INSTITUTO DE SEGURIDAD SOCIAL
PARA LAS
FUERZAS ARMADAS MEXICANAS

Normatividad

Adjetiva

Criterios Específicos de Seguridad en los Sistemas de Datos Personales del ISSFAM.

29 marzo
2022

Criterios Específicos de Seguridad en los Sistemas de Datos Personales del ISSFAM.

Introducción:

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), con fecha 26 de enero de 2017, publicó en el Diario Oficial de la Federación, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, la cual tiene como finalidad garantizar la protección de los datos personales para evitar se haga mal uso, comercialice, destruya, utilice o altere total o parcialmente la información que se encuentra bajo el resguardo de los sujetos obligados.

En virtud de lo anterior, se implementaron Criterios Específicos de Seguridad en este Instituto, que establecen los mecanismos de seguridad y protección en los sistemas de datos personales, contando con las condiciones técnicas y normativas de organización y funcionamiento de programas, equipos e instalaciones.

Del mismo modo, se atiende la necesidad de garantizar a las personas que el tratamiento dado a sus datos será el estrictamente necesario para el que fueron recabados o generados, así como el acceso, rectificación, cancelación y oposición de los mismos por parte de sus titulares, por lo anterior, la protección de los datos personales de las y los ciudadanos, implica observar principios y obligaciones establecidos en la ley de la materia antes citada, y permitirles el ejercicio de sus derechos a fin de garantizar en todo momento el respeto a su privacidad.

Objetivo

Los presentes Criterios tienen como objetivo establecer los principios y regular el acceso, rectificación, cancelación y oposición por parte de las y los Titulares, el tratamiento, las políticas de mantenimiento, seguridad y protección que se deberán observar para exactitud, la actualización, la seguridad, la difusión, la distribución y la transmisión de datos personales.

Marco Normativo

Externo:

- Constitución Política de los Estados Unidos Mexicanos.
- Ley Orgánica de la Administración Pública Federal.
- Ley Federal de Transparencia y Acceso a la Información Pública.
- Ley General de Transparencia y Acceso a la Información Pública.
- Ley General de Protección de datos Personales en Posesión de Sujetos Obligados.
- Ley General de Responsabilidades Administrativas.
- Lineamientos para la elaboración de versiones públicas, por parte de las Dependencias y Entidades de la Administración Pública Federal.
- Lineamientos para la Organización y Conservación de los Archivos de las Entidades y Dependencias de la Administración Pública Federal.

- Lineamientos para la Protección de Datos Personales.
- Lineamientos para la Clasificación y Desclasificación de Información de las Dependencias y Entidades de la Administración Pública Federal.
- Lineamientos que deberán observar las Dependencias y Entidades de la APF en la recepción, procesamiento, trámite, resolución y notificación de las solicitudes de acceso a datos personales que formulen los particulares, con exclusión de las solicitudes de corrección de dichos datos.
- Lineamientos que deberán observar las Dependencias y Entidades de la Administración Pública Federal en la recepción, procesamiento, trámite, resolución y notificación de las solicitudes de corrección de datos personales que formulen los particulares.
- Manual Administrativo de aplicación general en las materias de transparencia y archivos.
- Guía para la elaboración de un documento de seguridad emitida por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, el 17 de julio de 2009.

Interno:

- Ley del Instituto de Seguridad Social para las Fuerzas Armadas Mexicanas.
- Estatuto Orgánico del Instituto de Seguridad Social para las Fuerzas Armadas Mexicanas.
- Condiciones Generales de Trabajo.
- Criterios Específicos para la Clasificación y Desclasificación de Información en el Instituto de Seguridad Social para las Fuerzas Armadas Mexicanas.
- Criterios Técnicos para la Organización y Conservación de los Archivos en el ISSFAM.

Definiciones

Para los efectos de los presentes criterios, además de las definiciones establecidas en el artículo 3 de la Ley General de Protección de datos Personales en Posesión de Sujetos Obligados y Guía para la elaboración de un Documento de Seguridad, se entenderá por:

- **Accesos autorizados.-** Autorización concedida a las y los usuarios para la utilización de los sistemas de datos.

- **Área de consulta de datos personales.-** Espacio destinado para que el personal autorizado examine aquellos datos personales que están autorizados a consultar, sin posibilidad de modificar su contenido.

- **Área de recepción de datos personales.-** Espacio donde se reciben datos personales en cualquier tipo de soporte (físico, electrónico, o ambos) en tanto se siguen las demás fases de su tratamiento para integrarlos a uno o más sistemas de datos personales.

- **Área de resguardo de datos personales.-** Espacio para almacenar datos personales que han recibido el tratamiento correspondiente para que formen parte integral de uno o más sistemas de datos personales.

- **Autentificación.-** Comprobación de la identidad de una o un usuario de datos, asociado a una contraseña con su nombre.
- **Consentimiento.-** Es la manifestación de la voluntad expresada verbalmente o por escrito, por la cual la o el titular de los datos personales da su consentimiento o su negativa para que se proporcione información confidencial referente a su persona.
- **Control de acceso.-** Dispositivo que, por medio de la identificación y autenticidad, permite el acceso al sistema de datos.
- **Comité.**- El Comité de Transparencia del ISSFAM.
- **Copia de respaldo.**- Copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.
- **Derechos ARCO:** Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales.
- **Divulgación de incidentes.-** Acciones que adoptan la y el Titular de la dependencia o entidad y la o el Responsable de los sistemas de datos personales, a efecto de dar a conocer a las autoridades competentes, a las o los titulares de los datos, y en su caso, al público en general, los actos deliberados (intrusión, robo, etc.), los acontecimientos de caso fortuito o de fuerza mayor (desastres naturales, incendios, huelgas, etc.), que hubieran ocasionado la pérdida total o parcial de los datos personales bajo custodia.
- **Documento de Seguridad.**- Documento que contiene las medidas de Seguridad Administrativa, física y técnica, aplicable a un Sistema de Datos Personales con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información que este contiene.
- **Encargada o Encargado.-** Cualquier otra persona física o moral facultado por un instrumento jurídico expresamente autorizado por la o el Responsable para llevar a cabo el tratamiento físico o automatizado de los datos personales.
- **Identificación.-** Proceso de reconocimiento de identidad de un usuario, mediante una credencial con fotografía emitida por el ISSFAM, o por cualquier otro como credencial del IFE o INE.
- **INAI.-** Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.
- **Incidencia.-** Es toda aquella anomalía que pueda surgir y que afecte la seguridad de los datos.
- **Intrusión.-** Acción que una o más personas realizan para introducirse, sin derecho, en uno o más sistemas de datos personales a fin de alterar, copiar o sustraer datos personales que forman parte de esos sistemas.

- **ISSFAM.-** Instituto de Seguridad Social para las Fuerzas Armadas Mexicanas.
- **Ley.**- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- **Fichero.-** Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.
- **Personal Autorizado.-** Encargadas o Encargados y Usuarias o Usuarios, las y los servidores públicos que han recibido autorización para interactuar con uno o más sistemas de datos personales por parte del Responsable de dichos sistemas.
- **Personal de Informática.-** Personal que labora en el área de tecnologías de información, sistemas, telecomunicaciones u otras análogas.
- **Recurso.-** Cualquier parte componente de un sistema de información de carácter personal o confidencial.
- **Responsable.-** La o el servidor público titular de la unidad administrativa designado por el titular de la dependencia o entidad, que decide sobre el tratamiento físico o automatizado de datos personales, así como el contenido y finalidad de los sistemas de datos personales.
- **Sistema de datos personales (SDP).-** El conjunto de datos personales que estén en posesión de un sujeto obligado.
- **Soportes electrónicos.-** Medios de almacenamiento inteligibles sólo mediante el uso de algún aparato con circuitos electrónicos que procese su contenido para examinar, modificar o almacenar los datos; es decir, cintas magnéticas de audio, vídeo y datos, fichas de micro film, discos ópticos (CDs y DVDs), y demás medios de almacenamiento masivo no volátil.
- **Soportes físicos.-** Medios de almacenamiento inteligibles a simple vista, es decir, que no requieren de ningún aparato que procese su contenido para examinar, modificar o almacenar los datos; es decir, formularios impresos llenados “a mano” o “maquina”, fotografías y placas radiológicas, entre otros.
- **Usuaria o Usuario.-** Personal de las unidades administrativas del ISSFAM autorizado para acceder a la base de datos de carácter personal o confidencial.

PRINCIPIOS RECTORES DEL SISTEMA.

En el tratamiento de datos personales, las y los usuarios, responsables y las y los encargados del ISSFAM deberán de observar los siguientes principios:

- **Seguridad Jurídica:** Es la conducta a seguir sobre las decisiones del ISSFAM, al sistema de datos personales, remitiéndose al marco estricto de la Ley.

- **Protección integral:** Se requiere que en todo momento la o el responsable del sistema respete y garantice la protección que exige la interpretación y aplicación de la ley, y tome en cuenta la totalidad de los derechos a que está sujeto la transmisión de datos personales.

- **Transversalidad:** Entendiéndose como el acceso autorizado, por parte de la o del titular a los datos.

- **Disponibilidad:** Es aquella en la cual solo las personas autorizadas pueden tener acceso a la información, Sistema, con las limitaciones de la Ley.

ÁMBITO DE APLICACIÓN

Los presentes Criterios se aplicarán a los datos de carácter personal, registrados en medios físicos (expedientes de personal y clínicos), como automatizados (bases de datos del personal militar retirado, derechohabientes, pensionistas, pago de sus prestaciones, así como del personal que labora en el Instituto) en poder de las y los responsables de las Unidades Administrativas del ISSFAM.

Mismos que resultan aplicables a las Direcciones dentro del ISSFAM, que manejan Sistemas de Datos Personales, y son:

DIRECCIÓN	UBICACIÓN E INFORMACIÓN
Prestaciones Económicas	Primer Piso. Sistemas relativos a los beneficios que otorga el Instituto a la población objetivo como son: Seguros de vida, Becas, Seguro Institucional, pago a las y los militares retirados y sus derechohabientes como pensiones, pagas de defunción y ayuda para gastos de sepelio.
Prestaciones Sociales y de Salud	Segundo Piso Sistemas relativos a la Información de las y los integrantes de las Fuerzas Armadas Mexicanas en servicio activo y situación de retiro, así como sus derechohabientes, expedientes Clínicos y Dentales del personal que labora en el Instituto.
Vivienda	Quinto Piso Sistemas relativos a la información del personal administrador que maneja las UU.HH.MM. y NN, así como del Fondo de la Vivienda Militar y Créditos Hipotecarios.
Administrativa	Séptimo Piso. Sistemas relativos a la información del personal que labora en el Instituto, así como la información contenida en los archivos.

Los presentes criterios no son aplicables al Órgano Interno de Control, en virtud de que no manejan sistemas con datos personales.

COORDINACIÓN DE LOS SISTEMAS DE DATOS PERSONALES.

La Unidad de Transparencia, dependiente de la Dirección Jurídica, será la encargada ante el INAI de la Información de los Sistemas de Datos Personales, y tendrá las siguientes funciones:

- Actualizar, dar de alta y supervisar los cambios que deban realizarse a cada uno de los sistemas.
- Realizar supervisiones al personal **Encargado** y **Usuario** de los sistemas tanto físicos como automatizados, a fin de verificar que operen de la forma y fin para el que fueron creados.
- Remitir las actualizaciones realizadas de los sistemas, a la Subdirección de Tecnologías de Información y Comunicaciones, para que esta a su vez actualice la información contenida en las páginas web del ISSFAM.

De igual forma, cada Dirección nombrará a una persona responsable, con las siguientes funciones:

- Supervisar el funcionamiento de los sistemas de datos personales, así como la eficiencia de los mismos para su óptimo desempeño.
- Informar a la Unidad de Transparencia sobre cambios en los sistemas de datos como: personal responsable, personal encargado, usuarias y usuarios, altas, bajas, transmisiones, para que se reporten ante el INAI.
- Dar cumplimiento a las medidas de seguridad en el resguardo de los datos personales, conforme a los presentes criterios.
- Ordenar, archivar y resguardar los formatos de protección de datos personales para el conocimiento de la o del Titular de los mismos.

DERECHOS DE LAS Y LOS TITULARES DE LOS DATOS PERSONALES

La o el Titular de los datos personales, deberá ser previamente informado de modo fehaciente e inequívoco:

- De la existencia de un sistema de datos de carácter personal, de la finalidad de la recolección de éstos y de los destinatarios de la información en caso de transmisión de estos.
- Derecho a solicitar la información referente a sus datos personales, el origen de dichos datos así como las transmisiones realizadas.
- De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición; y
- En caso de que se recaben los datos a través de un tercero u otro medio, la o el titular de los datos deberá ser avisado en un término no mayor de treinta días hábiles a partir del momento del registro de los mismos de manera personal o por conducto de su representante.

CONSENTIMIENTO DE LA O EL TITULAR

Cuando exista una solicitud de información requiriendo datos personales, se necesitará el consentimiento de manera fehaciente de la o del titular. Para el caso de solicitud de una persona fallecida, se requerirá el consentimiento de manera fehaciente de la o el cónyuge y/o los parientes en línea recta ascendente y descendente sin limitación de grado y en línea transversal al segundo grado particular de la o el titular.

Los datos de carácter personal, objetos de tratamiento, solo podrán ser transmitidos a terceros, previo consentimiento de la o el titular, lo que es de carácter revocable y no se requerirá consentimiento de la o el titular cuando estos se transmitan entre dependencias, entidades de gobierno y diversas autoridades, en términos de los tratados y los acuerdos interinstitucionales, siempre y cuando la información se utilice para el ejercicio de facultades propias de los mismos.

No será necesario el consentimiento de la o el titular en los siguientes casos:

- Sea requerido por una autoridad Judicial en el ejercicio de sus atribuciones, es decir, este autorizado por una Ley;
- La transmisión sea entre Administraciones Públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.
- Su transmisión, sea relativa a la salud y tenga como finalidad remediar una urgencia médica.

DERECHO DE RECTIFICACIÓN Y CANCELACIÓN

El personal responsable del tratamiento de los datos de carácter personal tendrá la obligación de hacer efectivo los Derechos ARCO por parte de la o el interesado, cuando estos sean inexactos o incompletos, los cuales deberán conservarse durante los plazos previstos por la Ley y entre las relaciones de entidades.

FASES DEL TRATAMIENTO DE LOS DATOS PERSONALES

El tratamiento puede ser a través de diversas operaciones, ya sean físicas o por medios electrónicos, de manera que permiten: recabar datos personales, registrarlos en una base de datos, modificarlos, consultarlos, utilizarlos, comunicarlos, bloquearlos o incluso, destruirlos.

El tratamiento de los datos personales puede dividirse en tres fases o momentos que son:

1. El momento de la toma de los datos personales, es decir, cuando los datos se recaban de la persona.

2. El momento del tratamiento de los datos que, incluso pueden ser cruzados y relacionados junto con otros datos.

3. El momento de la utilización y, en su caso, comunicación de los resultados del tratamiento.

TRANSMISIÓN DE DATOS PERSONALES

En al ámbito de sus funciones, el ISSFAM para otorgar las prestaciones tanto al personal militar retirado, pensionistas, derechohabientes, así como los beneficios, derechos y obligaciones a sus empleadas y empleados, podrá realizar transmisiones de datos personales a diversas dependencias y entidades de la administración pública federal.

Dichas transmisiones se llevarán cabo considerando lo siguiente:

- Responsable directo.
- Tipo de datos
- Forma en que se transmiten
- Seguridad que se aplica y
- Responsable de la Dependencia donde se recibe la transmisión.

Asimismo, la transmisión podrá realizarse de dos formas, en soportes físicos y/o automatizados.

- **Transmisión de datos personales y traslado en soportes físicos:**

  La o el gestor previamente autorizado por la Unidad Administrativa, entregará la información a un destinatario, en caso de no encontrarse, la entregará a un destinatario secundario, previamente definido. El paquete con datos personales en soportes físicos deberá ir debidamente sellado, de forma tal que no sea sujeto de cualquier violación o apertura no autorizada del mismo. A la entrega del paquete a la o el destinatario deberá acreditar su identidad, presentando identificación oficial con fotografía (credencial de elector, pasaporte, etc.) y el personal de mensajería recabará el nombre, firma y un número de referencia que aparezca en tal identificación además de la fecha de entrega, en caso de que no se encuentre la o el destinatario se entregará al secundario.

  Asimismo, la o el Encargado o usuario y Usuaria del Sistema de Datos Personales verificará que el personal de mensajería haya entregado el paquete a la o el destinatario, como medida de seguridad. En caso de que se detecte que el paquete se entregó a otra persona, se reportará a la o el Titular de la Unidad Administrativa, así como a la o el destinatario de la información, a fin de reportarlo como un incidente.

- **Transmisión y traslado de datos personales en soportes electrónicos:**

  Para la transmisión de datos personales en medios electrónicos, el archivo deberá contar al menos con las siguientes medidas de seguridad, a fin de garantizar que la información no sea alterada:

A. En caso de que sea transmitida a través de correo electrónico, este deberá estar plenamente identificado, siendo solamente correos oficiales.

B. Los archivos deberán estar encriptados, mediante claves de acceso que solamente el destinatario primario conocerá.

C. Los archivos electrónicos deberán contar con protección de escritura, a fin de evitar que la información sea alterada.

D. Se deberá recabar por escrito acuse de recibo del destinatario, por correo electrónico o mediante oficio.

E. En caso de transmisión de datos personales se realice a través de sistemas previamente establecidos por las o los destinatarios, como Secretaría de la Función Pública o de Gobernación, se contará con la identificación de todas y todos los empleados que cuenten con acceso a dichos sistemas, así como un registro de las transmisiones que se lleven a cabo.

F. Cuando se traslade físicamente información en soportes electrónicos se tomarán las medidas antes mencionadas en cuanto a soportes físicos.

No se realizarán transmisiones de datos personales, objetos de un tratamiento temporal o definitivo, a otras Dependencias Gubernamentales que no proporcionen un nivel de protección similar, cuando menos, al que maneja el ISSFAM.

La ejecución de tratamiento de datos de carácter personal fuera de la Unidad Administrativa que contiene los ficheros y/o sistemas de datos personales deberá ser autorizada expresamente por la o el responsable del fichero y/o sistema y, en todo caso, deberá garantizarse el nivel de seguridad correspondiente.

NIVELES DE SEGURIDAD

De acuerdo a la naturaleza de los datos personales que son objeto de tratamiento, se dividirán en los siguientes niveles de seguridad:

Nivel Básico: Aplicable a todos los sistemas del ISSFAM que contienen datos de carácter personal, considerándose los siguientes rubros:

- De Identificación: nombre, grado, matrícula, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, firma electrónica, RFC, CURP, cartilla militar, lugar de nacimiento, fecha de nacimiento, sexo, nacionalidad, edad, nombres de familiares dependientes y beneficiarias o beneficiarios, fotografía.

- Laborales: Documentos de reclutamiento y selección, de nombramiento, de incidencia, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales.

Nivel medio: Se aplica aquellos sistemas que contienen datos personales que proporcionan un perfil de la persona y que permiten evaluar diversos aspectos de su personalidad como rendimiento laboral, crédito, fiabilidad o conducta; en especial, los que se refieran a su solvencia patrimonial y crédito, los que contengan infracciones administrativas o penales y los relativos a Hacienda Pública y servicios financieros.

- Datos patrimoniales: Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, servicios contratados, referencias personales.

- Datos sobre procedimientos administrativos seguidos en forma de juicio y/o jurisdiccionales: 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 o administrativa.

- Datos Académicos: trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros.

Nivel alto: Se considerarán en el ISSFAM lo siguiente:

- Datos de Salud: Estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, licencias médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos, prótesis, entre otros.
- Características personales: Tipo de sangre, huella digital.
- Características físicas: Color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros.

APLICACIÓN DE LOS NIVELES DE SEGURIDAD.

Todos los ficheros y/o sistemas que contengan datos de carácter personal deberán adoptar las medidas de seguridad calificadas como de nivel básico. Los ficheros y/o sistemas que contengan datos personales y que proporcionen un perfil de la persona y que permitan evaluar diversos aspectos de su personalidad, conducta y su solvencia patrimonial, deberán reunir, además de las medidas de nivel básico, las calificadas como de nivel medio.

Los ficheros y/o sistemas que contengan datos de ideología, religión, creencias, origen racial, salud física, mental, o vida sexual, los expedientes clínicos, así como los que contengan datos recabados para fines judiciales sin consentimiento del personal titular de los datos personales deberán reunir, además de las medidas de nivel básico y medio, las calificadas de nivel alto.

ARCHIVOS MAESTROS QUE CONTIENEN SISTEMAS DE DATOS PERSONALES

Los archivos maestros en los que se alojan los sistemas para el procesamiento de datos y el otorgamiento de prestaciones contempladas en la Ley del ISSFAM son los siguientes:

- Archivo datos generales de causahabientes (PR-DGCA)
- Archivo datos generales de beneficiarios (PR-DGBE)
- Archivo datos generales de personal militar retirado y pensionado que cobran en nómina (XX-RETIR).
- Archivo datos generales de administradores de Unidades Habitacionales (AA-ADMON)

El archivo que emplea los sistemas para el procedimiento de datos de control administrativo es:

- Archivo datos generales de empleadas o empleados de este Instituto (AH-MAEST)

NIVELES DE SEGURIDAD DE LOS SISTEMAS DE DATOS PERSONALES

De los archivos maestros antes señalados, se derivan los siguientes sistemas de datos personales correspondientes a las diferentes Unidades Administrativas:

NOMBRE DEL SISTEMA	NIVEL DE SEGURIDAD	TIPO DE SISTEMA	DATOS PERSONALES
PRESTACIONES ECONÓMICAS			
Producción de la nómina del personal militar retirado y pensionado (físico y electrónico).	MEDIO	Físico /Electrónico	Nombre, domicilio, teléfono particular, firma, estatura, peso, RFC, CURP, lugar de nacimiento, fecha nacimiento, nacionalidad, nombre de familiares, dependientes y beneficiarios, fotografía
Registro y cálculo para el pago de las aportaciones del seguro colectivo de retiro.	MEDIO	Electrónico	Nombre, domicilio, nombre de familiares, dependientes y beneficiarias o beneficiarios.
Registro, control y cálculo del pago del seguro de vida militar	ALTO	Electrónico	Nombre, domicilio, teléfono particular, firma, nombres de familiares dependientes y beneficiarias o beneficiarios, RFC, edad características personales (huella digital).

NOMBRE DEL SISTEMA	NIVEL DE SEGURIDAD	TIPO DE SISTEMA	DATOS PERSONALES
Registro, control y cálculo del pago del seguro institucional	BAJO	Electrónico	Nombre, domicilio, teléfono particular, firma, RFC, nombres de familiares dependientes y beneficiarias o beneficiarios, edad, huella digital.
Registro y control del trámite de ayuda para gastos de sepelio	ALTO	Físico/Electrónico	Nombre, domicilio, teléfono particular, teléfono celular, estado civil, firma, huella digital, RFC, CURP, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, fotografía, nombre de familiares, dependientes y beneficiarias o beneficiarios, títulos.
Registro y control del trámite de pagas de defunción	ALTO	Físico/Electrónico	Domicilio, teléfono particular, teléfono celular, estado civil, nombre, firma, huella digital, RFC, CURP, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y beneficiarias o beneficiarios, fotografía.
Registro, control y selección de beca	B AJO	Físico/Electrónico	Nombre, Nombres de Familiares, Dependientes y Beneficiarias o Beneficiarios.
Registro y control de dictámenes de retiros, pensiones y compensaciones.	ALTO	Físico/Electrónico	Nombre, domicilio, teléfono particular, teléfono particular celular, estado civil, Nombres de Familiares, Dependientes Y Beneficiarias o Beneficiarios, fotografía, firma, CURP, RFC, fotografía, lugar de nacimiento, fecha de nacimiento; características físicas (estatura, complexión, color de cabello, señas particulares, color de iris); datos de salud (discapacidades)

NOMBRE DEL SISTEMA	NIVEL DE SEGURIDAD	TIPO DE SISTEMA	DATOS PERSONALES
DIRECCIÓN DE PRESTACIONES SOCIALES Y DE SALUD			
Expedientes Dentales	ALTO	Físico	Nombre, sexo, ocupación, domicilio, teléfono particular, edad, firma, estado de salud.
Expedientes de la Consulta Médica	ALTO	Físico	Nombre, domicilio, teléfono particular, edad, firma, estado de salud.
Registro y control de la base de datos generales de militares y derechohabientes de la ley del ISSFAM	MEDIO	Electrónico	CURP, lugar de nacimiento, fecha de nacimiento, nombre, nombre de familiares, dependientes y beneficiarias o beneficiarios.
Control de envío de cédulas de identificación de derechohabientes del personal militar en servicio activo y en situación de retiro.	MEDIO	Electrónico	Nombre de Familiares, dependientes y beneficiarias o beneficiarios.
Control de la revista de supervivencia de personal militar retirado y pensionista.	BAJO	Físico/Electrónico	Nombre, domicilio, teléfono particular y firma.
Registro y control de la clave única de registro de población CURP	BAJO	Físico/Electrónico	Nombre, fecha de nacimiento, nacionalidad.
Registro y control de las ventas de gavetas y nichos del cementerio militar.	MEDIO	Físico/Electrónico	Nombre, domicilio, teléfono particular, teléfono particular celular, Nombres de Familiares, Dependientes y beneficiarias o beneficiarios, fotografía.

NOMBRE DEL SISTEMA	NIVEL DE SEGURIDAD	TIPO DE SISTEMA	DATOS PERSONALES
	DIRECCIÓN DE VIVIENDA		
Registro y control de ocupaciones y desocupaciones de viviendas, inventarios, anomalías y ordenes de descuento por desperfectos en las mismas.	MEDIO	Físico/Electrónico	Nombre, grado, estado civil, nombres de familiares.
Registro, Control y Calculo del Pago de la Devolución del Fondo de la Vivienda Militar.	MEDIO	Físico/Electrónico	Nombre, Nombres de Familiares, Dependientes y beneficiarias o beneficiarios.
Registro, control, selección y seguimiento de crédito hipotecario	MEDIO	Físico/Electrónico	Nombre, domicilio, teléfono particular, Nombres de Familiares, Dependientes y beneficiarias o beneficiarios, RFC, lugar de nacimiento, fecha de nacimiento, edad; datos de salud (incapacidades médicas); datos patrimoniales (bienes muebles e inmuebles, cuentas bancarias, seguros)

NOMBRE DEL SISTEMA	***NIVEL DE SEGURIDAD***	***TIPO DE SISTEMA***	***DATOS PERSONALES***
Registro y control de información de los empleados del Instituto, evaluaciones, renovaciones de contrato, historiales.	ALTO	Físico/Electrónico	Nombre, domicilio, teléfono particular, estado civil, edad, fecha de nacimiento, fotografía, firma, nombre de familiares, R.F.C., C.U.R.P., lugar de nacimiento, reconocimientos, títulos, cédula profesional, documentos de reclutamiento y selección, documentos de nombramiento, incapacidades médicas, documentos de capacitación, trabajo actual, trabajos anteriores, puesto, lugar de trabajo.
Registro y control de las aportaciones efectuadas por concepto del Seguro de Ahorro para el Retiro (S.A.R.).	B AJO	Físico/Electrónico	Nombre, RFC, lugar de nacimiento.

NOMBRE DEL SISTEMA	**NIVEL DE SEGURIDAD**	**TIPO DE SISTEMA**	**DATOS PERSONALES**
DIRECCIÓN ADMINISTRATIVA			
Registro de expedientes y control de préstamos en los archivos de Concentración, Prestaciones y Créditos Hipotecarios.	ALTO	Físico/Electrónico	Nombre, domicilio, estado civil, teléfono particular, RFC, firma, lugar de nacimiento, nacionalidad, idioma, nombres de familiares, dependientes y beneficiarias o beneficiarios, fecha de nacimiento, cumplimiento con el servicio militar, fotografía.
Registro y control de impuestos retenidos a las o los empleados para la declaración anual.	B AJO	Electrónico	Nombre, domicilio, teléfono particular, firma, nombres de familiares dependientes y beneficiarios, RFC, edad características personales (huella digital)

NOMBRE DEL SISTEMA	NIVEL DE SEGURIDAD	TIPO DE SISTEMA	DATOS PERSONALES
Cálculo de la nómina para el pago de las y los empleados	B AJO	Electrónico	Nombre, firma, R.F.C., C.U.R.P., incapacidades médicas, trabajo actual, puesto, lugar de trabajo.

MEDIDAS DE SEGURIDAD

Las medidas de seguridad comprenden los tres niveles, las cuales son acumulativas, en el sentido de que un nivel alto debe de cumplir con las medidas de nivel medio y básico y el nivel medio debe de cumplir con las medidas del nivel básico.

Para todos los sistemas de datos personales se deberán observar las siguientes medidas de seguridad:

Acceso en forma física

- El acceso al área de los archivos en el ISSFAM solo se permitirá a personal previamente autorizado.
- La entrega de expedientes se hará únicamente a las y los gestores. previamente identificados en el catálogo correspondiente, el cual se actualizará periódicamente, bajo ninguna circunstancia se llevará a cabo el préstamo de expedientes a personal no autorizado.
- Los préstamos solo se harán dentro de las horas y días laborables.
- Se llevará bitácora para el control del préstamo de expedientes, a través del sistema informático institucional en la cual se asentará el nombre del personal gestor solicitante, área de adscripción, motivo y tiempo de préstamo.
- Los expedientes con datos personales que se otorguen en préstamo deberán contar con la clasificación de información confidencial, así como el precinto, cosido, foliado, sello de liga y una caratula índice.
- La información del resumen dental o clínico, solo podrá ser manejada por personal ~~los~~ médico~~s~~, dentistas y la o el el Titular de los datos personales.

Acceso en forma electrónica

- La o el Responsable del Área solicitará a la Unidad de Transparencia claves de acceso a los SDP señalando los puntos a ingresar.
- El personal usuario de los SDP deberá apegarse a lo acotado en la Responsiva de Clave de Usuario del Sistema de Información del Instituto.
- Cualquier uso ajeno al institucional está estrictamente prohibido.
- La Subdirección de Tecnologías de Información y Comunicaciones tendrá la facultad de implementar un registro del acceso a los SDP, permitiendo identificar a la o el usuario, sistema, fecha y hora en que acceso.
- Queda prohibido la utilización de equipo no autorizado por la Subdirección de Tecnologías de Información y Comunicaciones.
- Las o los usuarios tendrán acceso autorizado únicamente a aquellos sistemas de datos personales que precisen para el desarrollo de sus funciones.

- La Unidad de Transparencia se reserva el derecho de accesar a cualquier equipo de cómputo que se encuentre dentro del ISSFAM con fines de seguridad y verificación de información.

Acceso a la Intranet o Internet del ISSFAM

El acceso a Intranet o Internet, deberá estar acotado por lo siguiente:

- Todas las conexiones a Internet dentro del ISSFAM deberán contar con la respectiva autorización por parte de la o del Director General. Las o los usuarios con acceso a Internet deberán contar con la autorización por parte de su respectiva Dirección, la cual será responsable por el uso y autorización de la conexión que tenga a su cargo.

- Queda prohibido el uso de cuentas de correo electrónico, ajenas a las proporcionadas por el ISSFAM, para cualquier trámite, transmisión y recepción de información y/o realización de trámites que utilicen datos o información del ISSFAM.

- El personal de la Subdirección de Tecnologías de Información y Comunicación se reserva el derecho de monitorear, queda prohibido el acceso a Información de información de carácter personal.

Asimismo, la transmisión interna de datos personales deberá ser exclusivamente para la realización de los trabajos del ISSFAM. Queda prohibido divulgar información confidencial utilizando el Internet o Intranet.

Recepción de datos

- Cuando se recaben datos personales, el personal responsable de recabarlos tendrá la obligación de identificarse a petición de la o el Titular de los datos.

- En los casos que se recaben datos personales a través de un tercero, la o el representante Legal deberá presentar carta poder y copia de identificación y de la o el Titular de los datos.

- Al momento de recabarse los datos personales se hará de conocimiento al Titular de los mismos a través de formato físico, el fundamento legal de la protección de estos, así como su finalidad de dicha recopilación, en los términos dispuestos por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y los Lineamientos de protección de datos personales.

Los datos personales recabados en el presente formato serán protegidos, incorporados y tratados en los Sistemas de datos personales correspondientes del Instituto de Seguridad Social para las Fuerzas Armadas Mexicanas, en donde la y el interesado podrá ejercer los Derechos ARCO ante el mismo.

Para el sistema denominado “Registro y control de información de las o los empleados del Instituto, evaluaciones, renovaciones de contratos e historiales” que maneja la Subdirección de Recursos Humanos, se colocará la siguiente leyenda:

Para el sistema denominado “Registro y control de información de las o los empleados del Instituto, evaluaciones, renovaciones de contratos e historiales” que maneja la Subdirección de Recursos Humanos, se colocará la siguiente leyenda:

Los datos personales recabados en el presente formato serán protegidos, incorporados y tratados en el (los) Sistema(s) de datos personales Registro y control de información de las o los empleados del Instituto.

Los datos personales recabados en el presente formato serán protegidos, incorporados y tratados en el (los) Sistemas (s) de datos personales Registro y control de información de los empleados del Instituto, evaluaciones, renovaciones de contrato e historiales, (los) cual(es) fue(ron) registrado(s) en el listado de sistemas de datos personales ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (www.inai.org.mx), y podrán ser transmitidos a diferentes dependencias gubernamentales como Secretaría de la Función Pública, Secretaría de Hacienda y Crédito Público, ISSSTE, Banjército, Juzgados y a las o los beneficiarios proporcionando la información requerida para los fines que afecte a su competencia, además de otras transmisiones previstas en la Ley mencionada.

La Unidad Administrativa Responsable del sistema de datos personales es la Subdirección de Recursos Humanos, ubicada en Av. Industria Militar No. 1053 séptimo piso, Col. Lomas de Sotelo, Del. Miguel Hidalgo C.P. 11200 México, D.F., donde la o el interesado podrá ejercer los derechos de acceso y corrección ante la misma.

Tratamiento de datos

- No está autorizado por ningún motivo enviar datos personales a empleadas o empleados que no se encuentren involucrados en la gestión del trámite.
- Los datos personales recabados solo serán utilizados para el fin que fueron recabados.
- El plazo de conservación de los datos personales será de acuerdo a las necesidades de cada área administrativa.
- De conformidad con las “Políticas de Uso Adecuados de Equipos y Sistemas” del ISSFAM, “…toda la información contenida en los Sistemas de Información Institucional, así como su integridad, confiabilidad, disponibilidad y exactitud es responsabilidad única y exclusiva de las áreas responsables de tales datos. La Subdirección de Tecnologías de Información y Comunicación será la responsable del buen funcionamiento de los equipos y los sistemas, así como de su disponibilidad, mantenimiento, resguardo y respaldo…”.

Registro de incidencias.

El procedimiento de notificación y gestión de incidencias contendrá necesariamente 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 y los efectos que se hubieran derivado de la misma.

En caso de robo o extravío de datos personales en soportes físicos, la o el Titular de la Unidad de Transparencia, la o el Responsable de los SDP, al tener conocimiento del incidente, informará al Órgano Interno de Control, a la Dirección Jurídica según corresponda, para que cada uno, en el ámbito de sus atribuciones, determine lo conducente.

En caso de robo o extravío de datos personales, se dará aviso a las y los titulares de los datos afectados para que tomen sus precauciones ante el posible uso ilegal de su información. Para tal efecto la o el Responsable de los SDP dará a viso por escrito a dichos titulares, a más tardar cinco días naturales de haber ocurrido el incidente, recabando el acuse de recibo de esta notificación.

Copias de respaldo y recuperación.

- La o el responsable del fichero y/o sistema se encargará de verificar la correcta aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.
- Los procedimientos establecidos para la realización de copias de respaldo y para la recuperación de los datos deberán garantizar su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.
- Las y los responsables de cada sistema de datos personales deberán supervisar que en las diferentes áreas a su cargo se realicen los respaldos de la información contenida en dichos sistemas, a fin de evitar pérdida de información. Por lo anterior, las Unidades Administrativas tendrán la coordinación necesaria con la Subdirección de Tecnologías de Información y Comunicaciones, para llevar a cabo los respaldos necesarios (CDs y/o DVDs u otro medio del que se disponga).

DOCUMENTO DE SEGURIDAD

La Unidad de Transparencia elaborará e implantará un documento de seguridad de carácter obligatorio para el personal encargado y usuario que tenga acceso a los datos personales. El documento deberá mantenerse en todo momento disponible, así como actualizado y será revisado en forma semestral, a fin de actualizarlo si es que existieran cambios relevantes en el sistema o en la organización del mismo.

MANTENIMIENTO DE LOS SISTEMAS DE DATOS PERSONALES

Las y los responsables de los sistemas de datos personales realizarán mantenimiento de la información contenida en los mismos, cuando la o el titular de los datos informe sobre la actualización de algún dato contenido en dichos sistemas.

FUNCIONES Y OBLIGACIONES DE LAS Y LOS RESPONSABLES, ENCARGADOS Y USUARIOS EN EL TRATAMIENTO DE DATOS PERSONALES EN LAS ÁREAS ADMINISTRATIVAS.

Las y los encargados y responsables de los ficheros y/o sistemas, así como las o los usuarios, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal, en los términos establecidos de los presentes criterios, con las siguientes funciones:

1. Mantener control de los equipos asignados a su área (cambio, alta y baja de los mismos).
2. Mantener el acceso restringido y bajo llave el archivo de la Dirección.
3. Proporcionar el préstamo de expedientes a las o los gestores autorizados, utilizando el vale de préstamo respectivo, así como registrar dichos préstamos en el control correspondiente.
4. Vigilar el acceso a los equipos de cómputo y terminales del Instituto.
5. No compartir archivos y carpetas en la red.
6. No extraer cualquier tipo de información, prohibiéndose el uso de equipos y dispositivos de almacenamiento de datos tales como grabadoras de CDs y/o DVDs, memorias USB , tarjetas de memoria, escaners, cámaras fotográficas, discos externos, etc., su uso está confinado para fines completamente indispensables y se deberá contar con la autorización del área de informática.
7. Dar acceso al personal de la Subdirección de Tecnologías de Información y Comunicaciones, a fin de revisar el equipo de cómputo que se encuentre dentro del instituto con fines de seguridad
8. El uso del sistema institucional deberá estar acotado por lo establecido en la “responsiva de usuario”, cualquier uso ajeno a la institucional esta estrictamente prohibido.

FUNCIONES DEL COMITÉ DE TRANSPARENCIA

Son funciones del Comité de Transparencia:

a) Velar por el cumplimiento de los presentes criterios sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de acceso a la información y datos personales.
b) Dictar las instrucciones precisas para adecuar los tratamientos a los principios de la Ley y los presentes criterios.
c) Proporcionar información a las o los titulares de los datos de carácter personal, en materia del tratamiento de sus datos.
d) Requerir a las o los responsables del tratamiento, así como a las o los encargados del sistema la adopción de las medidas de seguridad.
e) Las que le sean atribuidas, derivadas de la protección de datos personales en estricto apego a la Ley de la Materia.

INFRACCIONES Y SANCIONES.

El incumplimiento de las medidas de seguridad descritas en los presentes criterios será sancionado en los términos de la Ley General de Responsabilidades Administrativas, Ley General de Protección de datos Personales en Posesión de Sujetos Obligados independientemente de las que se generen o deriven del orden civil o penal.

TRANSITORIOS

Primero.- Los presentes criterios entrarán en vigor al día siguiente de su aprobación.

Segundo.- Todo lo no previsto en los presentes criterios se resolverá de acuerdo a lo establecido en la Ley Federal de Transparencia y Acceso a la Información Pública, Ley General de Transparencia y Acceso a la Información Pública y Ley General de Protección de datos Personales en Posesión de Sujetos Obligados.

Autorizado por el Comité de Mejora Regulatoria (COMERI), en su sesión ordinaria No. 3 del 29 de marzo de 2022. Aprobado por el Director General, mediante el acuerdo No. DTIPCOS 11222/197/2022 de esa misma fecha.

Titular de la Unidad de Transparencia y Presidente del Comité de Transparencia

Cor. J.M. y Lic., Director Jurídico
Julio César Meléndez García
(B-3986536)

Titular del Órgano Interno de Control e integrante del Comité de Transparencia

Gral. Brig. C.P. Ret. Mtro. Fin.
Alberto Gijón y Berrios
(6208408)

Coordinador de Archivos e
Integrante del Comité de Transparencia

Gral. Div. I.I. Ret.
Salvador Emiliano Aguirre Cervantes
(6416465)