INSTITUTO DE TRANSPARENCIA E
INFORMACIÓN PÚBLICA DE JALISCO

Guía para la elaboración de los Sistemas de Información Reservada o Confidencial

Guía para la elaboración de los Sistemas de Información Reservada o Confidencial

La protección de datos personales es un derecho humano fundamental, reconocido internacionalmente, tutelado por el **artículo 16 de la Constitución Política de los Estados Unidos Mexicanos**, que otorga el poder a toda persona física, para que sus datos personales sean tratados de forma que se garantice la privacidad y su derecho de autodeterminación, entendiéndose como tal, a la decisión del titular, sobre quién puede tratar sus datos personales y para qué fines.

Un dato personal se define, como cualquier información concerniente a una persona física identificada o identificable, como pueden ser el origen étnico o racial, las características físicas, morales o emocionales, la vida afectiva o familiar, el domicilio particular, el número telefónico y correo electrónico particulares, el patrimonio, la ideología, opinión política y creencia o convicción religiosa y filosófica, el estado de salud física y mental, el historial médico, la preferencia sexual y cualquier otro que afecte su intimidad.

Los datos personales pueden ser expresados en forma numérica, alfabética, gráfica, fotografía y acústica o en cualquier modalidad.

La **Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios**, en lo sucesivo **Ley**, garantiza el derecho de proteger los datos personales en posesión de cualquier sujeto obligado (Órganos Estatales, Municipio, Congreso del Estado, etc.) y tutelar el ejercicio del ciudadano a sus Derechos de Acceso, Rectificación, Cancelación y Oposición (por sus siglas conocidos como derechos ARCO) a sus datos personales.

Para garantizar la protección de los datos personales, los sistemas de información reservada o confidencial, no requieren el desarrollo desproporcionado o adecuaciones administrativas mayores, sino el control e interrelación de comunicación entre las unidades dependientes de la administración, para que sea el Comité de Clasificación de cada Sujeto Obligado, el encargado de acopiar y determinar mediante un acuerdo, sobre la procedencia de la información que integre cada Sistema.

Un sistema obedece a un conjunto organizado de información reservada o confidencial. De acuerdo con las definiciones contenidas en el **Reglamento de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus municipios**, en lo sucesivo **Reglamento**, un sistema de datos personales, es un conjunto organizado de datos de carácter personal, cualquiera que sea su soporte, organización o acceso, siempre que tenga una estructura que permita un fácil ingreso a los datos de una persona determinada.

El conocimiento previo en la identificación de cada sistema, sin duda es su definición, misma que se encuentra especificada de la siguiente forma en el Reglamento:

- **Sistema de Información Reservada:** conjunto organizado de información reservada, que contenga un catálogo con los expedientes de la información reservada que tenga bajo su resguardo;
- **Sistema de Información Confidencial:** todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

Ante la novedad que requiere el tema, la principal problemática es diferenciar la clasificación sobre el tipo de sistema que corresponde, a lo que deberíamos preguntarnos lo siguiente:

- ¿Qué tipo de información tenemos?
- ¿Dónde se encuentran? (archivos, computadoras, expedientes, bases de datos, página de internet, etc.)
- ¿Para qué se utilizan o se pueden utilizar?
- ¿Quiénes tienen o pueden tener acceso a ellos?
- ¿Por qué medios se transfieren esos datos?
- ¿Qué procedimientos de control existen para su manejo?

Las respuestas obtenidas ayudarán a determinar algunos aspectos importantes sobre la información que se utiliza su manejo, sin embargo, un elemento importante en la determinación de los sistemas, será el conocimiento respecto la organización administrativa y las atribuciones de cada una de las áreas del sujeto obligado.

El Sistema de Información Reservada

El sistema de información reservada, será adecuado de conformidad con la clasificación de reserva realizada por el **Comité de Clasificación** del sujeto obligado, a través de sus **Actas de Clasificación**; estas actas, son la base para identificar cada una de las categorías, que de conformidad con el reglamento de ley, son requisito de su contenido para ser considerado como un sistema de información reservada.

La información pública reservada, es aquella protegida, relativa a la función pública, que por disposición legal temporalmente queda prohibido su manejo, distribución, publicación y difusión general, existiendo un catálogo normativo en el **artículo 17 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus municipios**, de la información considerada con tal carácter; esta clasificación establece como información reservada la siguiente:

I. Aquella información pública, cuya difusión:

   a) Comprometa la seguridad del Estado o del municipio, la seguridad pública estatal o municipal, o la seguridad e integridad de quienes laboran o hubieren laborado en estas áreas, con excepción de las remuneraciones de dichos servidores públicos;
   b) Dañe la estabilidad financiera o económica del Estado o de los municipios;
   c) Ponga en riesgo la vida, seguridad o salud de cualquier persona;
   d) Cause perjuicio grave a las actividades de verificación, inspección y auditoría, relativas al cumplimiento de las leyes y reglamentos;
   e) Cause perjuicio grave a la recaudación de las contribuciones;
   f) Cause perjuicio grave a las actividades de prevención y persecución de los delitos, o de impartición de la justicia; o
   g) Cause perjuicio grave a las estrategias procesales en procesos judiciales o procedimientos administrativos cuyas resoluciones no hayan causado estado;

II. Las averiguaciones previas;

III. Los expedientes judiciales en tanto no causen estado;

IV. Los expedientes de los procedimientos administrativos seguidos en forma de juicio en tanto no causen estado;

V. Los procedimientos de responsabilidad de los servidores públicos, en tanto no se dicte la resolución administrativa o la jurisdiccional definitiva;

VI. La que contenga opiniones, recomendaciones o puntos de vista que formen parte del proceso deliberativo de los servidores públicos, en tanto no se adopte la decisión definitiva;

VII. La entregada con carácter reservada o confidencial por autoridades federales o de otros estados, o por organismos internacionales;

VIII. La considerada como secreto comercial, industrial, fiscal, bancario, fiduciario, bursátil o cualquier otro, por disposición legal expresa;

IX. Las bases de datos, preguntas o reactivos para la aplicación de exámenes de admisión académica, evaluación psicológica, concursos de oposición o equivalentes, y

X. La considerada como reservada por disposición legal expresa.

Se debe realizar una revisión sobre la clasificación en nuestras actas, en la que, analicemos su vigencia y pertinencia; lo que dará como resultado la identificación de un sistema de información reservada; que deberá ser validado por el Instituto de Transparencia e Información Pública de Jalisco, en lo sucesivo ITEI, y que conforme lo señala el artículo 52 del Reglamento, por lo que cada una de las actas de clasificación de información reservada, deberán contener lo siguiente:

I. El rubro temático;

II. La unidad administrativa interna que generó, obtuvo, adquirió, transformó o conserva la información;

III. La fecha de la clasificación;

IV. El fundamento legal;

V. El plazo de reserva o la especificación de reservado por evento,

VI. En su caso, las partes del documento que se consideran como reservadas;

Una vez que se realice lo anterior con la totalidad de las actas de clasificación de información reservada, como resultado se obtendrá su Sistema de Información Reservada.

Ejemplo:

SISTEMA DE INFORMACIÓN RESERVADA DEL INSTITUTO DE TRANSPARENCIA E INFORMACIÓN PÚBLICA DE JALISCO (ITEI)	
I. El rubro temático:	Los usuarios y contraseñas o claves para ingresar el Sistema Infomex Jalisco, de los diversos sujetos obligados adheridos a este sistema.
II. La unidad administrativa interna que generó, obtuvo, adquirió, transformó o conserva la información:	Dirección de Planeación y Gestión Administrativa por Conducto de la Coordinación de Informática y Sistemas.
III. La fecha de la clasificación:	31 de mayo de 2010
IV. El fundamento legal:	Artículos 2,3 fracción IX, 23 fracción II, 27,84, 85, 89 y 88 de la Ley de Transparencia e Información Pública del Estado de Jalisco. Artículos 39 y 40 del Reglamento Interior del Instituto de Transparencia e Información Pública de Jalisco. Artículos 6, 29, 30, 31, 32, 33, 34 y 35 del Reglamento para la Transparencia y Acceso a la Información Pública del Instituto de Transparencia e Información Pública de Jalisco. Lineamientos Catorce y Trigésimo y Cuarto de los Lineamientos Generales para la Clasificación, desclasificación y custodia de la información reservada y confidencial.
V. En su caso, las partes del documento que se consideran como reservadas:	El Sistema Infomex Jalisco, es una plataforma, que brinda un servicio coordinado a la sociedad, a efecto de que vía remota (Internet) pueda solicitar información a diversos sujetos obligados, que previamente estén adheridos al sistema. El mecanismo para la entrega de usuarios y contraseñas, , al sujeto obligado que recién se hubiere incorporado al Sistema Infomex Jalisco, se hace de forma confidencial, en sobre cerrado. Posteriormente, la persona responsable de manipular el sistema, puede cambiar el login, el nombre de su usuario y contraseña. Este Instituto, tiene acceso íntegro en los primeros dos casos, mientras que la contraseña se encuentra en formato encriptado. Este Instituto como administrador del sistema Infomex Jalisco, cuenta con una base de datos que relaciona los nombres de usuario, identificados por cada sujeto obligado adherido al sistema, con su respectiva contraseña encriptada, es decir, ésta no se puede leer a simple vista. Sin embargo existen programas informáticos especializados, que pueden acceder a estos datos encriptados. Cada usuario del sistema Infomex Jalisco, es responsable de la confidencialidad de su contraseña o clave, por lo que el propio sistema sugiere a los usuarios realicen el cambio de esta contraseña o clave por una designada por ellos, al hacerlo automáticamente cambia también en la base de datos mencionada en el apartado anterior, sin embargo, éstas conservan su confidencialidad al contar con un formato encriptado. Se clasifica como información reservada, la contenida en la base de datos almacenada en uno de los servidores en custodia, por la Coordinación de Informática y Sistemas.
VI. El plazo de reserva o la especificación de reservado por evento:	Por el tipo de información que se trata y conforme a la prueba de daño realizada, la información será reservada por el plazo máximo de diez años, a partir de la fecha de suscripción de la presente acta, sin prejuzgar que, en caso de existir causas para desclasificar la información, el plazo podrá disminuirse mediante la correspondiente acta que se celebre.
¿Dónde la puedo encontrar?	http://www.itei.org.mx/v3/documentos/art8-6j/actaclasifica/2010/acta_clasificacion31_mayo_2010.pdf

Respecto a la interpretación de cada categoría para el registro de los Sistemas de Información Reservada por cada sujeto obligado, se entiende por:

Rubro temático: Materia o asunto general o específico sobre los que la unidad administrativa ejerce sus atribuciones.

La unidad administrativa interna que generó, obtuvo, adquirió, transformó o conserva la información: Unidad administrativa interna que deberá hacer del conocimiento del Comité de Clasificación de Información Pública, sobre de la información que tenga en posesión y que pueda revestir la calidad de información reservada, conforme al artículo 18 de la Ley de la materia.

La fecha de la clasificación: Fecha en la que el Comité de Clasificación de Información Pública del sujeto obligado, sesionó y clasificó como reservada la información materia del acta correspondiente.

El fundamento legal: Artículo de la ley aplicable que dé certeza jurídica al caso concreto.

El plazo de reserva o la especificación de reservado por evento: El que se señale de conformidad con lo establecido en el artículo 19 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios.

En su caso, las partes el documento que se consideran como reservadas: Son las palabras, renglones o párrafos del documento que contienen información reservada, y que deben ser testados de conformidad con lo establecido en los Lineamientos para la elaboración de versiones públicas de documentos, que contengan información reservada o confidencial, y que aplican para los sujetos obligados contemplados en el artículo 24 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios.

El Sistema de Información Confidencial

La identificación de un sistema de información confidencial, requiere de un mayor esfuerzo, puesto que sus elementos de composición pueden resultar más complejos y novedosos. Por esa razón, es pertinente mencionar algunos factores que ayudan a determinar si se está ante un sistema de información confidencial, como lo son: la finalidad y los usos previstos por el cual se recaban datos personales, las personas o grupos de personas sobre los que se pretenda obtener o que resulten obligados a suministrarlos, el procedimiento de recolección de la información confidencial, los tipos de datos incluidos en el mismo y el sujeto obligado responsable.

Estos sistemas, se definen por el propósito y finalidad por el que se recolectan los datos personales, sobre las que se debe dar cumplimiento a las disposiciones legales en materia y aquellas que resulten aplicables.

Al interior de un sujeto obligado existen: sistemas de datos personales relativos al personal que labora en el ente, sistemas de proveedores y, dependiendo de su actividad específica, habrá sistemas de beneficiarios, contribuyentes, becarios, prestadores de servicio social y otros sistemas específicos, que obedecerán a la especialidad de las atribuciones que tiene cada institución.

Entonces, un sistema de datos personales, es un conjunto organizado de datos de carácter personal, cualquiera que sea su soporte, organización o acceso, siempre que tenga una estructura que permita un fácil acceso a los datos de una persona determinada.

Para determinar si la información que posea cualquier sujeto obligado se cataloga como información confidencial, deberán considerarse las siguientes hipótesis:

a) Que corresponda a una persona física, identificada o identificable, debiendo entenderse como identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, y que en razón de su contenido permite acceder al conocimiento de diversos aspectos de la persona, incluso obtener una imagen diversificada y compleja de la misma, apta para establecer perfiles de categorización a través de múltiples operaciones de tratamiento a que puedan ser sometidos, que puedan vincularse entre sí, afectando los datos más frágiles y vulnerables en la esfera del ser humano, a través de la exhibición pública y de la incursión sin consentimiento previo a la vida intima y familiar.

b) Que los datos de una persona se encuentren contenidos en sus archivos y que los mismos constituyan una asociación entre la información y la persona.

De la misma información referida, los datos personales sensibles deberán ser clasificados como información confidencial, en cuanto a las personas jurídicas, es la relativa al estado económico, comercial o la relativa a su identidad que de revelarse, pudiera anular o menoscabar su libre y buen desarrollo.

Datos personales: Es toda información numérica, alfabética, grafica, fotográfica, acústica o de cualquier otro tipo, susceptible de tratamiento respecto a una persona haciéndola identificable y determinado.

Datos personales sensibles: aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste.

En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual.

Para registrar un sistema de información confidencial, es previo requisito elaborar un **Aviso de Confidencialidad**, que debe cumplir con ciertos requisitos:

a) No usar frases inexactas, vagas o ambiguas;
b) Tomar en cuenta, para su redacción, los perfiles de los titulares de los datos personales.
c) No incluir textos o formatos que induzcan al titular a elegir una opción en específico;
d) En caso de que se incluyan casillas para que el titular otorgue su consentimiento, las mismas no deberán estar marcadas previamente; y
e) No remitir a textos o documentos que no estén disponibles para el titular;

II. Información:

a) La identidad y el domicilio del sujeto obligado que trata la información confidencial;
b) La información confidencial que será sometida a tratamiento;
c) El señalamiento expreso de información confidencial sensible que se tratarán;
d) Las finalidades del tratamiento;
e) Los mecanismos mediante los que el titular pueda manifestar su negativa para el trata-

miento de su información confidencial para aquellas finalidades que no son necesarias, ni hayan dado origen a la relación jurídica con el responsable;

f) Las transferencias de información confidencial que, en sucaso, se efectúen; el tercero receptor de los datos personales y las finalidades de las mismas;
g) La cláusula que indique si el titular acepta o no la transferencia cuando así lo requiera;
h) Los medios y el procedimiento para ejercer los derechos acceso rectificación cancelación y oposición;
i) Los mecanismos y procedimientos para que, en su caso, el titular pueda revocar su consentimiento al tratamiento de su información confidencial;
j) Las opciones y medios que el sujeto obligado ofrece al titular para limitar el uso o divulgación de la información confidencial;
k) La información, en su caso, sobre el uso de mecanismos en medios remotos o locales de comunicación electrónica, óptica u otra tecnología, que permita recabar datos personales de manera automática y simultánea al tiempo que el titular hace contacto con los mismos; y
l) Los procedimientos y medios a través de los cuales el responsable comunicará a los titulares los cambios al aviso de confidencialidad.

Algunas preguntas que se podrán hacer para iniciar con el proceso de creación de su aviso de confidencialidad y que podrán dar como resultado la base para su generación son:

- **Identificación:** ¿Quién tiene los datos y dónde se encuentra el responsable?
- **Finalidad:** ¿Para qué se necesitan y en qué los van a utilizar?
- **Negativa:** ¿Cuál es la forma en que el ciudadano puede negarse a que sus datos se utilicen para otros fines?
- **Datos:** ¿Qué tipo de datos personales, serán recabados? (revisar tipos en anexo A)
- **Transferencias:** ¿A quién o quiénes se les compartirán los datos?
- **Trámite:** ¿Cómo se ejercita el derecho a la protección y en dónde puede presentarse la solicitud de protección?
- **Consentimiento:** ¿En dónde puede el ciudadano revocar, modificar u oponerse al uso?
- **Tecnología:** ¿Cuento con tecnología que me permita que recabar datos personales? (registro de hábitos de navegación en los portales)

En la creación del aviso de confidencialidad siempre se deberá observar, el desarrollo de cada uno de los sistemas, mismos que para su registro deben cumplir con algunos requisitos que en su integración, tratamiento y tutela, que permitan la validación por cada Comité de Clasificación y el reconocimiento del ITEI.

En ese sentido, es pertinente precisar cada categoría solicitada, lo cual introduce y delimita cada una de ellas de la siguiente forma.

I. **La finalidad del sistema y los usos previstos para el mismo.**
El propósito para la recopilación de la información personal y el uso previsto, se refiere al empleo o destino que se le da a los datos personales obtenidos.

II. **Las personas o grupos de personas sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.**
Indicación de la denominación del grupo o sector del que se realice la obtención, manejo o tratamiento de dicha información, o que resulten obligados a suministrarlos.

III. **El procedimiento de recolección de la información confidencial;**
La forma o mecanismo por medio del cual se obtienen los datos personales (formulario, internet, transmisión electrónica o cualquier otro método)

IV. **La estructura básica del sistema y la descripción de los tipos de datos incluidos en el mismo;**

Estructura básica del sistema y la descripción de los tipos de datos incluidos.		
Datos Generales del Sistema		
Área	**Responsable**	**Cargo**
La instancia responsables del tratamiento del sistema de información confidencia	Responsable: el servidor público de la unidad administrativa a la que se encuentre adscrito el sistema de información confidencial, designado por el titular del ente público, que decide sobre el tratamiento de datos personales, así como el contenido y finalidad de los sistemas de información confidencial. Nota: se recomienda que el responsable sea el mayor jerárquico de cada área administrativa, esto con la finalidad de controlar e identificar de forma eficaz el sistema en donde se encuentra contenido el dato personal, cuando el ciudadano ejerza sus derechos ARCO	Deberá indicar el nombramiento del responsable
Domicilio	**Teléfono**	**Correo electrónico**
Deberá indicar el domicilio institucional del responsable.	Deberá señalar el teléfono institucional del responsable.	Deberá contener el correo institucional del responsable
Encargado(s)		
Área	**Encargado**	**Cargo**
Deberá indicar el área a la que se encuentra adscrito el servidor público denominado como encargado.	Encargado (s); los servidores públicos que en ejercicio de sus atribuciones, realiza tratamiento de datos personales de forma cotidiana. Nota: se recomienda incluir a todo servidor público que tenga que ver con los datos personales contenidos en el sistema, y deberá coincidir con las cesiones internas de las que sea objeto el sistema.	Señalar el nombramiento del encargado
Datos personales incluidos en el Sistema.		
Tipo de datos personales (Ver anexo A)		
Tipo de tratamiento	Definir si el tratamiento es automatizado, parcialmente automatizado y/o no automatizado	

V. De la cesión de las que pueden ser objeto la información confidencial;
Toda obtención de datos resultante de la consulta de un archivo, registro, base o banco de datos, una publicación de los datos contenidos en él, su interconexión con otros sistemas y la comunicación de datos realizada por una persona distinta a la interesada, así como la transferencia o comunicación de datos realizada entre entes públicos, estableciendo su finalidad la cual está estrechamente vinculada al ejercicio de competencias legales y al cumplimiento de funciones administrativas.

VI. El sujeto obligado responsable;
Definir el nombre del sujeto obligado al que le corresponde administrar cada sistema de información confidencial.

VII. El nivel de protección exigible.
Los sujetos obligados deben mantener medidas de seguridad pertinentes con la indicación del nivel de seguridad que resulte aplicable, básico, medio o alto.

El responsable o encargado del sistema de información confidencial, debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

Las medidas de seguridad previstas revisten dos características principales:

Se trata de medidas que constituyen mínimos exigibles, por lo que el ente público deberá observarlas sin perjuicio del estado la tecnología, la naturaleza de los datos almacenados y los riesgos a los que están expuestos.

El ente público debe adoptar las medidas adicionales que estime necesarias para garantizar la protección y resguardo de la información. Las medidas son acumulativas, es decir, el nivel medio implica la adopción de medidas de seguridad descritas en este nivel, más las dispuestas para el nivel básico y las de nivel alto, implican la adopción de las medidas definidas para los tres niveles (básico, medio y alto).

Algunas de las siguientes preguntas nos ayudaran a delimitar nuestras medidas de seguridad y con ello, garantizar la debida protección y resguardo de la información en nuestros sistemas de información confidencial.

	Pregunta	Explicación/ Respuesta
Medidas de Seguridad	¿Ha adoptado medidas de seguridad con el propósito de evitar la alteración, pérdida, transmisión y acceso no autorizado a los datos personales que se tratan en sus sistemas de información confidencial?	Si es así, indique cuáles son esas medidas de seguridad y si se encuentran descritas en algún documento de la dependencia o entidad.
	Con objeto de determinar las medidas de seguridad a aplicar para evitar su alteración, pérdida, transmisión y acceso no autorizado, indique cuáles datos personales trata en sus sistemas de información confidencial.	Se trata de describir cómo es el sistema de información confidencial en el que se aplican las medidas de seguridad.
	Describa brevemente cómo es el sistema de información, que se utiliza para tratar los datos personales. Por ejemplo, equipos de proceso conectados a una red interna; equipo de proceso portátil, etc.	Indique cuáles son los datos personales que trata en el Sistema de información confidencial, con el fin de poder determinar las medidas de seguridad que serían aplicables al mismo.
	¿Cuál es el nombre del sistema de información confidencial con el que lo ha comunicado al Instituto?	Para identificar el sistema de información confidencial al que se aplican las medidas de seguridad diga cuál es el nombre con el que identifica el sistema.
	¿En qué tipo de ficheros informáticos se tratan los datos personales: base de datos, hoja de cálculo, procesador de textos, etc?	Indique en qué tipo de informáticos se tratan los datos personales.
	¿En qué soporte informático se tratan los datos personales (disco duro, CD, DVD, disquetes, etc.)?	Indique en qué tipo de soporte o soportes informáticos se tratan los datos personales.

Identificación	¿Cómo se identifica a los usuarios (por usuario debe entenderse tanto una persona física como un proceso informático) que acceden a datos personales en el sistema de información confidencial?	Señale si para identificar a los usuarios se utiliza un nombre de usuario (login) u otro método
	¿Cómo se comprueba (autentica) que un usuario que accede a datos personales en el sistema de información es quién dice ser?	Indique cómo se comprueba la identidad de un usuario, por ejemplo mediante contraseñas (password), etc.
	Si la autenticación de los usuarios se hace mediante el uso de contraseñas, ¿Existe un procedimiento para asignar las contraseñas, distribuirlas, guardarlas?	Si se utilizan contraseñas para autenticar la identidad de los usuarios indique si hay un procedimiento para asignar las contraseñas, distribuirlas y guardarlas.
Autenticación	El procedimiento indicado en el apartado anterior, ¿garantiza la confidencialidad e integridad de las contraseñas?	Indique si este procedimiento garantiza la confidencialidad e integridad.
Incidencias	En caso de que se produzca una incidencia que afecte a la seguridad de los datos personales, ¿cómo se actúa ante esta situación?	Describa cómo se actúa ante una incidencia que se produzca en el sistema de información confidencial en el que se traten datos personales. Indique si hay establecido un procedimiento o se adoptan otras medidas.
	Si hay establecido un procedimiento para responder a las incidencias, explique en qué consiste. Por ejemplo, si se lleva a cabo un registro de las incidencias en el que quede constancia de: • La incidencia, • El momento en que se ha producido, • La persona que la notifica, a quién se comunica y • Los efectos derivados de la misma.	Si cuenta con un procedimiento para gestionar las incidencias explique cómo es y, en su caso, si refleja los aspectos que aquí se indican.
	Si como consecuencia de una incidencia se han tenido que recuperar datos personales, ¿queda constancia de la persona que los ha recuperado y los datos que han tenido que ser recuperados?	Indique qué información se hace constar en caso de que haya sido necesario recuperar datos como consecuencia de una incidencia que se haya producido en el sistema de información confidencial.
	Para recuperar los datos, ¿es necesaria alguna autorización del responsable del sistema?	En caso de que sea necesario recuperar datos señale si ese proceso tiene que ser autorizado por el responsable del sistema u otra persona.

Acceso	Los usuarios del sistema de datos personales, ¿pueden acceder a cualquier información o su acceso está limitado únicamente a aquél para el que se les haya autorizado?	Indique si los usuarios pueden acceder libremente a los datos personales que se tratan en el sistema o su acceso únicamente está limitado a aquéllos para los que estén autorizados.
	En caso de que el acceso de los usuarios se haga previa autorización, ¿qué criterios se siguen para otorgar ésta (funciones que cumple, etc.)?	Si el acceso a los datos por el usuario tiene que ser autorizado indique con base en qué razones se proporciona (cumplimiento de una determinada función, puesto desempeñado, etc.)
	En su caso, ¿quién establece los criterios para conceder o denegar el acceso a los datos o al sistema?	Indique quién es la persona o cargo en la dependencia o entidad que concede, modifica o deniega el acceso de los usuarios.
	Si el acceso de los usuarios tiene que ser autorizado, ¿se lleva una relación actualizada de los mismos?	Señale si se lleva a cabo una relación de los usuarios a los que se autoriza el acceso.
	El acceso físico a los locales donde están los sistemas de información y equipos de proceso, ¿puede realizarse por cualquier persona o solamente por la que se encuentre autorizada para ello?	Responda si el acceso físico a los lugares donde estén ubicados los sistemas de información o equipos de proceso está limitado sólo a al personal autorizado o si puede realizarse por cualquiera.
	¿Se lleva un registro (log) de los accesos a los sistemas de información confidencial?	Indique si se lleva un registro de los accesos y que información se deja de los mismos (usuario que accede, hora, fecha, tipo de acceso, etc.).

Anexo A

Clasificación de datos personales:

- **Datos identificativos:** El nombre, domicilio, teléfono fijo, teléfono móvil, firma, clave de Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP), Clave de Elector, Matrícula del Servicio Militar Nacional, número de pasaporte, lugar y fecha de nacimiento, nacionalidad, edad, fotografía y demás análogos.
- **.Datos de origen:** Documentos que contengan datos referentes al origen étnico o racial.
- **Datos ideológicos:** Son aquellos referentes a la ideología u opinión política, opinión pública, afiliación sindical y creencia o convicción religiosa y filosófica.
- **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 estupefacientes, uso de aparatos oftalmológicos, auditivos, prótesis, estado físico o mental de la persona, así como la información sobre la vida sexual.
- **Datos laborales:** Documentos de reclutamiento y selección, nombramiento, incidencia, capacitación, actividades extracurriculares, referencias laborales, referencias personales, solicitud de empleo, hoja de servicio y demás análogos.
- **Datos patrimoniales:** Los correspondientes a bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, fianzas, servicios contratados, referencias personales y demás análogos.
- **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.
- **Datos académicos:** Trayectoria educativa, calificaciones, títulos, cédula profesional, certificados y reconocimientos y demás análogos.
- **Datos de tránsito y movimientos migratorios:** Información relativa al tránsito de las personas dentro y fuera del país, así como información migratoria.

Anexo B

Sistema de Información Confidencial de _____

Datos de identificación			
Fecha de Elaboración.	Día	Mes	Año
Sujeto Obligado.			
Unidades Administrativas Responsables.			

Contenido del Sistema	
Finalidad de sistemas y los usos previstos.	
Las personas o grupos de personas sobre las cuales se obtienen los datos.	
Procedimiento de recolección	

Estructura básica del sistema y la descripción de los tipos de datos incluidos		
Datos Generales del Sistema		
Área	Responsable	Cargo
Domicilio	Teléfono	Correo electrónico

Encargado(s)		
Área	Encargado	Cargo

Datos personales incluidos en el Sistema	
Tipo de datos personales	
Tipo de tratamiento	

Cesión de la que puede ser objeto la información confidencial		
Cesión de la información	Finalidad de la cesión	
Nivel de protección exigible	Básico	
	Medio	
	Alto	

Fundamentación