemas de datos personales.

De igual forma, deberá designar al servidor público que servirá como enlace entre el sujeto obligado y el Instituto; el nombramiento podrá recaer en el titular de la Unidad de Información del sujeto obligado; dicho servidor público coordinará a los responsables de los sistemas de datos personales al interior del sujeto obligado.

El Titular del sujeto obligado deberá reportar al Instituto el nombramiento o sustitución del responsable de cada sistema de datos personales, así como del enlace, en un plazo no mayor a diez días hábiles posteriores a la designación correspondiente.

Tratamiento por usuarios.

CUADRAGÉSIMO.- En caso de que el tratamiento de datos personales sea por parte de usuarios, el responsable deberá asegurarse que dicha acción esté regulada en un contrato, que deberá constar por escrito, o en alguna otra forma que permita acreditar su celebración, contenido y alcance, en el cual se establecerá que el usuario únicamente tratará los datos conforme a las instrucciones del responsable, que así mismo no los aplicará o utilizará con una finalidad distinta a la establecida en el contrato y que no los comunicará a otras personas, en estricto apego a lo dispuesto por la Ley y los presentes Lineamientos.

En el contrato se estipularán las medidas de seguridad que se deban implementar para el tratamiento por el usuario.

Concluida la relación contractual, los datos de carácter personal deberán ser devue tos al responsable o, en su caso, destruidos.

Informe anual.

CUADRAGÉSIMO PRIMERO.- El informe anual que hace referencia la fracción III del artículo 35. deberá contener los siguientes apartados:

I. Número de solicitudes de acceso, rectificación, cancelación y oposición de datos personales presentadas ante el sujeto obligado, así como su resultado.
II. El tiempo de respuesta a la solicitud.
III. El estado que guardan las denuncias presentadas ante los órganos internos de control.
IV. Sistemas de datos personales creados, modificados y/o suprimidos.
V. Acciones desarrolladas para dar cumplimiento a las disposiciones contenidas en la Ley.

VI. Cesiones de datos personales efectuadas y que deberán detallar:
a) Identificación del sistema mediante número de folio otorgado por el Instituto, del sujeto obligado cedente y del cesionario.
b) Finalidad de la cesión.
c) La mención de si se trata de una cesión total o parcial de un sistema de datos personales.
d) Las categorías de datos de que se trate.
e) Fecha de inicio y término de la cesión y, en su caso, la periodicidad de la misma.
f) Medio empleado para realizar la cesión.
g) Medidas y niveles de seguridad empleados para la cesión;
h) Obligaciones al término del tratamiento.
i) El nivel de seguridad aplicado por el cesionario; y,
j) Cualquier otro dato relevante, derivado de las obligaciones previstas en la Ley, o que a juicio del Consejo General del Instituto, sea necesario.

CUADRAGÉSIMO SEGUNDO.- El enlace del sujeto obligado, tendrá las siguientes obligaciones:

I. Coordinar a los responsables de cada sistema de datos personales al interior del sujeto obligado para el cumplimiento de la Ley, los Lineamientos y demás normativa aplicable.
II. Supervisar que los responsables de cada sistema de datos personales mantengan actualizada la inscripción de los sistemas bajo su responsabilidad en el Registro electrónico creado por el Instituto.

TÍTULO TERCERO
DE LA AUTORIDAD RESPONSABLE DEL CONTROL Y VIGILANCIA

CAPÍTULO ÚNICO
DEL INSTITUTO CHIHUAHUENSE PARA LA TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA

CUADRAGÉSIMO TERCERO.- De conformidad con el artículo 37 de la Ley, el Instituto cuenta con la facultad para intervenir en la creación, modificación y supresión de sistemas de datos personales sujetos al ámbito de aplicación de la Ley, que no se ajusten a las disposiciones de la misma, de los presentes Lineamientos y de las demás disposiciones que resulten aplicables. Para ello dispondrá de medios de investigación indispensables para dirigir y garantizar el cumplimiento de la Ley.

A tal efecto, tendrá acceso a los sistemas de datos personales, podrá inspeccionarlos y recabar toda la información necesaria para el cumplimiento de su función de control, podrá solicitar la exhibición o el envío de documentos y datos, así como examinarlos en el lugar en donde se encuentren instalados, salvaguardando la confidencialidad de la información proporcionada por los entes públicos. Esta facultad la ejercerá a través de la Dirección de Acceso a la

Información y Protección de Datos Personales, y del personal que el Consejo General, en su caso, autorice para tal efecto. En la vistas de inspección, el personal del Instituto serán nombrados inspectores.

Visitas de inspección y su procedimiento.

CUADRAGÉSIMO CUARTO.- El Instituto, en términos del artículo 37 fracción XVI de la Ley, podrá realizar visitas de inspección, las cuales no podrán referirse a información de acceso restringido, a efecto de evaluar la actuación de los sujetos obligados, de conformidad con lo siguiente:

I. Toda visita de inspección deberá ajustarse a los procedimientos y formalidades establecidos en estos Lineamientos.
II. Los inspectores, al practicar una visita, deberán llevar siempre consigo el Acuerdo del Consejo General del Instituto que determinó la diligencia en el que deberá precisarse el ente público que ha de inspeccionarse, el objeto de la visita, el alcance que deba tener y las disposiciones legales que la fundamenten.
III. Los responsables o encargados del sistema de datos personales objeto de inspección estarán obligados a permitir el acceso y dar facilidades e informes a los inspectores para el desarrollo de su labor.
IV. Al iniciar la visita, el inspector deberá exhibir credencial vigente con fotografía, expedida por el Instituto, que lo acredite para desempeñar dicha función, así como el acuerdo a que se refiere la fracción II de este numeral, de la que deberá dejar copia al responsable del sistema de datos personales de que se trate o a la persona con quien se entienda la diligencia.
V. De toda visita de inspección se levantará acta circunstanciada, en presencia de dos testigos propuestos por el responsable del sistema de datos personales o servidor público con quien se entienda la diligencia o, en su caso, por quien la practique si aquél se hubiere negado a proponerlos.
VI. De toda acta se dejará copia al servidor público con quien se entendió la diligencia, aunque se hubiere negado a firmar, lo que no afectará la validez de la diligencia ni del documento de que se trate, siempre y cuando el inspector haga constar tal circunstancia en el acta.
VII. En las actas se hará constar:
   a) Identificación del sujeto obligado visitado.
   b) Hora, día, mes y año en que se inicie y concluya la diligencia.
   c) Calle, número, colonia, fraccionamiento, parque industrial, etc., teléfono u otra forma de comunicación disponible, municipio y código postal en que se encuentre ubicado el lugar en que se practique la visita.
   d) Número y fecha del Acuerdo del Consejo General del Instituto, que la motivó.
   e) Nombre y cargo de la persona con quien se entendió la diligencia.
   f) Nombre y cargo de las personas que fungieron como testigos.
   g) Datos relativos a la actuación, pruebas recabadas.
   h) Declaración o manifestaciones del visitado, si quiere hacerlas.
   i) Otra información, que a criterio del inspector, responsable del sistema de datos personales, encargado o aquel con quien se entienda la diligencia, resulte relevante se asiente en el acta; y,

j) Nombre y firma de quienes intervinieron en la diligencia. Si se negare a firmar el visitado, ello no afectará la validez del acta, debiendo el inspector asentar la razón relativa.

VIII. La visita debe entenderse con el responsable del sistema de datos personales. En caso de que no se encontrara presente, la diligencia se entenderá con el encargado del tratamiento de datos personales y, en su defecto, con quien se encuentre presente, circunstancia que se hará constar en el acta.

IX. Los visitados a quienes se haya levantado acta de inspección podrán formular observaciones en el acto de la diligencia y ofrecer pruebas en relación a los hechos contenidos en ella, o bien por escrito, así como hacer uso de tal derecho dentro del término de cinco días hábiles siguientes a la fecha en que se hubiere levantado; y

X. Transcurrido el plazo señalado en la fracción anterior, el Instituto deberá emitir una resolución dentro del término de quince días hábiles en la que podrá:

a) Determinar que el sistema de datos personales se ajusta a lo establecido en la Ley;

b) Determinar que existen irregularidades que contravienen lo establecido en la Ley y demás normatividad aplicable, caso en el que formulará recomendaciones al sujeto obligado, a efecto de que subsane las inconsistencias detectadas dentro del plazo y condiciones que al efecto se determinen.

El sujeto obligado deberá informar por escrito al Instituto, dentro de los cinco días hábiles siguientes a que termine el plazo a que se refiere el anterior inciso b), sobre la atención a las recomendaciones formuladas por el Instituto.

Ante la omisión del sujeto obligado en presentar los informes o en solventar las recomendaciones, la Dirección de Acceso a la Información y Protección de datos Personales dará vista al Consejo para los efectos legales correspondientes, sin que esta situación exima al visitado del cumplimiento de las mismas.

En caso de que, en la visita de inspección se advirtiera un posible tratamiento ilícito de los datos personales, se estará a lo dispuesto en los Lineamientos Trigésimo Tercero y Trigésimo Cuarto de los presentes Lineamientos.

TÍTULO CUARTO
DE LOS DERECHOS Y DEL PROCEDIMIENTO PARA SU EJERCICIO

CAPÍTULO I
DERECHOS DE ACCESO, RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN.

CUADRAGÉSIMO QUINTO.- El interesado podrá, a través del derecho de acceso a datos personales, obtener información relativa a sus datos personales, incluidos en un determinado sistema o la totalidad de los datos sometidos a tratamiento en los sistemas de datos personales en posesión de un sujeto obligado.

La obligación de acceso se dará por cumplida cuando el responsable ponga a disposición del titular los datos personales en sitio, en su caso, mediante la expedición de copias simples, medios magnéticos, ópticos, sonoros, visuales u

holográficos, o utilizando otras tecnologías de la información que se hayan previsto en el aviso de privacidad, siempre y cuando el soporte del sistema de datos personales así lo permita. En todos los casos, el acceso deberá ser en formatos legibles o comprensibles para el titular.

CUADRAGÉSIMO SEXTO.- Para efectos de la rectificación de datos personales, la solicitud deberá indicar qué datos requiere sean rectificados o completados, así como la corrección que haya de realizarse, y deberá ir acompañada de la documentación que justifique la procedencia de la petición.

CUADRAGÉSIMO SÉPTIMO.- En el ejercicio del derecho de cancelación de datos personales, se considerará que los datos son inadecuados, cuando éstos no guarden una relación con el ámbito de aplicación y finalidad por la cual fueron recabados, o bien, si dejaron de ser necesarios con respecto a dicha finalidad; asimismo, se considerarán como excesivos, si los datos obtenidos son más de los estrictamente necesarios en relación a dicha finalidad.

El interesado también podrá solicitar la cancelación de sus datos cuando el tratamiento de los mismos no se ajuste a lo dispuesto en la Ley o en estos Lineamientos.

En la solicitud de cancelación, el interesado deberá indicar a qué datos se refiere, exponiendo las razones por las cuales considera que el tratamiento no se ajusta a lo dispuesto en la Ley.

La cancelación procederá respecto de la totalidad de los datos personales del titular, contenidos en una base de datos, o sólo parte de ellos, según lo haya solicitado.

Los derechos de rectificación y cancelación no procederán en aquellos supuestos en que así lo disponga una Ley.

De resultar procedente la cancelación, el responsable deberá:

I. Establecer un periodo de bloqueo con el único propósito de determinar posibles responsabilidades en relación con su tratamiento hasta el plazo de prescripción legal o contractual de éstas, y notificarlo al titular o a su representante en la respuesta a la solicitud de cancelación, que se emita dentro del plazo de diez días que establece el artículo 47 de la Ley;

II. Atender las medidas de seguridad adecuadas para el bloqueo;

III. Llevar a cabo el bloqueo en el plazo de diez días que establece el artículo 47 de la Ley, y

IV. Transcurrido el periodo de bloqueo, llevar a cabo la supresión correspondiente, bajo las medidas de seguridad previamente establecidas por el responsable.

El bloqueo tiene como propósito impedir el tratamiento, a excepción del almacenamiento, o posible acceso por persona alguna, salvo que alguna disposición legal prevea lo contrario.

El periodo de bloqueo será hasta el plazo de prescripción legal o contractual correspondiente.

CUADRAGÉSIMO OCTAVO.- El derecho de oposición podrá ejercerse cuando:

I. Exista causa legítima y su situación específica así lo requiera, lo cual debe justificar que aún siendo lícito el tratamiento, el mismo debe cesar para evitar que su persistencia cause un perjuicio al titular, o
II. Requiera manifestar su oposición para el tratamiento de sus datos personales a fin de que no se lleve a cabo el tratamiento para fines específicos.

El interesado o su representante legal, podrá oponerse a la publicación de su nombre en los Boletines Judiciales, así como en las listas de acuerdos que se publiquen por medios electrónicos, una vez que hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hayan sido recabados, o cuando el tratamiento de los mismos no se ajuste a lo dispuesto por la propia Ley o los Lineamientos.

En caso de que la oposición sea procedente, dará lugar a la cancelación del dato, previo bloqueo, mientras transcurren los plazos previstos, a efecto de depurar las responsabilidades que correspondan.

No procederá el ejercicio del derecho de oposición en aquellos casos en los que el tratamiento sea necesario para el cumplimiento de una obligación legal impuesta al sujeto obligado.

CAPÍTULO II
DEL PROCEDIMIENTO PARA SU EJERCICIO

CUADRAGÉSIMO NOVENO.- Los derechos de acceso, rectificación, cancelación y oposición son personalísimos y, solo podrán ser ejercidos directamente por el interesado o su representante legal, quienes tendrán que acreditar su personalidad.

El titular de los datos personales podrá designar por escrito a aquellas personas que, en caso de fallecimiento, puedan ejercer los derechos de acceso, rectificación, cancelación u oposición con respecto a dichos datos.

En caso de que el titular de los datos personales no haya designado a ninguna persona, el ejercicio de estos derechos con respecto a los datos personales del fallecido, corresponderá al albacea de la sucesión, previa acreditación de su identidad y personalidad en los términos de la legislación civil.

En materia de salud solo se dará acceso a los registros médicos de las personas fallecidas cuando sean necesarios para la prevención o diagnóstico médico de los descendientes de la persona fallecida; la prestación de asistencia médica o la gestión de servicios de salud del solicitante.

Procedimiento.

QUINCUAGÉSIMO.- El promovente en la solicitud de acceso, rectificación, cancelación u oposición, sin perjuicio de lo establecido en el Título Cuarto, Capítulo II de la Ley, deberá:

I. Precisar el nombre correcto del sujeto obligado a quien se dirija.
II. Identificarse plena e indubitablemente como titular de los datos personales, dejando constancia de ello en el expediente, mediante documento suficiente para tal efecto, mientras que quien ostente, en su caso, la representación legal del mismo, deberá acreditarla en los términos de la legislación civil, debiendo, asimismo, identificarse plena e indubitablemente.
Para el caso de menores de edad o personas incapaces: El padre, tutor o representante legal del interesado, además de identificarse plena e indubitablemente, deberá acreditar que es la persona que ejerce la patria potestad, tutela o la representación legal del menor o incapaz de que se trate en términos del Código Civil del Estado de Chihuahua.
III. Identificar los datos personales a los que se quiera acceder, respecto de los que se solicita su rectificación, cancelación u oposición a su tratamiento, de conformidad con lo previsto en el artículo 51 de la Ley.
IV. Señalar lugar y medio para recibir notificaciones, dentro de la capital del Estado cuando la Unidad de Información tenga su domicilio en ésta, o en la localidad donde tenga su domicilio la Unidad de Información ante la que se ejercita alguno de los derechos A.R.C.O.
Cuando el medio empleado para promover la solicitud sea el sistema electrónico aprobado por el Instituto, y no habiendo señalado uno diverso, se tendrá el mismo como medio para recibir notificaciones.

En ningún caso los datos personales solicitados o las correcciones realizadas podrán enviarse por medios electrónicos.

QUINCUAGÉSIMO PRIMERO.- Presentada la solicitud de acceso, rectificación, cancelación u oposición al tratamiento de datos personales, por cualquiera de los medios establecidos en el artículo 49 de la Ley, la Unidad de Información del sujeto obligado, observará el siguiente procedimiento:

I. Deberá registrar la recepción a través del Sistema electrónico, independientemente de que la recepción haya sido física, por correo registrado, mensajería o por medios electrónicos, asignando un número de folio único, con el cual el solicitante podrá dar seguimiento a su solicitud.

II. Registrada la solicitud se verificará el cumplimiento de los requisitos señalados en los artículos 50 y 51 de la Ley y el Quincuagésimo de los presentes Lineamientos. Satisfechos dichos requisitos se turnará a la unidad administrativa que corresponda para que proceda a la localización de la información solicitada, a fin de emitir la resolución correspondiente, de no ser así se prevendrá al interesado, bajo el apercibimiento que señala el artículo 47 párrafo tercero de la Ley.

III. La Unidad de Información, notificará al solicitante la determinación tomada en relación con su petición, en el domicilio o a través del medio señalado para tal efecto.

Cuando el sujeto obligado determine que la solicitud de datos personales es procedente, la misma se hará efectiva dentro de los diez días hábiles siguientes contados a partir de concluido el plazo previsto por el artículo 47 de la Ley, en su caso, previo pago del costo de reproducción.

QUINCUAGÉSIMO SEGUNDO.- En caso de que la solicitud presentada no corresponda a una solicitud de acceso, rectificación, cancelación u oposición al tratamiento de datos personales, la Unidad de Información del sujeto obligado deberá notificar dicha circunstancia al solicitante dentro del plazo de cinco días hábiles y, en su caso, orientarlo para que realice el trámite que corresponda.

Asimismo, cuando se presente una solicitud de acceso, rectificación, cancelación u oposición al tratamiento de datos personales y de ésta se aprecie que su objeto es diverso al derecho A.R.C.O. que pretende ejercer, la Unidad de Información del sujeto obligado dentro de los cinco días hábiles siguientes a la recepción de la misma, orientará al solicitante para que presente su solicitud de conformidad con el derecho que corresponda.

En caso de que el sujeto obligado al que se dirija la solicitud de acceso, rectificación, cancelación u oposición al tratamiento de datos, no sea el competente para atenderla, dentro de los cinco días hábiles siguientes a aquel en que se presente la solicitud se procederá a orientar al interesado o a su representante legal para que acuda al sujeto obligado que se considere deba contar con los datos objeto del ejercicio de los mencionados derechos.

CAPÍTULO III: DEL RECURSO DE REVISIÓN

QUINCUAGÉSIMO TERCERO.- El recurso de revisión previsto por la Ley de Protección de Datos Personales del Estado de Chihuahua, es el medio de defensa jurídico del cual podrá hacer uso todo interesado que se considere agraviado por la resolución recaída a las solicitudes de acceso, rectificación, cancelación, u oposición de datos personales, o bien ante la omisión de la respuesta correspondiente, mismo que será tramitado observando los plazos, procedimientos y requisitos, señalados en la Ley de Transparencia y Acceso a la Información Pública del Estado de Chihuahua y en los Lineamientos Relativos al Recurso de Revisión que Previene el Capítulo V, del Título Cuarto, de dicha Ley.

QUINCUAGÉSIMO CUARTO.- La interposición del Recurso de Revisión, deberá presentarse por el titular del derecho o su representante; ya sea mediante escrito libre, en los formatos que para tal efecto determine el Instituto o a través del sistema que éste establezca, en el plazo previsto en la Ley de Transparencia y Acceso a la Información Pública del estado de Chihuahua.

Tanto el formato como el sistema deberán ser puestos a disposición por el Instituto en su sitio de Internet, en las Unidades de Información y en los sitios de Internet de los sujetos obligados.

La presentación del recurso de revisión podrá hacerse en el domicilio del Instituto así como en el domicilio de la Unidad de Información del sujeto obligado que corresponda.

Al promover el Recurso de Revisión, el promovente, ya sea el titular o su representante deberán acreditar fehacientemente su identidad o personalidad respectivamente, en los términos establecidos en el numeral Cuadragésimo Séptimo, de los presentes Lineamientos.

El Instituto podrá tener por reconocida la identidad del titular o la personalidad del representante cuando la misma ya hubiere sido acreditada ante el sujeto obligado responsable al ejercer su derecho ARCO.

QUINCUAGÉSIMO QUINTO.- El Recurso de Revisión procederá cuando exista una inconformidad por parte del titular, derivada de acciones u omisiones del sujeto obligado con motivo del ejercicio de los derechos ARCO cuando:

I. El titular no reciba respuesta por parte del sujeto obligado.
II. El sujeto obligado no otorgue acceso a los datos personales solicitados o lo haga en un formato incomprensible.
III. El sujeto obligado se niegue a efectuar las rectificaciones a los datos personales.
IV. El titular no esté conforme con la información entregada por considerar que es incompleta o no corresponde a la solicitada, o bien, con el costo o, en su caso, con la modalidad de reproducción.
V. El sujeto obligado se niegue a cancelar los datos personales.
VI. El sujeto obligado persista en el tratamiento a pesar de haber procedido la solicitud de oposición, o bien, se niegue a atender la solicitud de oposición.

QUINCUAGÉSIMO SEXTO.- El Recurso de Revisión deberá satisfacer los siguientes requisitos:

I. El nombre del titular o, en su caso, el de su representante legal;

II. El nombre del responsable ante el cual se presentó la solicitud de acceso, rectificación, cancelación u oposición de datos personales;

III. El domicilio para oír y recibir notificaciones;

IV. La fecha en que se le dio a conocer la respuesta del responsable, o la fecha en que venció el término para que el sujeto obligado atendiera la solicitud de acceso, rectificación, cancelación u oposición de datos personales.

V. Manifestar expresamente los hechos en los que funda la impugnación y

VI. Los demás elementos que se considere procedente hacer del conocimiento del Instituto.

QUINCUAGÉSIMO SÉPTIMO.- El promovente, deberá adjuntar a su escrito recursal los documentos siguientes:

I. Copia de la solicitud del ejercicio de derechos que corresponda, así como copia de los documentos anexos para cada una de las partes, de ser el caso;

II. El documento que acredite que actúa por su propio derecho o en representación del titular;

III. El documento en que conste la respuesta del responsable, de ser el caso;

IV. En el supuesto en que impugne la falta de respuesta del responsable, deberá acompañar una copia en la que obre el acuse o constancia de recepción de la solicitud del ejercicio de derechos por parte del responsable;

V. Las pruebas documentales que ofrece para demostrar sus afirmaciones.

QUINCUAGÉSIMO OCTAVO.- El Instituto suplirá las deficiencias de la queja en los casos que así se requiera, siempre y cuando no altere el contenido original de la solicitud de acceso, rectificación, cancelación u oposición de datos personales, ni se modifiquen los hechos o peticiones expuestos en la misma o en la solicitud de protección de datos.

QUINCUAGÉSIMO NOVENO.- Además de las causales de desechamiento del Recurso de Revisión previstas en el artículo 75 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chihuahua, este será desechado cuando:

a) El Instituto no sea competente; o
b) Se trate de un Recurso de Revisión ofensivo o irracional.

TRANSITORIOS.

PRIMERO.- Publíquense los presentes Lineamientos en el Periódico Oficial del Estado de Chihuahua.

SEGUNDO.- Los presentes Lineamientos entrarán en vigor el día de su publicación en el Periódico Oficial del Estado de Chihuahua.

TERCERO.- Los sujetos obligados deberán notificar al Instituto la relación de los sistemas de datos personales que posean bajo su custodia en el plazo previsto en el artículo Segundo Transitorio de la Ley de Protección de Datos del Estado de Chihuahua.

CUARTO.- Los sujetos obligados deberán haber registrado los sistemas de datos personales que posean, en el **Registro Electrónico de Sistemas de Datos Personales**, dentro del plazo de trescientos sesenta y cinco días naturales, contados a partir de la entrada en vigor de los presentes Lineamientos.

Así lo acordó el Consejo General del Instituto Chihuahuense para la Transparencia y Acceso a la Información Pública, por unanimidad de votos, en Sesión Extraordinaria celebrada en fecha veintiseis de junio de dos mil catorce.

LIC. ENRIQUE MEDINA REYES

CONSEJERO PRESIDENTE

LIC. EDUARDO JOSÉ GÓMEZ ARRIAGA

SECRETARIO EJECUTIVO