NOMBRE DEL DOCUMENTO: CRITERIOS DE SEGURIDAD PARA LA PROTECCIÓN DE LOS SISTEMAS DE DATOS PERSONALES DE PRONÓSTICOS PARA LA ASISTENCIA PÚBLICA

FIRMAS

REVISÓ:

ARELY FERNANDA VASALLO ERAZO
GERENTE JURÍDICO

SUSANA LÓPEZ GONZÁLEZ
GERENTE DE RECURSOS HUMANOS

ALEJANDRO RAMÍREZ HERNÁNDEZ
GERENTE DE RECURSOS MATERIALES

YEDID NAYELI DÍAZ HERNANDEZ
GERENTE DE SERVICIO MÉDICO

JAIME GARAY TSCHESCHNER
DIRECTOR DE FINANZAS

RAÚL GALINDO QUIÑONEZ
SUBDIRECTOR GENERAL DE SERVICIOS COMERCIALES

LUIS ANGEL RODRÍGUEZ ALEMÁN
SUBDIRECTOR GENERAL DE INFORMÁTICA

JUAN CARLOS GASTELUM TREVIÑO
SUBDIRECTOR GENERAL DE ADMINISTRACIÓN Y FINANZAS

AUTORIZÓ:

VIRGINIA CRISTINA DÍAZ ANAYA
SUBDIRECTORA GENERAL DE ASUNTOS JURÍDICOS

ÍNDICE

I. OBJETIVO

Establecer los criterios y las medidas administrativas, físicas y técnicas de seguridad aplicables a los sistemas de datos personales, que Pronósticos para la Asistencia Pública deberá observar para la protección de los archivos que contengan, generen, obtengan, adquieran, transformen o conserven datos personales, así como, contar con las medidas necesarias para el resguardo de los sistemas de datos personales y evitar que sufran alteración, pérdida o acceso no autorizado**.**

II. ALCANCE

Este documento es de observancia general para las unidades administrativas de Pronósticos para la Asistencia Pública, que manejen datos personales.

III. FUNDAMENTO JURÍDICO Y REFERENCIAS NORMATIVAS

Fundamento Jurídico:

Leyes.

- Constitución Política de los Estados Unidos Mexicanos
- Ley Orgánica de la Administración Pública Federal.
- Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.
- Ley Federal de Procedimiento Administrativo.
- Ley Federal de Responsabilidades Administrativas de los Servidores Públicos.

Reglamentos.

- Reglamento de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

- Reglamento Interior de la Secretaría de la Función Pública.

Lineamientos.

- Lineamientos de Protección de Datos Personales.

- Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal para notificar al Instituto Federal de Acceso a la Información Pública los índices de expedientes reservados.

- 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.

- Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal en la recepción, procesamiento y trámite de las solicitudes de acceso a la información gubernamental que formulen los particulares, así como en su resolución y notificación, y la entrega de la información en su caso, con exclusión de las solicitudes de acceso a datos personales y su corrección.

- 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 acceso a datos personales que formulen los particulares, con exclusión de las solicitudes de corrección de dichos datos.

Otros.

- Recomendaciones sobre medidas de seguridad aplicables a los sistemas de datos personales, emitidas por el IFAI (ahora Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales).

- Guía para elaboración de un documento de seguridad.

Referencias Normativas:

- ISO 9001: Sistemas de Gestión de la Calidad – Requisitos
- ISO/IEC 27001: Sistemas de Gestión de Seguridad de la Información – Requerimientos
- WLA-SCS: Estándar de Control de la Seguridad.

IV. POLÍTICAS

GENERALES

1. Se considera información confidencial, todos los archivos que contengan datos personales y su resguardo será responsabilidad del titular del área que la integre, reciba, obtenga o transforme.

2. Se consideran como áreas responsables de manejar información con datos personales, es decir información confidencial, las que a continuación se describen en la siguiente tabla:

ÁREAS RESPONSABLES	SISTEMA
Dirección de Finanzas	Ganadores de Premios
Gerencia de Recursos Humanos	Administración de Recursos Humanos
Gerencia de Recursos Materiales	Proveedores y Prestadores de Servicio
Gerencia del Servicio Médico	Derechohabientes al Servicio Médico Proveedores del Servicio Médico
Subdirección General de Servicios Comerciales	Base de Datos Integral

3. Las áreas responsables deben reportar al Comité de Información las actualizaciones y transmisiones totales o parciales de datos personales que realicen las Unidades Administrativas de Pronósticos para la Asistencia Pública y de su notificación oportuna a través del “Sistema Persona”.

LOS RESPONSABLES DE LOS SISTEMAS DE DATOS PERSONALES

4. Las áreas responsables que generen, obtengan, adquieran, transformen o conserven datos personales, deben nombrar a un responsable del sistema, el cual debe incorporar los datos referentes al mismo en la aplicación informática establecida por el INAI para este propósito.

5. Las áreas responsables de los sistemas de datos personales deben detallar específicamente el tratamiento, las medidas de seguridad, el tiempo por el que estarán almacenadas y en su caso, la forma de destrucción; además de incluir la leyenda de protección a que se refiere el artículo Decimoctavo de los Lineamientos de Protección de Datos Personales conforme al modelo contenido en el Anexo A y la autorización explícita en el SAJ-06 REGISTRO DE SISTEMA DE DATOS PERSONALES, mismo que puede ser consultado en el Sistema Integral de Gestión de Pronósticos para la Asistencia Pública.

LA IDENTIFICACIÓN DE LOS SISTEMAS DE DATOS PERSONALES Y DEL NIVEL DE SEGURIDAD APLICABLE

6. Se considera un dato personal o información confidencial lo siguiente:

   - La información debe corresponder a una persona física, identificada e identificable.
   - La información debe estar contenida en los archivos o documentos de Pronósticos para la Asistencia Pública.

7. Las áreas responsables deben aplicar, a los sistemas de datos personales que manejan información confidencial, las medidas y el nivel de seguridad, contenidas en el Anexo B de este documento, de acuerdo a las posibilidades y recursos disponibles del área.

APLICACIÓN DE LOS PRINCIPIOS PARA LA PROTECCIÓN DE DATOS PERSONALES

8. El tratamiento de datos personales se hará invariablemente con base en los principios de licitud, calidad, acceso y corrección de información, seguridad, custodia y consentimiento para su transmisión.

9. La creación, integración o posesión de sistemas de datos personales debe obedecer exclusivamente a las atribuciones legales, reglamentarias y/o las establecidas por la Ley Federal de las Entidades Paraestatales y/o en el Estatuto Orgánico de Pronósticos para la Asistencia Pública y deberán obtenerse a través de los medios previstos en dichas disposiciones legales.

10. Los datos personales deben tratarse únicamente para la finalidad determinada y legítima para la cual fueron obtenidos, con la posibilidad de ampliar las aplicaciones o tratamiento de los mismos con fines estadísticos u otros legalmente aceptados, que pueden realizarse siempre y cuando exista la autorización expresa y ésta quede asentada en el formato SAJ-06 REGISTRO DE SISTEMA DE DATOS PERSONALES; mismo que puede ser consultado en el Sistema Integral de Gestión de Pronósticos para la Asistencia Pública, acreditado por el Comité de Información de Pronósticos o acuerdo que hubiera otorgado el titular de los datos.

11. Los sistemas de datos personales se almacenarán de forma tal que permitan a los titulares de los mismos, el ejercicio de los derechos de acceso y corrección previstos por la Ley, el Reglamento y los Lineamientos emitidos por el INAI (Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales).

12. Las áreas responsables deben hacer del conocimiento al titular de los datos, en el momento de recabarlos y de forma escrita, el fundamento y motivo de ello, así como los propósitos para los cuales se tratarán dichos datos.

13. Las áreas responsables que generen o posean sistemas de datos personales, deben adoptar las medidas necesarias para garantizar la integridad, confiabilidad, confidencialidad y disponibilidad de los mismos mediante acciones que eviten su alteración, pérdida, transmisión y acceso no autorizado, conforme lo establecen las políticas de seguridad de la información implementadas por la Entidad.

14. La custodia y cuidado de los datos personales serán responsabilidad directa de los titulares de las áreas; en cuanto a los responsables, encargados y usuarios deben tener un manejo cuidadoso en su tratamiento.

15. Toda transmisión de datos personales deberá contar con el consentimiento explícito del titular de los datos, mismo que deberá otorgarse en forma libre, expresa e informada.

16. Las áreas responsables, conforme al ámbito de su competencia, solo pueden transmitir los datos personales a su resguardo bajo las siguientes condiciones:

    a) Por razones estadísticas o de interés general, posterior a la disociación de los mismos.
    b) Cuando se transmitan con otras dependencias o entidades, siempre y cuando se utilicen para el ejercicio de atribuciones o facultades.
    c) Cuando exista una orden judicial.
    d) Cuando se contrate a terceros para la prestación de un servicio. En este caso se suscribirá preferentemente un convenio de confidencialidad.
    e) Cuando se requieran para dar cumplimiento al artículo séptimo de la Ley, fracción XIII, inciso c).
    f) Cuando sea información de personas a las que se les entreguen por cualquier motivo recursos públicos.
    g) Cuando se hubiera recabado o forme parte de un registro o fuente de acceso público.

TRATAMIENTO DE LOS DATOS PERSONALES

17. Las áreas responsables de los sistemas de datos personales bajo su resguardo, deben tenerlos debidamente integrados y en el caso del “Sistema Persona”, éstos deben de mantenerse actualizados, de manera tal que no altere la veracidad de la información, conforme lo establecen las políticas de seguridad de la información implementadas por la Entidad.

18. Las áreas responsables en el “Sistema Persona” deben verificar periódicamente que los datos que se encuentren, sean exactos y en caso de detectar alguna inexactitud, deberán tomar las acciones necesarias para realizar las correcciones, siempre que posean los documentos que justifiquen la actualización.

19. Las áreas responsables de Pronósticos darán de baja los datos personales que hayan sido objeto de tratamiento y no contengan valores históricos, estadísticos o contables.

20. Los datos personales solo pueden ser utilizados en sistemas de datos personales que cuenten con medidas de seguridad.

21. Las áreas responsables de manejar los datos personales, deben hacer de conocimiento al titular de los datos, los formatos físicos y electrónicos utilizados para el manejo de los mismos, conforme lo establece la Ley, el fundamento legal aplicable y la finalidad del Sistema Persona.

22. Las áreas responsables de Pronósticos que recaben datos personales a través de orientación telefónica, página web, u otros sistemas, deben establecer un mecanismo por el que se debe informar previamente a los solicitantes que sus datos personales serán recabados, la finalidad de este requerimiento, el tratamiento y seguridad que tendrán sus datos. Dicha información en caso de ser almacenada, debe ser reportada en el Sistema Persona y a la Unidad de Enlace de Pronósticos para la Asistencia Pública y de conformidad con el Anexo B del presente instrumento.

23. Los datos personales no pueden asociarse al titular de éstos, ni permitir por su estructura, contenido o grado de desagregación, la identificación individual del mismo, particularmente cuando estos datos requieran ser compartidos.

24. En caso de contratarse a un tercero para manejar la información del Sistema Persona, se debe firmar un convenio de confidencialidad, el cual debe especificar la obligatoriedad de conservar la confidencialidad de los mismos, la implementación de medidas de seguridad y custodia necesarios.

TRANSMISIÓN CON CONSENTIMIENTO DEL TITULAR

25. Sólo se podrán difundir datos personales generados o en posesión de Pronósticos para la Asistencia Pública, cuando así lo considere una disposición legal y/o cuando se tenga el consentimiento del titular de la información, el cual debe ser otorgado por escrito incluyendo firma autógrafa y la copia de identificación oficial a través de un medio de autentificación y, en su caso, cumplir con las disposiciones aplicables en materia de certificados digitales y/o firmas electrónicas.

26. Las áreas que realicen transmisiones totales o parciales de sistemas de datos personales deben notificar al INAI a través del "Sistema Persona" y a la Unidad de Enlace de Pronósticos para la Asistencia Pública, dentro de los diez primeros días hábiles de los meses de marzo y septiembre.

27. El informe debe contener al menos, lo siguiente:

- Identificación del Sistema de datos personales, del transmisor y del destinatario de los datos.
- Finalidad de la transmisión; así como el tipo de datos que son objeto de la transmisión.
- Las medidas de seguridad y custodia que adoptaron o fueron adoptadas por el transmisor y destinatario.
- Plazo por el que conservará el destinatario los datos que le hayan sido transmitidos, el cual podrá ser ampliado mediante aviso al INAI.
- Señalar si una vez concluidos los propósitos de la transmisión, los datos personales deberán ser destruidos o devueltos al transmisor, al igual que cualquier soporte o documento en que conste algún dato de carácter personal objeto de la transmisión.

DE LOS INFORMES OBLIGATORIOS

28. Cada área responsable de datos personales, debe realizar el registro de los mismos en el "Sistema Persona" o en el que el INAI hubiera dispuesto para este efecto, cumpliendo con los datos requeridos por el registro.

29. Las áreas responsables deben informar oportunamente a través del "Sistema Persona" al Comité de Información, las transmisiones totales o parciales de sistemas de datos personales que realicen.

DE LA SUPERVISIÓN

30. El Comité de Información puede supervisar lo referente al cumplimiento de la protección de datos personales y a la aplicación de las medidas de seguridad establecidas, sugiriendo en su caso, las acciones pertinentes a cada situación detectada, atendiendo en todo momento, las posibilidades de su aplicación.

31. Las áreas deben dar seguimiento y cumplimiento a las sugerencias e informarán de los avances obtenidos al Comité de Información.

32. Las áreas deben designar a un responsable de los sistemas de datos personales, el cual coordinará que cada persona que genere o maneje algún sistema de datos personales para el registro, reporte el control de los mismos, dentro de su área.

33. El Comité de Información debe coordinar y supervisar las acciones de seguridad, disponibilidad y exactitud de los datos, además de propiciar la capacitación del personal en la medida de las posibilidades.

34. Toda la documentación generada para la implementación y seguimiento de las medidas de seguridad debe ser información reservada y de acceso restringido.

DE LA SEGURIDAD DE LOS SISTEMAS DE DATOS PERSONALES

35. Las áreas deben tomar como guía y apoyo en materia de medidas de seguridad aplicables a los sistemas de datos personales tanto físicos como automatizados, las contenidas en las recomendaciones emitidas por el INAI.

36. Los sistemas de datos personales relacionados o derivados de las actividades de contratos, convenios y/o prestación de servicios estarán sujetos al menos a las medidas de seguridad establecidas en este documento.

37. Los titulares de las áreas correspondientes y los responsables de uno o más sistemas de datos personales, deben verificar la aplicación de las medidas de seguridad, a fin de realizar la evaluación, implementación y supervisión de ellas en sus áreas.

MEDIDAS DE SEGURIDAD

38. Cuando se deba crear un sistema de datos personales se debe designar al responsable del mismo y se le debe notificar al Comité de Información y al Titular de la Comisión de Servicios Logísticos y de Administración de Archivos, detallando al menos los siguientes aspectos:

    - Denominación del sistema de datos personales.
    - Objetivo del mismo.
    - Tiempo de vigencia.
    - Si se relacione con un convenio, contrato o servicio.
    - Área que lo crea.
    - Responsable del sistema.
    - Estructura de datos.
    - Áreas internas y/o personal autorizado para su manejo.
    - Tipo de soporte del archivo.
    - Área de resguardo.
    - Formato de recopilación de información.
    - Manejo externo.

39. Las áreas responsables de datos personales deben establecer una bitácora de registro y seguimiento de las actividades que se realicen con los sistemas de los datos personales.

40. La bitácora de registro debe tener hojas foliadas y rubricadas y contener al menos los siguientes puntos:

    - Ficha de identificación del sistema con denominación, área de resguardo responsable y objetivo.
    - Áreas internas y/o personal autorizado para su manejo.
    - Actividades realizadas con fechas desde el inicio hasta la conclusión de la vigencia.
    - Incidentes o intrusiones.
    - Actas.

41. Las áreas responsables que requieran mantener en custodia datos personales en la medida de las posibilidades, deben contar con un área privada o aislada para recabarlos y permitir su consulta, además de tener mecanismos para restringir el acceso a los sistemas resguardados.

42. La puerta de acceso del área de consulta tendrá que contar con cerradura.

43. En caso de existir ventanas o muros divisorios transparentes en el área de consulta, la visión obstruida mediante una película translúcida (por ejemplo, papel albanene).

44. El equipo de cómputo que se encuentre en el área de Sistema de Datos Personales debe estar provisto de la tecnología necesaria y suficiente para verificar la identidad del usuario que labora en el área de consulta. Ello implica que, mediante la verificación de claves de acceso, dicho personal accede al equipo a fin de realizar el tratamiento que corresponda al resguardo de datos personales.
45. El usuario que labora en el área de consulta debe ostentar una identificación con fotografía (credencial o gafete) emitido por Pronósticos para la Asistencia Pública.

46. No estará permitido el libre acceso y el uso del equipo de cómputo a cualquier persona dentro del área de consulta.

47. En las áreas de consulta debe existir señalización visible sobre: horarios de atención, restricciones de acceso, prohibiciones que aplican y el procedimiento para dar aviso al personal de vigilancia en caso de sospecharse la presencia de personas no autorizadas.

48. Las medidas de seguridad contenidas en el presente documento, deberán implementarse, por las áreas responsables de los Sistemas de Datos Personales.

49. Las áreas responsables, a través del Comité de Información, conjuntamente con la Subdirección General de Informática, expedirán en el ámbito de su competencia, un documento que contenga las medidas administrativas, físicas y técnicas de seguridad aplicables a los sistemas de datos personales, tomando en cuenta los Lineamientos de Protección de Datos Personales y las recomendaciones que en la materia emita el INAI.

50. El documento de seguridad que se emita deberá mantenerse siempre actualizado y será de observancia obligatoria para todos los servidores públicos de la Entidad, así como las personas externas que debido a la prestación de un servicio tengan acceso a los sistemas de datos personales y/o al sitio donde se ubican los mismos.

OBLIGACIONES DE LOS USUARIOS DE LOS SISTEMAS DE DATOS

51. Los asuntos no previstos en el presente documento, serán resueltos por el Comité de Información de Pronósticos para la Asistencia Pública conforme a las disposiciones legales correspondientes.

52. Los usuarios deben adoptar las medidas para el resguardo de los sistemas de datos personales, de manera que se evite su alteración, pérdida o acceso no autorizado.

53. Los usuarios no deben divulgar la información que se encuentre en los sistemas de datos personales.

54. Los usuarios deben notificar al responsable del sistema de datos personales los incidentes que se presenten.

55. Los usuarios deben de mantener la información de los sistemas de datos personales actualizada, contando con documentación que soporte los cambios realizados.

56. Los usuarios deben garantizar la integridad, confiabilidad, confidencialidad y disponibilidad de los sistemas de datos personales

V. CONTROL DE CAMBIOS

REVISIÓN	DESCRIPCIÓN DEL CAMBIO	FECHA
00	Incorporación al Sistema de Gestión de Calidad y de Seguridad de la Información.	Mayo, 2008
01	Actualización de responsables de revisar y autorizar el documento y cambio del tipo de documento de público a reservado.	Junio, 2010
02	Se actualizaron los responsables de firmar el documento y el Índice; se modificó el Objetivo, el Alcance del documento, el Fundamento Jurídico y se actualizó la versión de las normas. Se modificó la clave del documento “CTJ-CRI-02” por “SAJ-CRI-02”, así como las políticas 2, 3, 4, 5, 6, 7, 9, 10, 11, 13, 17,18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 35, 37, 38, 40, 45, 48. Se adicionaron las políticas 49 y 50. Se modificó y cambió la numeración de las políticas: 51 (actual 53), 52 (actual 54). Cambiaron de numeración las políticas 49 (actual 51), 50 (actual 52), 53 (actual 55) y 54 (actual 56). En el apartado de Glosario de términos se adicionó una leyenda para efectos de aplicación de los conceptos que lo integran; se modificó el Control de Cambios conforme a las actualizaciones realizadas.	Junio, 2016

VI. GLOSARIO

Además de las definiciones establecidas en los artículos 3 de la Ley Federal de Transparencia y Acceso a la información Pública Gubernamental, 2 de su Reglamento, y las referidas en los Lineamientos expedidos por el Instituto Federal de Acceso a la Información Pública (ahora Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales), para los efectos del presente instrumento se entenderá por:

COMITÉ DE INFORMACIÓN: El establecido en los artículos 29 y 30 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

DATOS PERSONALES: Cualquier información concerniente a una persona física identificada o identificable.

DESTINATARIO: Cualquier persona física o moral, pública o privada que recibe datos personales.

ENCARGADO: La persona física o moral, facultado por un Instrumento jurídico o expresamente autorizado por el responsable para llevar a cabo el tratamiento físico automatizado de los datos personales.

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

INFORMACIÓN: La contenida en los documentos que los sujetos obligados generen, obtengan, adquieran, transformen o conserven por cualquier título.

RESPONSABLE: El servidor público titular de la Unidad Administrativa designado por el titular de la Entidad, que decide sobre el tratamiento físico o automatizado de datos personales, así como el contenido y finalidad de los sistemas de datos personales.

SERVIDOR PÚBLICO: Los mencionados en el primer párrafo del artículo 108 Constitucional y todas aquéllas personas que manejen o apliquen recursos públicos federales.

SISTEMA PERSONA: Es la aplicación informática desarrollada por el INAI, para mantener actualizado el listado de los Sistemas de Datos Personales que posean las dependencias o entidades de la Administración Pública Federal; para registrar e informar sobre las transmisiones, modificaciones y cancelaciones de los mismos.

TITULAR DE LOS DATOS: Persona física a quien se refieren los datos personales que sea objeto de tratamiento.

TRANSMISIÓN: Toda entrega total o parcial de sistemas de datos personales realizada por Pronósticos para la Asistencia Pública 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 base de datos, acceso a redes de telecomunicación, así como a través de la utilización de cualquier otra tecnología que lo permita.

TRANSMISOR: Pronósticos para la Asistencia Pública, respecto de los datos personales objeto de la transmisión que posee.

TRATAMIENTO: Operaciones y procedimientos físicos o automatizados que permiten recabar, registrar, reproducir, conservar, organizar, modificar, transmitir y cancelar datos personales.

UNIDAD DE ENLACE: La Subdirección General de Asuntos Jurídicos de Pronósticos para la Asistencia Pública.

USUARIO: Servidor público facultado por un instrumento jurídico o expresamente autorizado por el responsable y que utiliza de manera cotidiana datos personales para el ejercicio de sus atribuciones, por lo que accede a los sistemas de datos personales, sin la posibilidad de agregar o modificar su contenido.

VII. ANEXOS

ANEXO A

PRONÓSTICOS PARA LA ASISTENCIA PÚBLICA

Formato de Protección de Datos Personales

Los datos personales recabados serán protegidos y serán incorporados y tratados en el Sistema de datos personales **(indicar nombre[1])**, con fundamento en **(indicar[2])** y cuya finalidad es **(describirla[3]),** el cual fue registrado en el Listado de sistemas de datos personales ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales y podrán ser transmitidos a **(indicar[4])**, con la finalidad de **(indicar[5])**, además de otras transmisiones previstas en la Ley. La Unidad Administrativa responsable del Sistema de datos personales es **(indicarlo[6])**, y la dirección donde el interesado podrá ejercer los derechos de acceso y corrección ante la misma es **(indicarla[7])**. Lo anterior se informa en cumplimiento del Decimoséptimo de los Lineamientos de Protección de Datos Personales, publicados en el Diario Oficial de la Federación **(incluir fecha[8])**

ATTE:

Nombre y Firma del Responsable

[1] Indicar el nombre del sistema de datos personales.
[2] Indicar el fundamento legal que faculta a la dependencia o entidad para recabar los datos personales en el sistema de datos personales.
[3] Describir la finalidad del sistema de datos personales.
[4] Indicar las personas u organismos a los que podrán transmitirse los datos personales contenidos en el sistema de datos personales.
[5] Describir la finalidad de la transmisión.
[6] Indicar el nombre de la unidad administrativa responsable del sistema de datos personales.
[7] Indicar el nombre de la unidad de enlace responsable del sistema de datos personales.
[8] Anotar la fecha de publicación en el Diario Oficial de la Federación de los presentes Lineamientos.

ANEXO B

TABLA PARA LA DETERMINACIÓN DE LOS NIVELES DE SEGURIDAD APLICABLE

Nivel de seguridad aplicable	Tipo de datos contenidos en el Sistema de Datos Personales
Nivel básico: Las medidas de seguridad aplicables a todos los sistemas de datos personales.	**1. De Identificación:** Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, firma electrónica, Registro Federal de Contribuyentes, Clave Única del Registro de Población, cartilla militar, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares dependientes y beneficiarios, fotografía, costumbres, idioma o lengua, entre otros. **2. 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, referencias personales, entre otros.
Nivel medio: Medidas adicionales a las de nivel básico.	**1. Datos Patrimoniales**: Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados, referencias personales, entre otros. **2. 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. **3. Datos Académicos:** Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros. **4. Tránsito y movimientos migratorios:** Información relativa al tránsito de las personas dentro y fuera del país e información migratoria de las personas, entre otros.
Nivel alto: Medidas adicionales a las de nivel básico y medio.	**1. Datos Ideológicos*:*** Creencia religiosa, ideología, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y/o asociaciones religiosas, entre otros. **2. Datos de Salud:** Estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos, prótesis, entre otros. **3. Características personales:** Tipo de sangre, huella digital, u otros análogos. **4. Características físicas:** Color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros. **5**. **Vida sexual:** Preferencia sexual, hábitos sexuales, entre otros. **6. Origen:** Étnico y racial.