ECONOMÍA
SECRETARÍA DE ECONOMÍA

IMPI
INSTITUTO MEXICANO DE LA PROPIEDAD INDUSTRIAL

DOCUMENTO DE SEGURIDAD

DEL INSTITUTO MEXICANO DE LA PROPIEDAD INDUSTRIAL

COMITÉ DE TRANSPARENCIA

ECONOMÍA
SECRETARÍA DE ECONOMÍA

IMPI
INSTITUTO MEXICANO DE LA PROPIEDAD INDUSTRIAL

IMPI
INSTITUTO MEXICANO
DE LA PROPIEDAD
INDUSTRIAL

DOCUMENTO DE SEGURIDAD

DEL INSTITUTO MEXICANO DE LA PROPIEDAD INDUSTRIAL

COMITÉ DE TRANSPARENCIA

CONTENIDO

1. Introducción.
2. Glosario.
3. Marco Normativo.
4. Ámbito de aplicación.
5. Inventario de Datos Personales y de los Sistemas de Tratamiento.
6. Medidas de Seguridad
7. Análisis de riesgos
8. Análisis de brecha.
9. Plan de Trabajo.
10. Mecanismos de Monitoreo y Revisión de las Medidas de Seguridad.
11. Programa General de Capacitación.

1. INTRODUCCIÓN

El derecho de acceso y rectificación de datos personales para el sector público federal encuentra su antecedente en la Ley Federal de Transparencia y Acceso a la Información, con publicación en el año 2002.

Conforme a las reformas a los artículos 6 y 16 de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia, acceso a la información y protección de datos personales, efectuadas en 2009 y 2014 se propició la emisión de normatividad tendiente a garantizar el ejercicio del derecho humano.

Así con la reforma al artículo 16 constitucional, toda persona tiene derecho a la protección de sus datos personales, a través del ejercicio de derechos ARCO, (Acceso, Rectificación, Cancelación y Oposición) al uso de su información personal. No obstante no fue sino hasta la reforma del artículo 6° Constitucional en el año 2014, cuando se fijaron las bases para la emisión de una Ley de carácter General para la información en posesión de entes públicos.

Sin embargo no fue sino hasta, el 26 de enero de 2017 cuando se expidió la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), con el objeto de establecer las bases, principios y procedimientos para garantizar el derecho que tienen toda persona física a la protección de sus datos personales en posesión de los tres órdenes de gobierno, con lo cual , se definen las bases mínimas y condiciones homogéneas que regirán el tratamiento de los datos personales y el ejercicio de los derechos de acceso, rectificación, cancelación y oposición (Derechos ARCO) mediante procedimientos sencillos y expeditos.

En enero 26 de 2018, se publicaron los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales de Protección de Datos Personales), en los que se desarrollan y concentran las obligaciones exigibles del derecho a la protección de datos personales en el sector público federal, para evitar la fragmentación o atomización de ordenamientos que puedan repercutir en el cumplimiento efectivo de la LGPDPPSO por parte de los responsables en el ámbito federal.

A partir de la publicación de la LGPDPPSO y de los lineamientos Generales de Protección de Datos Personales, todas las dependencias y entidades -incluidos partidos políticos-, al llevar a cabo el tratamiento de los datos personales de personas físicas, adquieren el carácter de "Responsable" y deberán tratar dichos datos conforme a los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad; adoptar medidas de seguridad en atención a los sistemas de datos que traten; plasmar en un documento de seguridad dichas

medidas, garantizar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, entre otras obligaciones previstas.

Ahora bien, en atención a dichas disposiciones el **Instituto Mexicano de la Propiedad Industrial (IMPI)** es una autoridad administrativa en materia de propiedad industrial, organismo descentralizado, con personalidad jurídica y patrimonio propio, el cual tiene entre las facultades previstas, en el artículo 6° fracciones III, IV y V de la Ley de la Propiedad Industrial, tramitar y, en su caso, otorgar patentes de invención, y registros de modelos de utilidad, diseños industriales, esquemas de trazado de circuitos integrados, marcas y avisos comerciales, emitir declaratorias de notoriedad o fama de marcas, emitir declaraciones de protección a denominaciones de origen e indicaciones geográficas, autorizar el uso de las mismas; la publicación de nombres comerciales, así como la inscripción de sus renovaciones, transmisiones o licencias de uso y explotación, y las demás que le otorga esta Ley y su reglamento, para el reconocimiento y conservación de los derechos de propiedad industrial.

Así como sustanciar los procedimientos de nulidad, caducidad y cancelación de los derechos de propiedad industrial, formular las resoluciones y emitir las declaraciones administrativas correspondientes, conforme lo dispone esta Ley y su reglamento y, en general, resolver las solicitudes que se susciten con motivo de la aplicación de la misma; realizar las investigaciones de presuntas infracciones administrativas; ordenar y practicar visitas de inspección; requerir información y datos; ordenar y ejecutar las medidas provisionales para prevenir o hacer cesar la violación a los derechos de propiedad industrial; oír en su defensa a los presuntos infractores, e imponer las sanciones administrativas correspondientes en materia de propiedad industrial; **es un sujeto obligado en materia de protección de datos personales y por ende responsable del tratamiento de los datos personales que trata para el ejercicio de sus atribuciones.**

Así, entre los "Deberes" previstos en la LGPDPPSO, está el de elaborar un documento de seguridad (artículo 35) en el cual se describa y de cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que poseen las distintas unidades administrativas de la entidad. La elaboración de este documento fue coordinada por la Unidad de Transparencia del Instituto Mexicano de la Propiedad Industrial.

A su vez, el Comité de Transparencia es quien tiene entre sus funciones, la de coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la del responsable, de conformidad con las disposiciones previstas en la LGPDPPSO y demás disposiciones que resulten aplicables al ser la autoridad máxima en materia de protección de datos personales.
Para la elaboración del Documento de Seguridad se llevaron a cabo las siguientes actividades:

- Análisis de la normatividad, para identificar los requisitos mínimos que deberán contenerse en el documento en cuestión.

- Se desarrolló como metodología la implementación de formato a razón de homologar la información requerida.

- Se esquematizaron a través de formatos los requisitos mínimos que debe contener el mismo de conformidad con la normatividad aplicable.

- Se realizó una guía para el llenado de cada uno de los formatos estructurados.

- Se realizaron reuniones de trabajo con las 10 unidades administrativas que conforman la estructura del IMPI, incluida la Dirección Divisional de Sistemas y Tecnología de la Información a efecto de recopilar información homologada

Una vez determinados los datos y las fechas de los entregables se llevó a cabo la verificación de los mismos a efecto de que cumplieran con los siguientes:

- Los sistemas de tratamiento de datos con que cuentan, su objetivo y el fundamento normativo para llevar a cabo dicho tratamiento.

- La descripción e identificación de la estructura de los sistemas de tratamientos datos personales, en la cual se incluyen los datos personales que contienen los sistemas de tratamiento y su idoneidad, la manera en que se obtienen, el administrador del sistema, sus operadores, usuarios, el tipo de soporte en que se encuentran, las características del lugar en que se localizan, si es posible su portabilidad, si existe transferencia y si hay encargados.

A la fecha se cuenta con la elaboración del presente documento, no obstante deberá ajustarse y seguirse trabajando como parte de un programa de datos personales, en materia de vulnerabilidades y análisis de riesgo.

2. GLOSARIO

Para efectos del presente Documento de Seguridad, se entenderá por:

1). **Áreas:** Instancias de los sujetos obligados previstas en los respectivos reglamentos interiores, estatutos orgánicos o instrumentos equivalentes, que cuentan o puedan contar, dar tratamiento, y ser responsables o encargadas de los datos personales;

2). **Aviso de privacidad:** Documento a disposición del titular de forma física, electrónica o en cualquier formato generado por el responsable, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos;

3). **Bases de datos:** Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización;

4). **Bloqueo:** La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponda;

5). **Comité de Transparencia:** Instancia a la que hace referencia el artículo 43 de la Ley General de Transparencia y Acceso a la Información Pública;

6). **Cómputo en la nube:** Modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente;

7). **Consejo Nacional:** Consejo Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales a que se refiere el artículo 32 de la Ley General de Transparencia y Acceso a la Información Pública;

8). **Consentimiento:** Manifestación de la voluntad libre, específica e informada del titular de los datos mediante la cual se efectúa el tratamiento de los mismos;

9). **Datos personales:** Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información;

10). **Datos personales sensibles:** Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual;

11). **Derechos ARCO:** Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales;

12). **Días:** Días hábiles;

13). **Disociación:** El procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo;

14). **Documento de seguridad:** Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee;

15). **Encargado:** La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable.

16). **Evaluación de impacto en la protección de datos personales:** Documento mediante el cual los sujetos obligados que pretendan poner en operación o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales, valoran los impactos reales respecto de determinado tratamiento de datos personales, a efecto de identificar y mitigar posibles riesgos relacionados con los principios, deberes y derechos de los titulares, así como los deberes de los responsables y encargados, previstos en la normativa aplicable;

17). **Fuentes de acceso público:** Aquellas bases de datos, sistemas o archivos que por disposición de ley puedan ser consultadas públicamente cuando no exista impedimento por una norma limitativa y sin más exigencia que, en su caso, el pago de una contraprestación, tarifa o contribución. No se considerará fuente de acceso público cuando la información contenida en la misma sea obtenida o tenga una procedencia ilícita, conforme a las disposiciones establecidas por la presente Ley y demás normativa aplicable;

18). **Instituto:** Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, el cual es el organismo garante de la Federación en materia de protección de datos personales en posesión de los sujetos obligados;

19). **Medidas compensatorias:** Mecanismos alternos para dar a conocer a los titulares el aviso de privacidad, a través de su difusión por medios masivos de comunicación u otros de amplio alcance;

20). **Medidas de seguridad:** Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales;

21). **Medidas de seguridad administrativas:** Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales;

22). **Medidas de seguridad físicas:** Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

a) Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;

b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;

c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y

d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad;

23). Medidas de seguridad técnicas: Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

a) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;

b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;

c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y

d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales;

24). Organismos garantes: Aquellos con autonomía constitucional especializados en materia de acceso a la información y protección de datos personales, en términos de los artículos 6o. y 116, fracción VIII de la Constitución Política de los Estados Unidos Mexicanos;

25). Plataforma Nacional: La Plataforma Nacional de Transparencia a que hace referencia el artículo 49 de la Ley General de Transparencia y Acceso a la Información Pública;

26). Programa Nacional de Protección de Datos Personales: Programa Nacional de Protección de Datos Personales;

27). **Remisión:** Toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado, dentro o fuera del territorio mexicano;

28). **Responsable:** Los sujetos obligados a que se refiere el artículo 1 de la presente Ley que deciden sobre el tratamiento de datos personales;

29). **Sistema Nacional:** El Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales;

30). **Supresión:** La baja archivística de los datos personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el responsable;

31). **Titular:** La persona física a quien corresponden los datos personales;

32). **Transferencia:** Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado;

33). **Tratamiento:** Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales, y

34). **Unidad de Transparencia:** Instancia a la que hace referencia el artículo 45 de la Ley General de Transparencia y Acceso a la Información Pública.

3. MARCO NORMATIVO

Para efectos del presente documento, la normatividad aplicable es la siguiente:

Constitución Política de los Estados Unidos Mexicanos.

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada en el Diario Oficial de la Federación el 26 de enero de 2017.

Lineamientos generales de protección de datos personales para el sector público, publicados en el Diario Oficial de la Federación el 26 de enero de 2018.

Lineamientos que establecen los parámetros, modalidades y procedimiento para la portabilidad de datos personales, publicados en el Diario Oficial de la Federación el12 de febrero de 2018

Ley Orgánica de la Administración Pública Federal, cuya última reforma fue publicada en el Diario Oficial de la Federación el 24 de abril de 2018.

Acuerdo rediente el cual se aprueban las disposiciones administrativas de carácter general para la elaboración, presentación y valoración de impacto en la protección de datos personales.

Ley de la Propiedad Industrial Diario Oficial de la Federación 27 junio 1991

Reglamento de la Ley de la Ley de la Propiedad Industrial 23 de noviembre de 1994

Estatuto Orgánico Última reforma publicada DOF: 02-01-2018

4. ÁMBITO DE APLICACIÓN

Conforme a los Deberes referidos en la LGPDPPSO, el presente documento es de aplicación para todas las unidades administrativas del IMPI, que en el ejercicio de sus atribuciones y funciones, administren bases de datos en sistemas de tratamiento de datos personales, ya sea de manera total o parcial en el tramo de la información que les corresponda.

De igual forma será aplicable al tratamiento de datos personales que obren en soportes físicos y/o electrónicos, con independencia de la forma o modalidad de su creación, procesamiento, almacenamiento y organización. Se reconoce el hecho de que los datos personales podrán ser expresados en forma numérica, alfabética, gráfica, alfanumérica, fotográfica, acústica, o en cualquier otro formato.

Todos los servidores públicos que tengan acceso a los datos personales, están obligados a conocer, aplicar las medidas de seguridad propias de cada Sistema en el que se concentren los datos en todas y cada una de las fases del tratamiento de los mismos, conforme al rol o perfil que desempeñan, iniciando desde la obtención de los datos personales y finalizando con su eliminación.

A efecto de poder hacer más accesible la distinción de los diferentes roles que se tienen al interior del IMPI, se llegó a la siguiente categorización:

Funciones genérica en cualquier nivel de tratamiento

Tratar los datos personales con responsabilidad y con las medidas de seguridad que se haya establecido para tal fin.

Obligaciones genéricas en cualquier nivel de tratamiento

Guardar confidencialidad sobre la información que conozcan en el desarrollo de sus actividades.

Estar capacitado en materia de tratamiento de datos personales.

Dar aviso a los superiores jerárquicos, ante cualquier acción que pueda poner en riesgo los datos personales, y en general que puedan vulnerar la seguridad de los datos personales

De manera particular y de conformidad con los cargos, encargos y/o designaciones de los servidores público, se define cuatro roles básico en el tratamiento de los datos personales con las siguientes funciones

Responsable del Sistema: Titular de la Unidad Administrativa donde se administre el Sistema de que se trate, quien deberá:

Dar aviso a la Unidad de Transparencia de los Sistemas que involucren tratamiento de datos personales, a cargo de dicha Unidad Administrativa.
Designar al Administrador del Sistema.
Validar que la información entregada por los titulares de los datos personales, sea la estrictamente necesaria para cumplir con los fines legales para los cuales se hubieran recabado.

Administrador del Sistema: Será el servidor público a quien designe de manera expresa el Titular de la Unidad Administrativa. Tiene a su cargo la responsabilidad de la administración del sistema y de los operadores, quien deberá:

Mantener actualizado el Sistema
Determinar los servidores públicos que deben tener acceso a los datos personales, en función del tratamiento que debe aplicarse a los mismos.
Autorizar los accesos de los servidores públicos, determinar los privilegios y limitantes y llevar un registro de los mismos.
Implementar las medidas de seguridad con la finalidad de evitar vulneraciones de la información.

Operador (personal operativo)
Sus funciones quedan determinadas de acuerdo al perfil quese haya asignado en el tratamiento de los datos personales de cada uno de los sistemas.

Enlace de datos personales
Conocer del Inventario de Sistemas· que involucren tratamiento de datos personales y por cada uno. Conocer el tipo de datos personales que se recaban y el nombre del Encargado por cada Sistema,
Dar seguimiento a las acciones de capacitación para los servidores públicos involucrados en el tratamiento de los datos personales.
Atender a los requerimientos de información que solicite la Dirección Divisional de Sistemas y Tecnologías de la Información

En caso de existir figura de "Encargado", en la formalización de la prestación del servicio que implique la transferencia de datos para su tratamiento, deberá atenderse a lo previsto en el Artículo 59 de la LGPDPPSO y los artículos correspondientes de los Lineamientos Generales de Protección de Datos Personales, que se refieren a la existencia de algún instrumento jurídico que incluya cláusulas sobre el tratamiento de datos personales conforme a las instrucciones del responsable, que prevean que los datos no se tratarán para finalidades distintas a las previstas, que establezcan que se implementarán medidas de seguridad, que se informará al responsable en caso de vulneración, que se guardará confidencialidad respecto de los datos personales, que éstos se suprimirán o devolverán al concluir la relación jurídica en atención a las normas jurídicas sobre su conservación y que se abstendrán de transferirlos salvo determinación del responsable en atención a la normatividad y al aviso de privacidad correspondiente.

5. INVENTARIO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO.

Como fue mencionado anteriormente se desarrollaron actividades dentro de las cuales se consideró a fin de dar cumplimiento, generar metodologías para homologar la información, mediante el uso de formatos para ser requisitados por las unidades administrativas competentes de esta entidad.

Resultado de ello fue la descripción mediante un formato por secciones donde se señaló puntualmente la información que se debía documentar, siendo este el que sigue:

0. NÚMERO Y NOMBRE DEL ÁREA O UNIDAD ADMINISTRATIVA	**0** Indicar el número de clave del área (Ejemplo: 200 Dirección Divisional de Patentes, 300 Dirección Divisional de Marcas, etc)
1. Nombre del Sistema	**1** Indicar el nombre del Sistema de Datos Personales (Ejemplo: Marcanet, SAGPAT, Vidoc, Expedientes de Personal, Sistema de Viáticos, Expediente Servicio Social etc.)
2. Objetivo	**2** Indicar cuales son las finalidades concretas, licitas, explicitas y legítimas, relacionada con las atribuciones normativas conferidas, por las que recaba los datos.
3. Fundamento Legal	**3** Indicar el fundamento legal que faculta al responsable para llevar a cabo el tratamiento, indicando los artículos, apartados, fracciones, incisos y nombre de los ordenamientos o disposición normativa vigente que le confiere atribuciones para realizar el tratamiento de datos personales, precisando su fecha de publicación o, en su caso, de la última reforma o modificación.
4. DATOS PERSONALES QUE CONTIENE EL SISTEMA	**4** Indicar todos los datos personales que son solicitados y que se contienen en la base de datos del sistema y su idoneidad

5. FORMA DE OBTENCIÓN DE LOS DATOS PERSONALES **Directa** Formulario físico Formulario electrónico Texto físico Texto electrónico Vía telefónica Otro **Indirecta** (obtenida, creada, generada en algún otro sistema) **Descripción**	**5** Indicar la forma en que se obtienen los datos personales que obran en el sistema o bien si estos provienen de otro sistema
7. Administrador del Sistema Nombre Cargo Teléfono Correo electrónico Función Obligación	Se entiende como Administrador al servidor público quien tiene a su cargo la responsabilidad de la administración del sistema y de los operadores del mismo
8. Usuarios u Operador del Sistema Nombre Cargo Teléfono Correo electrónico Función Obligación	**8** Se entiende como Usuario u Operador del sistema a quienes hagan uso del sistema conforme al perfil delimitado, para el cumplimiento de funciones asignadas al puesto
9. Tipo de soporte Electrónico Físico Ambos Descipción	**9** Indicar el tipo de medio de almacenamiento en que residen los datos personales a custodia: **Soportes físicos.** Son los 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, documentos, oficios, formularios impresos llenados “a mano” o “a máquina”, fotografías, placas radiológicas, carpetas, expedientes, entre otros. **Soportes electrónicos.** Son los 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 microfilm, discos ópticos (CDs y DVDs), discos magneto-ópticos, discos magnéticos (flexibles y duros) y demás medios de almacenamiento masivo no volátil.
10. Transferencias o transmisiones de datos personales *SI *No *Describir en que consiste la transferencia o transmisión	**10** Entiéndase como la comunicación de datos o entrega total o parcial de los mismos, a cualquier persona distinta a su titular, sea mediante el uso de medios físicos o electrónicos, tales como la interconexión de computadoras o bases de datos, acceso a redes de telecomunicación, así como a través de la utilización de cualquier otra tecnología que lo permita. En el ámbito de la Administración Pública Federal se tienen: a) **Interinstitucionales:** Transmisiones de datos a dependencias y entidades de la APF, entidades federativas y municipios; b) **Internacionales:** Transmisiones a gobiernos u organismos internacionales, y c) **Con entes privados u organizaciones civiles públicas o privadas**
11. Portabilidad de datos *SI *No	**11** Indicar si las características del sistema permiten apreciar un sistema de datos personales estructurado comúnmente utilizado
12. Nivel de protección que requieren los datos	**12** Indicar el nivel aplicable, el cual estará determinado en base a los datos en posesión, siguiendo los criterios internacionales de seguridad para el resguardo eficaz de los mismos. Los niveles de seguridad responden a la mayor o menor necesidad de garantizar la integridad de los datos personales, en base a lo que se detalla a continuación: **A. Nivel básico** : De Identificación: Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, firma electrónica, RFC, CURP, cartilla militar, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares dependientes y beneficiarios, fotografía, costumbres, idioma o lengua, entre otros. 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.

	B. Nivel medio: Datos Patrimoniales: Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados, referencias personales, entre otros. Datos sobre procedimientos administrativos relativos a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio en materia laboral, civil, penal o administrativa. Datos Académicos: Títulos, cédula profesional, certificados y reconocimientos, entre otros. Tránsito y movimientos migratorios: Información relativa al tránsito de las personas dentro y fuera del país e información migratoria de las personas, entre otros. **C. Nivel alto**: **Datos Ideológicos**: Creencia religiosa, ideología, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y/o asociaciones religiosas, entre otros. **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. **Características personales**: Tipo de sangre, ADN, huella digital, u otros análogos. **Características físicas**: Color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros. **Vida sexual**: Preferencia sexual, hábitos sexuales, entre otros. **Origen**: Étnico y racial
13. Actualización de la información contenida en el sistema	**13** Indicar la frecuencia con que se actualiza la información directamente en la base de datos del sistema (diaria, bimestral, anual…)
14. Plazo de conservación de los datos personales	**14** Indicar cuanto tiempo permanecerán los datos personales en el Sistema de Datos conforme a su vigencia y finalidad, es decir atendiendo al ciclo de vida del trámite o servicio por motivo del cual se obtuvieron
15. Medidas de Seguridad	**15** Indicar los elementos de seguridad con que se cuenta y se abordan en tres modalidades tomando como base el estándar internacional ISO/IEC 27002:2005 que se refiere a mejores prácticas sobre seguridad de la información: **Seguridad física**: son el conjunto de acciones y

	mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento (Ejemplo: elementos de seguridad, portación de credencial institucional, acceso perimetral a instalaciones, identificación de equipos de móviles y portátiles; mobiliario, documentos y materiales mediante controles de entrada y salida entre otros) **Seguridad administrativa**: se traducen en políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación, ciclo de vida de los datos en posesión, en función de la finalidad para la que fueron recabados. • **Política de seguridad.** Definición de directrices estratégicas en materia de seguridad de activos, alineadas a las atribuciones de las dependencias o entidades. Incluye la elaboración y emisión interna de políticas, entre otros documentos regulatorios del sujeto obligado. • **Cumplimiento de la normatividad.** Los controles establecidos para evitar violaciones de la normatividad vigente, obligaciones contractuales o la política de seguridad interna. Abarca, entre otros, la identificación y el cumplimiento de requerimientos tales como la legislación aplicable al sujeto obligado, los derechos de propiedad intelectual, la protección de datos personales y la privacidad de la información personal. • **Organización de la seguridad de la información.** Establecimiento de controles internos y externos a través de

	los cuales se gestione la seguridad de activos. Considera, entre otros aspectos, la organización interna, que a su vez se refiere al compromiso de la alta dirección y la designación de responsables, entre otros objetivos; asimismo, considera aspectos externos como la identificación de riesgos relacionados con terceros. • **Clasificación y control de activos.** Establecimiento de controles en materia de identificación, inventario, clasificación y valuación de activos conforme a la normatividad aplicable. • **Seguridad relacionada a los recursos humanos.** Controles orientados a que el personal conozca el alcance de sus responsabilidades respecto a la seguridad de activos, antes, durante y al finalizar la relación laboral. • **Administración de incidentes.** Implementación de controles enfocados a la gestión de incidentes presentes y futuros que puedan afectar la integridad, confidencialidad y disponibilidad de la información. Incluye temas como el reporte de eventos y debilidades de seguridad de la información. • **Continuidad de las operaciones.** Establecimiento de medidas con el fin de contrarrestar las interrupciones graves de la operación y fallas mayores en los sistemas de información. Incluye planeación, implementación, prueba y mejora del plan de continuidad de la

	operación del sujeto obligado. **Seguridad técnica**: son las aplicables a sistemas de datos personales en soportes electrónicos, servicios e infraestructura de telecomunicaciones y tecnologías de la información, entre otras, se prevén las siguientes acciones: • **Gestión de comunicaciones y operaciones**. Establecimiento de controles orientados a definir la operación correcta y segura de los medios de procesamiento de información, tanto para la gestión interna como la que se lleva a cabo con terceros. Incluye, entre otros aspectos, protección contra código malicioso y móvil, copias de seguridad, gestión de la seguridad de redes y manejo de medios de almacenamiento. • **Control de acceso**. Establecimiento de medidas para controlar el acceso a la información, activos e instalaciones por parte de los responsables autorizados para tal fin, considerando en ello, la protección contra la divulgación no autorizada de información. Abarca, entre otros temas, gestión de acceso de los usuarios, control de acceso a redes, control de acceso a sistemas operativos y control de acceso a las aplicaciones y a la información. • **Adquisición, desarrollo, uso y mantenimiento de sistemas de información**: Integración de controles de seguridad a los sistemas de información, desde su adquisición o desarrollo, durante su uso y mantenimiento, hasta su cancelación o baja definitiva. Considera procesamiento adecuado en las aplicaciones, controles criptográficos y seguridad de los archivos de sistema, entre otros.
16. Acceso a instalaciones	**16** Indicar los elementos que se advierten en el sujeto obligado respecto a: 1. **Seguridad perimetral exterior** (las instalaciones del sujeto obligado): ¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones?24

	Para las personas que acceden a sus instalaciones: a) ¿Cómo las identifica? b) ¿Cómo las autentifica? c) ¿Cómo les autoriza el acceso? 2. **Seguridad perimetral interior** (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos): *¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema?25* *Para las personas que acceden a dichos espacios interiores:* *a) ¿Cómo las identifica?* *b) ¿Cómo las autentifica?* *c) ¿Cómo les autoriza el acceso?* Por ejemplo, se espera que precise el tipo de puertas y cerraduras instaladas, si tiene instalados controles biométricos, si administra la asignación de llaves y/o claves de acceso para abrir puertas y/o estantería, si cuenta con vigilancia las 24 horas, si hay un sistema de vídeo-vigilancia, entre otras medidas.
17. Perfiles de usuario y contraseña	**17** Indicar en este rubro el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica. 1. Modelo de control de acceso [alguno de los siguientes]: a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)? b) ¿Es discrecional (matriz de control de acceso)? c) ¿Está basado en roles (perfiles) o grupos? d) ¿Está basado en reglas? 2. Perfiles de usuario y contraseñas en el

	sistema operativo de red: a) ¿Cuenta con un sistema operativo de red instalado en sus equipos? b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas? c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? 3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de datos personales: a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas? b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? 4. Administración de perfiles de usuario y contraseñas: a) ¿Quién da de alta nuevos perfiles? b) ¿Quién autoriza la creación de nuevos perfiles? c) ¿Se lleva registro de la creación de nuevos perfiles? 5. Acceso remoto al sistema de datos personales: a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema? b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento? c) ¿Cómo se evita el acceso remoto no autorizado?
18. Bitácoras de acceso y operación cotidiana, seguridad aplicable Soporte físico Soporte electrónico	**Ejemplo de medidas de seguridad aplicables a bitácoras para sistemas en soportes físicos:** El Responsable del sistema procura un estricto control y registro de: 1. Las autorizaciones emitidas para facultar el acceso a un servidor público a fin de que éste, en el ejercicio de sus funciones, pueda interactuar con uno o más de los sistemas a su cargo. 2. La asignación, actualización y reemplazo de las llaves que entrega a los autorizados para que éstos puedan abrir el mecanismo de apertura de la puerta en la zona de acceso

	restringido. 3. Las acciones que los autorizados llevan a cabo en el área de resguardo. Para ello, designa a un Encargado quien anota lo siguiente: Quién solicita el acceso, cuándo se lleva a cabo (fecha y hora de entrada y salida), la razón que lo motiva y número del expediente utilizado. 4. El préstamo de expedientes es asistido por un sistema de cómputo que utiliza códigos de barras en los gafetes del personal autorizado y en los expedientes. 5. El sistema de préstamo de expedientes genera una bitácora electrónica que se respalda diariamente en un servidor dentro del centro de cómputo que administra el área de informática. Su integridad se garantiza copiando dicha bitácora en un CD-R diariamente. 6. El Encargado del sistema es la persona designada para analizar la bitácora cada mes mediante una herramienta adquirida para tal fin. **Ejemplo de medidas de seguridad aplicables a bitácoras para sistemas en soportes electrónicos**: 1. El Responsable del sistema -en coordinación con las áreas de informática y seguridad de la información- lleva un estricto control y registro de: a) Las bitácoras de eventos ocurridos a nivel sistema operativo en los equipos (servidores, cortafuegos, almacenamiento masivo) que habilitan la operación del sistema de datos personales. Entre otras, se generan bitácoras para desempeño del servidor: intentos de acceso (exitosos y fallidos); accesos denegados a usuarios y terminales; uso de herramientas para administración del servidor, y fecha y hora de los eventos anteriores. b) Las bitácoras de eventos generados a nivel software aplicativo del sistema de datos personales. Entre otras, se generan bitácoras para mensajes de error; apertura, modificación y cierre de archivos; violaciones de seguridad detectadas por el software aplicativo, y fecha y hora de estos eventos. c) Las bitácoras de eventos relativos a las actividades de usuarios (capturistas, Encargados, el propio Responsable y el administrador del servidor) en su interacción con el sistema de datos personales. Entre otras,

	se generan bitácoras para: Archivos, servicios y recursos utilizados; intentos de acceso (exitosos y fallidos); comandos y operaciones iniciadas, y fecha y hora de dichos eventos. d) El conjunto de bitácoras permiten registrar, entre otros, los siguientes datos: Quién accede a los datos personales, desde dónde y con qué; accesos (intentos exitosos y fallidos) y salidas; propósito del acceso (sólo para modificaciones en el software aplicativo); operaciones llevadas a cabo; datos personales (registros y campos) utilizados de la base de datos, y fecha y hora de estos eventos. e) Las bitácoras arriba mencionadas están todas en soportes electrónicos y se almacenan al menos por dos años en CD-R. Se tiene una copia en el centro de datos y otra se lleva a una bóveda bancaria subcontratada también para los respaldos.
19. Lugar de almacenamiento de las bitácoras y tiempo de conservación y conservación de integridad	**19** Indicar lugar donde reside la bitácora sea físico o electrónico y como se mantiene la integridad de las bitácoras Ejemplo a) Se garantiza copiándolas en un servidor del centro de datos el cual las graba en CD-R. b) Algunas se copian cada hora, otras a diario. c) La integridad de las copias se garantiza además con "resúmenes" creados por un algoritmo "digestor". d) Se cuenta con una herramienta de software que automatiza estas operaciones. Deberá especificarse si las áreas de informática y seguridad de la información han designado una persona que se encarga de realizar un análisis de las bitácoras generadas como puede ser: a) Se cuenta con la ayuda de una herramienta informática adquirida para tal propósito. b) Cada semana se llevan a cabo análisis de bitácoras pero no de todas ellas. Depende de la bitácora y de las amenazas detectadas en el entorno.
20. Registro de incidentes	especificar si lleva registro de los incidentes relativos a soportes físicos, como lo son la pérdida o alteración no autorizada de expedientes, y para el caso de soportes electrónicos, ofrecer detalles sobre el registro de incidentes en el cual consigne los procedimientos realizados para la recuperación

	de los datos o para permitir la disponibilidad del proceso 1. Los datos que deberá registrar son: a) La persona que resolvió el incidente; b) La metodología aplicada; c) Para soportes físicos: Los oficios, documentos, expedientes, estantes o archiveros, tanto los dañados como los recuperados, y d) Para soportes electrónicos: Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados. 2. Si el registro está en soporte físico o en soporte electrónico; 3. Cómo asegura la integridad de dicho registro, y 4. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos. **Ejemplo de procedimiento en caso de presentarse un incidente**: a) El Encargado elabora y entrega un informe al Responsable a más tardar al día siguiente de haber ocurrido el incidente. Dicho informe precisa los soportes físicos o electrónicos afectados y, en su caso, los recuperados. b) El incidente se registra en una hoja de cálculo anotando quién resolvió el incidente y los soportes dañados y recuperados. Dicha hoja está protegida con una contraseña de acceso. Su integridad se garantiza generando y almacenando un resumen creado por un algoritmo digestor en un servidor del centro de datos y respaldándola en un CD-R después de registrar un incidente. c) En caso de robo o extravío de datos personales, el Responsable del sistema, al tener conocimiento del incidente, da vista al titular de la dependencia o entidad para su conocimiento y al titular del área jurídica o aquél que tenga facultades para presentar denuncias o querellas ante el Ministerio Público para que en el ámbito de sus atribuciones, determine lo conducente d) A no más de 3 días naturales de haber ocurrido el incidente, el Responsable del sistema da aviso al público mediante un desplegado de prensa que difunde el hecho por diversos medios, según la gravedad del caso, a escala local, regional o nacional. e) En caso de robo o extravío de datos personales, se alerta a los titulares de los datos

	afectados para que tomen sus precauciones ante el posible uso ilegal de su información. Para tal efecto, el Responsable del sistema da aviso por escrito a dichos titulares, a más tardar cinco días naturales de haber ocurrido el incidente, recabando el acuse de recibo de esta notificación. Adicionalmente, se da aviso por correo electrónico o por teléfono.
21. Procedimiento de respaldo y recuperación de datos	**21** Indicar si es el caso donde los medios de respaldo con que se cuenta, siendo deseable al menos dos lugares distintos que cumplan con las condiciones de seguridad; o bien si se utiliza un espacio externo seguro para guardar de manera sistemática datos y respaldos; 1. Señalar si realiza respaldos completos, diferenciales o incrementales; 2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad; 3. Cómo y dónde archiva esos medios, y 4. Quién es el responsable de realizar estas operaciones (el sujeto obligado o un tercero) Indicar si se cuenta con un plan de contingencia y si este atiende lo siguiente: 1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene pero se encuentra desarrollándolo. 2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia del mismo. 3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente: a) El tipo de sitio (caliente, tibio o frío); b) Si el sitio es propio o sub contratado con un tercero; c) Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio, y d) Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia. El tipo de sitio **caliente, tibio o frío** se refiere a la infraestructura, el equipo y el software disponibles en el sitio alterno; por lo que a mayor disponibilidad de dichos elementos

	resulta una menor demora para restablecer las operaciones de uno o más sistemas. Ejemplos de lo anterior son, en cuanto a infraestructura: aire acondicionado, cableado, suministro de energía eléctrica y enlaces de comunicaciones; en cuanto al equipo: servidores, almacenamiento y periféricos, y por lo que se refiere al software: sistemas operativos, manejadores de bases de datos y aplicaciones. Por lo tanto: i) **En un sitio alterno caliente** se mantienen disponibles en todo momento la infraestructura, el equipo y el software; lo único que hace falta para iniciar operaciones son los datos y el personal. Este tipo de sitios alternos es el más costoso pero supone tan solo unas cuantas horas para restaurar operaciones. ii) **El sitio alterno tibio** cuenta con infraestructura no configurada y equipos equivalentes que pueden estar disponibles en pocas horas pero no contienen software ni datos. Este tipo de sitios alternos es el punto medio en costo y tiempo para restaurar operaciones. iii) **El sitio alterno frío** cuenta con un ambiente mínimo de infraestructura y no cuenta con el equipo. Este tipo de sitios alternos es el menos costoso pero supone demora de algunos días para restablecer operaciones
22. Plan de contingencia	**22** Indicar el Prestador de servicios persona física o moral, pública o privada ajena al IMPI que sola o conjuntamente con otros, trata datos personales a nombre y por cuenta en subcontratación.
23. Encargado de datos	**23**. Existe un prestador de servicios, persona física o moral, pública o privada ajena al IMPI que sola o conjuntamente, trate datos personales a nombre y por cuenta de este Instituto

0. NÚMERO Y NOMBRE DEL ÁREA O UNIDAD ADMINISTRATIVA- 300 DIRECCIÓN DIVISIONAL DE MARCAS	
1. Nombre del Sistema	MARCANET, VIDOC Y SIGA.
2. Objetivo	Salvaguardar los derechos y prerrogativas que otorga la Ley de la Propiedad Industrial a los titulares de algún derecho reconocido por la misma Ley; así como dejar a salvo derechos de terceros.
3. Fundamento Legal	DECRETO POR EL QUE SE CREA EL INSTITUTO MEXICANO DE LA PROPIEDAD INDUSTRIAL (Publicado en el Diario Oficial de la Federación el 10 de diciembre de 1993). o Artículos 1°, 2o. fracciones I, II y III y ARTICULO 3o., fracciones I a IX. LEY DE LA PROPIEDAD INDUSTRIAL (Última reforma publicada en el DOF el 18 de mayo de 2018). o Artículos 1°., 2o., fracciones I a VII y artículo 3o., fracciones I a II y IV a VI; Artículo 6°, primer párrafo y fracciones I a XVI, XVIII, XIX y XXII; 89, fracción IV, 98 TER-4; 113, 116 y 126, fracción IV; 165 BIS 4, fracción I, 167, fracción I, 170, fracción I y 175, fracción I; artículos 179 y 180, primer párrafo; 181, fracciones I a IV, así como artículos 182 y 183. REGLAMENTO DE LA LEY DE LA PROPIEDAD INDUSTRIAL (Última reforma publicada en el DOF 16-12-2016). o Artículos 1o., 3°., segundo párrafo, 5°., fracciones I a IV y párrafos penúltimo y antepenúltimo; artículos 9°., 10, 12, 16, fracción I, 59 QUÁRTER; 64, fracciones I y II; 65 fracción I y 68 fracción I. ACUERDO por el que se modifica el diverso que establece las Reglas para la presentación de solicitudes ante el Instituto Mexicano de la Propiedad Industrial (Última reforma publicada DOF: 09-08-2018). o Artículos 1, 33, y 34, fracciones I a VIII y XIV a XVII.

4. DATOS PERSONALES QUE CONTIENE EL SISTEMA (señalar con una X, según corresponda)	
Dato personal	Idoneidad (informar para que se recaba el dato)
Nombre de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros); CURP, correo electrónico, domicilio, y número telefónico.	Salvaguardar los derechos de solicitantes a obtener un derecho relativo a propiedad industrial y protección de derechos de propiedad intelectual, garantizando el otorgamiento de los derechos y prerrogativas que otorga la Ley de la Propiedad Industrial a los titulares de derechos, y terceros a los que la Ley reconoce y protege, dejando a salvo sus derechos y prerrogativas legales; así como facilitar los trámites para la obtención de derechos y autorizaciones establecidas en la Ley de la Propiedad Industrial.

5. FORMA DE OBTENCIÓN DE LOS DATOS PERSONALES (señalar con una X, según corresponda)			
Directa		**Indirecta** (obtenida, creada, generada en algún otro sistema)	
Formulario físico	X	Descripción: Formatos de uso obligatorio para la solicitud de los trámites, y escritos adicionales que se reciben en soporte físico y soporte electrónico, acompañados de documentos físicos y electrónicos, tales como formularios de datos y documentos diversos.	
Formulario electrónico	X		
Texto físico	X		
Texto electrónico	X		
Vía telefónica			
Otro:			

6. Responsable del Sistema	
Nombre	PAOLA FRANCO ABARCA
Cargo	DIRECTORA DIVISIONAL DE MARCAS
Teléfono	53340700, extensión 10039
Correo electrónico	paola.franco@impi.gob.mx
Función	Dirigir y administrar los recursos humanos, materiales y de sistemas electrónicos puestos a disposición de la DDM, para el estudio y en su caso, otorgamiento de los derechos sobre signos distintivos; así como su mantenimiento y conservación, en términos de la Ley de la Propiedad Industrial y demás disposiciones derivadas de ella.
Obligación	Establecer las políticas, directrices y supervisión del correcto desempeño de las atribuciones conferidas en la Ley de la Propiedad y demás disposiciones aplicables.

7. Administrador del Sistema SIGMAR	
Nombre	Eduardo Conde Ángeles
Cargo	Coordinador Departamental de Desarrollo de Sistemas de Marcas
Teléfono	53640700 Ext 10102
Correo electrónico	eduardo.conde@impi.gob.mx
Función	Coordinador
Obligación	Administración Técnica del Sistema de Gestión de Marcas
8. Usuarios u Operador del Sistema	
Nombre	**Se acompaña relación del personal**
Cargo	
Teléfono	
Correo electrónico	
Función	
Obligación	

9. Tipo de soporte (señalar con una X, según corresponda)

*Electrónico		*Físico		*Ambos	X

*Descripción: Expedientes físicos que se resguardan en el archivo de Marcas en soporte papel.
Información que en formato digital se visualizan en el Sistema Integral de Gestión de Marcas, en el que se almacena la información contenida en los expedientes administrativos de solicitudes en trámite y registro de signos distintivos.

10. Transferencias o transmisiones de datos personales (señalar con una X, según corresponda)

*SI	X		NO

*Describir en que consiste la transferencia o transmisión

Marca en línea. Herramienta electrónica que permite a los usuarios de los servicios que presta el Instituto, llevar a cabo la presentación y tramitación de solicitudes de marca, mediante la captura de la información necesaria para obtener el registro, el pago electrónico de la tarifa y la firma electrónica de la solicitud, lo anterior sin necesidad de acudir a las oficinas del Instituto.
Consultable en: https://eservicios.impi.gob.mx/seimpi/

11. Portabilidad de datos (señalar con una X, según corresponda)

SI		NO	X

12. Nivel de protección que requieren los datos

Nivel medio.

13. Actualización de la información contenida en el sistema

Los datos se actualizan en tres periodos de tiempo; de inmediato, diariamente y semanalmente.

14. Plazo de conservación de los datos personales

Cuatro años.

15. Medidas de Seguridad

Físicas	-Se cuenta con un servicio de seguridad que es proporcionado por el Servicio de Protección Federal. -El Instituto cuenta con sistemas de video-vigilancia en cada los inmuebles de Arenal y Pedregal, operando al 50% de su capacidad. Los servidores públicos deben portar en todo momento su credencial institucional, así como hacer uso del hand-punch al ingreso y salida diaria. -El personal externo debe registrarse, dejar una identificación oficial, así como portar en todo momento el gafete de visita que le sea proporcionado en recepción. -La autorización de los accesos es proporcionada por cada área, mediante mesa de ayuda o correo electrónico. -Asimismo, con el fin de garantizar la integridad de la información del Instituto, se lleva a cabo una revisión del interior de mochilas, portafolios, bolsas grandes, maletas de equipaje, etc., registros en caso de ingreso con equipo de cómputo, así como del interior de las cajuelas de los vehículos que ingresan a las instalaciones. -Acceso restringido al acervo documental que obra en el Archivo de Marcas, solo personal autorizado accede, portando gafete institucional. -Consulta de expedientes del personal del Instituto, se efectúa siempre que porte credencial institucional y habiendo llenado formato de solicitud de expediente a consultar. -La consulta solo se realiza en el área destinada para tal fin, sin que se permita acceder con portafolios, mochilas o accesorios diversos que pudieran permitir la extracción de documentos o expedientes. -La consulta de expedientes al público en general se efectúa siempre que se porte gafete de acceso a las instalaciones del Instituto; se requiere el llenado de la cédula de préstamo de expediente y se entrega expediente después de haber solicitado al interesado una identificación con fotografía y se consulta el expediente en el área designada para tal fin, teniendo control

	visual de los usuarios, por el personal que atiende al público.
Administrativas	**Medidas de Seguridad administrativa:** **Política de seguridad.** - Se cuenta con Políticas de Seguridad para protección de la información. - Se cuenta con una Guía de Responsabilidades en Materia de Seguridad de la Información del empleado del instituto, la cual se da a conocer a los empleados en su proceso de contratación y se pone a la disposición en la intranet Institucional. **Cumplimiento de la normatividad.** - La adopción de medidas necesarias para garantizar la integridad, confidencialidad y disponibilidad; se realiza a través del cumplimiento de los controles mínimos de seguridad de la información como lo requisita el MAAGTICSI en el proceso ASI 6 en su factor crítico 1 - Se cuenta con cartas de aceptación de riesgos en las cuales se mencionan los controles a implementar por cada dominio tecnológico bajo el marco de MAAGTICSI e ISO/IEC27001 y 27002. **Organización de la seguridad de la información.** - Existencia de Grupos de trabajo para evaluación e implementación de seguridad de la información. - Cartas de Responsables de Dominios Tecnológicos. - Designación del RSI - Designación del ERISC ante el CNI. - Identificación de riesgos a la información mediante mapas de operación. - Tratamiento de los riegos mediante análisis y SOA de los mismos. - Implementación de controles mínimos y basados en análisis de los mismos. - Revisión periódica de los controles implementados. **Clasificación y control de activos.** - Se cuenta con catálogos de activos e infraestructuras críticas del Instituto que pueden resguardar información de datos personales. - Se cuenta con análisis de riegos de activos e infraestructuras críticas del Instituto que pueden resguardar información de datos personales. **Seguridad relacionada a los recursos humanos.** Responsivas para el uso de claves privilegiadas y tratamiento de información. - Se cuenta con cartas de uso de claves y equipo de cómputo, los cuales permiten acceso a aplicativos con información que pudiesen contener datos personales, las cartas son entregadas a todos los empleados del Instituto y firmadas por los mismos. - Se cuenta con cartas de confidencialidad y responsabilidad de uso de claves, las cuales permiten acceso a aplicativos con información almacenada que pudiesen contener datos personales, las cartas son firmadas por los administradores de los dominios tecnológicos. - Asignaciones de personal responsables de los activos de resguardo de información. **Administración de incidentes.** - Administración de incidentes de seguridad, gestión y tratamiento - Evaluación de pruebas de penetración y vulnerabilidad a los aplicativos informáticos. - Base de datos de conocimiento sobre incidentes para tratamiento de brechas. **Continuidad de las operaciones.** - Se cuenta con respaldo de información en cinta, las cuales se encuentran alojadas en bóveda externa de seguridad, para su uso en caso de caídas en la operación.
Técnicas	**Medidas de Seguridad técnicas.** La adopción de medidas necesarias para garantizar la integridad, confidencialidad y disponibilidad; se realiza a través del cumplimiento de los controles mínimos de seguridad de la información como lo requisita el MAAGTICSI en el proceso ASI 6 en su factor crítico 1 Todo acceso físico y lógico a donde se resguarda información que incluye datos personales requiere autenticación con usuario y clave para poder ingresar a los mismos. • Gestión de comunicaciones y operaciones. - A fin de mitigar el riesgo por perdida de datos, se realizan respaldo encriptado de estos en cintas magnéticas las cuales son enviadas a bóveda externa de seguridad externa al instituto conservando roles que permitan, recuperación hasta de un mes hacia atrás. - Uso de protección contra virus y malware en equipos de cómputo y buzones de correo electrónico así como en la navegación en internet. - Uso en encriptación en la transmisión de datos dentro de la infraestructura del instituto. - Almacenamiento cifrado de la información. - Uso de aplicativos en infraestructura para monitorear y prevenir ataques automatizados - Monitoreo perimetral para contención de posibles ataques a la información • Control de acceso. - Resguardo de los equipos que funcionan como repositorio en área especial dedicada (centro de cómputo) con acceso restringido y vigilancia 7x24x365. - El acceso al centro de cómputo es controlado y restringido por la DDSTI.

	- El control de acceso en puerta al SITE, se realiza por doble factor, biométrico (huella digital) y password. - Se cuenta con registro en bitácora manual y electrónica sobre los accesos al centro de cómputo. -Se tiene video vigilancia con monitoreo vía intranet e internet. - Los accesos a los activos e información son controlados por el dominio tecnológico a cargo del mismo, generando las listas autorizadas de acceso. - El acceso a aplicativos que puedan resguarden información personal es controlado y restringido usuarios autorizados, mediante validación por usuario y contraseña y basada en roles el acceso. • Adquisición, desarrollo, uso y mantenimiento de sistemas de información: Integración de controles de seguridad a los sistemas de información, desde su adquisición o desarrollo, durante su uso y mantenimiento, hasta su cancelación o baja definitiva. Considera procesamiento adecuado en las aplicaciones, controles criptográficos y seguridad de los archivos de sistema, entre otros. - Acceso restringido a la información con uso de cuenta personal. (Sistemas operativos, Bases de Datos, aplicativos de gestión y resguardo) - Acceso restringido a la información con base en roles.

16. Acceso a instalaciones

-Se cuenta con un servicio de seguridad que es proporcionado por el Servicio de Protección Federal.
-El Instituto cuenta con sistemas de video-vigilancia en cada los inmuebles de Arenal y Pedregal, operando al 50% de su capacidad.
-Los servidores públicos deben portar en todo momento su credencial institucional, así como hacer uso del hand-punch al ingreso y salida diaria.
-El personal externo debe registrarse, dejar una identificación oficial, así como portar en todo momento el gafete de visita que le sea proporcionado en recepción.
-La autorización de los accesos es proporcionada por cada área, mediante mesa de ayuda o correo electrónico.
-Asimismo, con el fin de garantizar la integridad de la información del Instituto, se lleva a cabo una revisión del interior de mochilas, portafolios, bolsas grandes, maletas de equipaje, etc., registros en caso de ingreso con equipo de cómputo, así como del interior de las cajuelas de los vehículos que ingresan a las instalaciones.

- Resguardo de los equipos que funcionan como repositorio en área especial dedicada (centro de cómputo) con acceso controlado y restringido.
- El acceso al centro de cómputo es controlado y restringido por la DDSTI.
- Se generan claves de acceso al centro de cómputo previa solicitud y análisis de la misma para la activación de accesos, las cuales tienen una duración máxima de 6 meses, la cual debe renovarse al finalizar este periodo.
- El control de acceso en puerta al SITE, se tiene por cerradura electromagnética administrada por control biométrico.
- El control biométrico de autorización de acceso al centro de cómputo trabaja en doble factor, biométrico (huella digital) y contraseña.
- Se cuenta con rondas de vigilancia al centro de cómputo por parte del personal de Policía Federal durante los horarios inhábiles para los empleados del instituto.
-Se tiene video vigilancia con monitoreo vía intranet e internet en7 x 24 x 365.
- Oficinas mobiliario destinado al almacenamiento (gavetas, lockers y escritorios) cuentan con cerraduras y llaves, además de tiene el servicio continuo de cerrajería para reparaciones.

17. Perfiles de usuario y contraseña

17 Indicar en este rubro el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.

1. Modelo de control de acceso
Basado en roles (perfiles) y discrecional (matriz de control de acceso) para acceso a equipos de cómputo, sistemas de gestión y servicios informáticos.

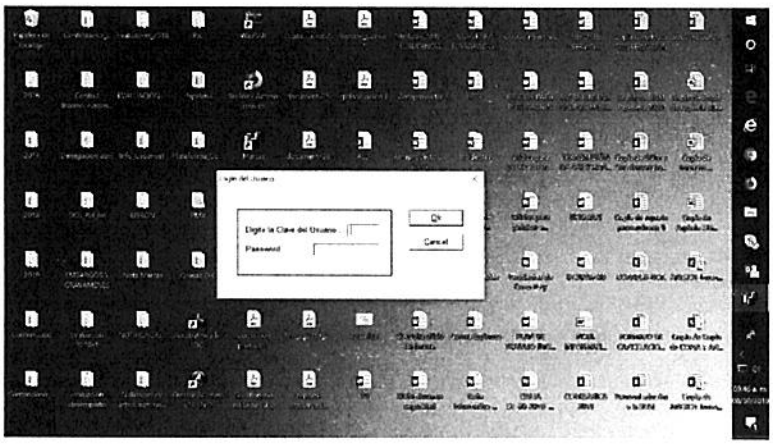
2. Perfiles de usuario y contraseñas en el sistema operativo de red:
a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
Se cuenta con sistema operativo de red y administrado por aplicativo nativo al mismo
b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
Si, se hace administran bajo uso de Directorio Activo y se tiene control de los perfiles de usuario así como control en las contraseñas en cuanto a composición y tiempos de cambio de la misma.
c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Si, se hace administran bajo uso de Directorio Activo.
3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de datos personales:
a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
Si, se hace administran bajo uso de Directorio Activo y se tiene control de los perfiles de usuario así como control en las contraseñas en cuanto a composición y tiempos de cambio de la misma.
b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?

Si, se hace administran bajo uso de Directorio Activo

4. Administración de perfiles de usuario y contraseñas:
a) ¿Quién da de alta nuevos perfiles?
La DDSTI a petición expresa de la Dirección Divisional responsable.
b) ¿Quién autoriza la creación de nuevos perfiles?
La Dirección Divisional responsable.
c) ¿Se lleva registro de la creación de nuevos perfiles?
Si

5. Acceso remoto al sistema de datos personales:
a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
No
b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
No
c) ¿Cómo se evita el acceso remoto no autorizado?
- Mediante la acls de negación vía firewall a puertos y aplicativos no autorizados

18. Bitácoras de acceso y operación cotidiana, seguridad aplicable (señalar con una X, según corresponda)

	Soporte físico	-El soporte físico del Archivo de Marcas, no tiene bitácoras diarias, pero se cuenta con información de las personas que solicitaron algún expediente para su consulta, conteniendo el nombre del solicitante, el número de expediente solicitado y la fecha.
	Soporte electrónico	EN SIGMAR, se incluye un apartado de préstamo de expedientes para los usuarios internos en las áreas de trabajo. EJEMPLO: 

19. Lugar de almacenamiento de las bitácoras y tiempo de conservación y conservación de integridad

Los registros de movimiento de expedientes se encuentran dentro del SIGMAR y puede ser consultado el movimiento de expedientes.

20. Registro de incidentes

-Soportes físicos: El incidente debe ser reportado al Coordinador Departamental y se toman acciones para la conservación documental física, formulándose un acta de lo sucedido y de la cual se integra una copia al expediente respectivo.
-En el caso de expedientes no localizados, se tiene el soporte de documentos en imágenes y se procede a la formación de un expediente en soporte físico, integrado de la impresión de las imágenes que se encuentran dentro del sistema y se procede a efectuar búsquedas exhaustivas por área para la localización y resguardo del expediente respectivo.

Soportes electrónicos:
A la fecha del presente no se han presentado incidentes físicos o electrónicos que impliquen la pérdida o alteración no autorizada de expedientes.

21. Procedimiento de respaldo y recuperación de datos

A fin de mitigar el riesgo por perdida de datos, se realizan respaldo de estos en cintas magnéticas las cuales son enviadas a bóveda de seguridad externa al instituto conservando roles que permitan la recuperación hasta de un mes hacia atrás.

Se mantiene un proceso de administración de servicios (procesamiento de computo central, Servidores físicos y

virtuales, administración de las bases de datos respaldos de información y restauración de información)

(Disponible en el portal MAAGTICSI del Instituto) el cual incluye lo siguiente:

Programa de Capacidad
Programa de Continuidad
Programa de Disponibilidad

22. Plan de contingencia

-El archivo de marcas en una contingencia que impida el acceso a las instalaciones del Instituto, dejaría de prestar expedientes para consulta, debido al volumen de expedientes que se encuentran en el mismo, siendo extremadamente complicado trasladar los acervos documentales en soporte papel a otro edificio o lugar, debidamente acondicionado para el soporte y resguardo de los expedientes físicos; no obstante, se procede a asegurar la conservación de los acervos documentales, e tano puedan iniciarse las actividades regularmente; asimismo, se tiene el respaldo de cada expediente en el sistema de marcas, accediendo a SIGMAR para los usuarios internos y los usuarios externos, tienen acceso a la plataforma MARCANET, en donde pueden consultar los documentos que conforman cada expediente de su interés, así como datos de los registros y solicitudes en trámite.
-El soporte documental se tiene en la mayoría de los casos en soporte físico y electrónico, siendo en menor cuantía los expedientes que solo se encuentran en soporte electrónico.

Sistemas:
La información se encuentra resguardada en lugares que tienen controles estrictos de acceso.

23. Encargado de datos (señalar con una X, según corresponda)

Existe un prestador de servicios, persona física o moral, pública o privada ajena al IMPI que sola o conjuntamente, trate datos personales a nombre y por cuenta de este Instituto	SI	**X**	NO	
22. Plazo de conservación de los datos personales	4 años			

0. NÚMERO Y NOMBRE DEL ÁREA O UNIDAD ADMINISTRATIVA 200 DIRECCIÓN DIVISIONAL DE PATENTES			
1. Nombre del Sistema	Sistema Automatizado de Gestión de Patentes (SAGPAT)		
2. Objetivo	Es la herramienta electrónica través de la cual la Dirección Divisional de Patentes administra las solicitudes de patente y registros que ingresan. Este sistema también funge como registro histórico, se lleva un control sobre los actos de autoridad que emite la Dirección en relación con el trámite; así como de las promociones que ingresan los solicitantes. El sistema es el medio electrónico de todos los documentos que gestiona la Dirección Divisional de Patentes.		
3. Fundamento Legal	El tratamiento respectivo se realiza con fundamento en los artículos 9, 13, 30, 30 BIS, 37, 37 BIS, 38, 47, 52 BIS, 181, 183 y 186 de la Ley de la Propiedad Industrial (LPI), 5, 18 y 20 del Reglamento de la LPI (RLPI), y 22, fracciones I, II, III, IV, V, VIII, IX la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) así como para dar cumplimiento a lo dispuesto por los artículos 6, fracciones X, XII, incisos a) y b) y XVI, 8, 38, segundo párrafo, 52, 59, 189 fracción III de la LPI, 13, 14, 15, 18 y 39, del Reglamento de la Ley de la Propiedad Industrial, 1° y 3, fracciones III, inciso a) y IV, del Decreto por el cual se crea el IMPI, 12 del Convenio de París para la Protección de la Propiedad Industrial y a los tratados internacionales y acuerdos institucionales suscritos por el IMPI.		
4. DATOS PERSONALES QUE CONTIENE EL SISTEMA (señalar con una X, según corresponda)			
Dato personal	Idoneidad (informar para que se recaba el dato)		
Nombre	Son recabados con la finalidad de dar trámite a la solicitud		
Domicilio	Contactar al solicitante, su representante en relación al trámite. Notificar actos y resoluciones que así lo requieran		
Nacionalidad	Contactar al solicitante, su representante en relación al trámite. Notificar actos y resoluciones que así lo requieran		
5. FORMA DE OBTENCIÓN DE LOS DATOS PERSONALES (señalar con una X, según corresponda)			
Directa		**Indirecta** (obtenida, creada, generada en algún otro sistema)	
Formulario físico	**X**	**Descripción:** El solicitante ingresa Formato de Solicitud debidamente llenado ante la Dirección Divisional de Patentes, mediante el cual se toman los datos para su captura en el Sistema Automatizado de Gestión de Patentes (SAGPAT)	
Formulario electrónico	**X**		
Texto físico			
Texto electrónico			
Vía telefónica			
Otro			
6. Responsable del Sistema			
Nombre	Eulalia Méndez Monroy		
Cargo	Directora Divisional de Patentes		
Teléfono	53340700 Ext. 10010		
Correo electrónico	eulalia.mendez@impi.gob.mx		
Función	Supervisión de las actividades registradas en el Sistema de Gestión (SAGPAT); Autorización de perfiles o roles; autorización de uso y/o acceso al sistema.		
Obligación	Supervisión de las actividades registradas en el Sistema de Gestión (SAGPAT)		
7. Administrador del Sistema			
Nombre	Agustín Fernando Bello Vázquez		
Cargo	Director Divisional de Sistemas y Tecnología de la Información		
Teléfono	53340700 Ext. 10000		
Correo electrónico	agustin.bello@impi.gob.mx		
Función	Supervisión de las actividades registradas en el Sistema de Gestión (SAGPAT). Autorización de uso y/o acceso al sistema		
Obligación	Supervisión de las actividades registradas en el Sistema de Gestión (SAGPAT).		
8. Usuarios u Operador del Sistema			
Nombre	Se anexa listado		
Cargo			
Teléfono			
Correo electrónico			
Función			
Obligación			
9. Tipo de soporte (señalar con una X, según corresponda)			
*Electrónico		*Físico		*Ambos	**X**
*Descripción: Los expedientes físicos se encuentra bajo resguardo de la Coordinación Departamental de Archivo de Patentes y el soporte electrónico en el Sistema Automatizado de Gestión de Patentes (SAGPAT)			
10. Transferencias o transmisiones de datos personales (señalar con una X, según corresponda)			
*SI	X		NO
*Describir en que consiste la transferencia o transmisión Se transfieren datos únicamente cuando estos ya se encuentran disponibles al público, sin embargo, ello no impide el ejercicio de los derechos ARCO ante el receptor, que en el caso de invenciones corresponden a la Organización Mundial			

de la Propiedad Intelectual (OMPI), a la Oficina Europea de Patentes (EPO), y a la Oficina de Propiedad Intelectual de la Unión Europea (EUIPO). El IMPI efectúa transferencias que no requieren consentimiento, a partir de la información pública, con la finalidad de divulgación: **a)** en materia de patentes y modelos de utilidad a la Oficina Europea de Patentes, para su publicación en ESPACENET y LATIPAT y referenciación en el European Patent Register, conforme al párrafo 18 del Memorándum de Entendimiento No. 2015/0099 de 15 de julio de 2015 y a los apartados 3, inciso c) y 7 del Memorándum de Entendimiento No. 2013/0264 de 25 de septiembre de 2013, y **b)** en materia de diseños industriales a la Oficina de Propiedad Intelectual de la Unión Europea (EUIPO), para su publicación en Designview conforme al apartado 3, inciso a) Memorando de Entendimiento sobre Cooperación Bilateral entre la EUIPO de 05 de octubre de 2016 y artículo 2 del Acuerdo sobre el proyecto de cooperación Designview de 24 de septiembre de 2014.

11. Portabilidad de datos (señalar con una X, según corresponda)

SI		NO	X

12. Nivel de protección que requieren los datos

Nivel Básico

13. Actualización de la información contenida en el sistema

Se actualiza diario, en atención a las promociones ingresadas por los solicitantes, inventores, apoderados legales.

14. Plazo de conservación de los datos personales

De acuerdo a lo dispuesto por el Artículo 18 del Reglamento de la Ley de la Propiedad Industrial, los expedientes podrán consultarse y permanecerán en el archivo del Instituto durante la vigencia de los derechos de propiedad industrial a que se refieran, salvo aquellos casos en los que el Instituto considere que deberán permanecer por más tiempo. Así mismo, se cuenta con una vigencia documental, archivo de concentración de 5 años.

15. Medidas de Seguridad

Físicas	Los elementos de seguridad con que cuenta el Instituto, están basados en el marco del Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones, y de Seguridad de la Información (MAAGTICSI) así como del estándar ISO/IEC 27001 e ISO/IEC 27002, ambos en sus versiones vigentes. Para el caso de la DDSTI, el uso y tratamiento de datos personales corresponde al resguardo de estos bajo la figura de custodio y su manipulación únicamente en el alcance del ejercicio sus facultades. Medidas de Seguridad física: - Control de acceso perimetral en primera línea al acceso a instalaciones Personal de Policía Federal custodian el acceso a los inmuebles del Instituto - Se exige portabilidad de credencial de identificación oficial del Instituto a todo empleado y de gafetes de acceso a todo personal externo. - Resguardo de datos electrónicos en equipos de cómputo con acceso por personal con rol autorizado. - Control de acceso perimetral en segunda línea al acceso a las instalaciones de resguardo - Equipos de resguardo de información hospedados en sitio con acceso controlado y restringido a personal autorizado con monitoreo de vigilancia 7x24x365. - El acceso al sitio de hospedaje, posee triple factor de autenticación (listado de personal autorizado, acceso biométrico dactilar, así como el uso de usuario y contraseña. - Registro en bitácora electrónica del acceso al sitio. El personal de la Dirección Divisional de Patentes, en su totalidad, accede al Sistema a través de las computadoras que cada uno tiene asignada. No obstante, el Sistema es restrictivo ya que todo usuario cuenta con una clave única de acceso. Los equipos de cómputo se encuentran distribuidos por áreas administrativas; de forma que cada empleado adscrito a un área determinada cuenta con una computadora.
Administrativas	**Medidas de Seguridad administrativa:** **Política de seguridad.** - Se cuenta con Políticas de Seguridad para protección de la información. - Se cuenta con una Guía de Responsabilidades en Materia de Seguridad de la Información del empleado del instituto, la cual se da a conocer a los empleados en su proceso de contratación y se pone a la disposición en la intranet Institucional. **Cumplimiento de la normatividad.** - La adopción de medidas necesarias para garantizar la integridad, confidencialidad y disponibilidad; se realiza a través del cumplimiento de los controles mínimos de seguridad de la información como lo requisita el MAAGTICSI en el proceso ASI 6 en su factor crítico 1

	- Se cuenta con cartas de aceptación de riesgos en las cuales se mencionan los controles a implementar por cada dominio tecnológico bajo el marco de MAAGTICSI e ISO/IEC27001 y 27002. **Organización de la seguridad de la información.** - Existencia de Grupos de trabajo para evaluación e implementación de seguridad de la información. - Cartas de Responsables de Dominios Tecnológicos. - Designación del RSI - Designación del ERISC ante el CNI. - Identificación de riesgos a la información mediante mapas de operación. - Tratamiento de los riegos mediante análisis y SOA de los mismos. - Implementación de controles mínimos y basados en análisis de los mismos. - Revisión periódica de los controles implementados. **Clasificación y control de activos.** - Se cuenta con catálogos de activos e infraestructuras críticas del Instituto que pueden resguardar información de datos personales. - Se cuenta con análisis de riegos de activos e infraestructuras críticas del Instituto que pueden resguardar información de datos personales. **Seguridad relacionada a los recursos humanos.** Responsivas para el uso de claves privilegiadas y tratamiento de información. - Se cuenta con cartas de uso de claves y equipo de cómputo, los cuales permiten acceso a aplicativos con información que pudiesen contener datos personales, las cartas son entregadas a todos los empleados del Instituto y firmadas por los mismos. - Se cuenta con cartas de confidencialidad y responsabilidad de uso de claves, las cuales permiten acceso a aplicativos con información almacenada que pudiesen contener datos personales, las cartas son firmadas por los administradores de los dominios tecnológicos. - Asignaciones de personal responsables de los activos de resguardo de información. **Administración de incidentes.** - Administración de incidentes de seguridad, gestión y tratamiento - Evaluación de pruebas de penetración y vulnerabilidad a los aplicativos informáticos. - Base de datos de conocimiento sobre incidentes para tratamiento de brechas. **Continuidad de las operaciones.** - Se cuenta con respaldo de información en cinta, las cuales se encuentran alojadas en bóveda externa de seguridad, para su uso en caso de caídas en la operación.
Técnicas	**Medidas de Seguridad técnicas.** La adopción de medidas necesarias para garantizar la integridad, confidencialidad y disponibilidad; se realiza a través del cumplimiento de los controles mínimos de seguridad de la información como lo requisita el MAAGTICSI en el proceso ASI 6 en su factor crítico 1 Todo acceso físico y lógico a donde se resguarda información que incluye datos personales requiere autenticación con usuario y clave para poder ingresar a los mismos. • Gestión de comunicaciones y operaciones. - A fin de mitigar el riesgo por perdida de datos, se realizan respaldo encriptado de estos en cintas magnéticas las cuales son enviadas a bóveda externa de seguridad externa al instituto conservando roles que permitan, recuperación hasta de un mes hacia atrás. - Uso de protección contra virus y malware en equipos de cómputo y buzones de correo electrónico, así como en la navegación en internet. - Uso en encriptación en la transmisión de datos dentro de la infraestructura del instituto. - Almacenamiento cifrado de la información. - Uso de aplicativos en infraestructura para monitorear y prevenir ataques automatizados - Monitoreo perimetral para contención de posibles ataques a la información • Control de acceso. - Resguardo de los equipos que funcionan como repositorio en área especial dedicada (centro de cómputo) con acceso restringido y vigilancia 7x24x365. - El acceso al centro de cómputo es controlado y restringido por la DDSTI. - El control de acceso en puerta al SITE, se realiza por doble factor, biométrico (huella digital) y password. - Se cuenta con registro en bitácora manual y electrónica sobre los accesos al centro de cómputo. -Se tiene video vigilancia con monitoreo vía intranet e internet. - Los accesos a los activos e información son controlados por el dominio tecnológico a cargo del mismo, generando las listas autorizadas de acceso. - El acceso a aplicativos que puedan resguarden información personal es controlado y restringido usuarios autorizados, mediante validación por usuario y contraseña y basada en roles el acceso. • Adquisición, desarrollo, uso y mantenimiento de sistemas de información: Integración de controles de seguridad a los sistemas de información, desde su adquisición o desarrollo, durante su uso y mantenimiento, hasta su cancelación o baja definitiva. Considera

	procesamiento adecuado en las aplicaciones, controles criptográficos y seguridad de los archivos de sistema, entre otros. - Acceso restringido a la información con uso de cuenta personal. (Sistemas operativos, Bases de Datos, aplicativos de gestión y resguardo) - Acceso restringido a la información con base en roles.

16. Acceso a instalaciones

- Resguardo de los equipos que funcionan como repositorio en área especial dedicada (centro de cómputo) con acceso controlado y restringido.
- El acceso al centro de cómputo es controlado y restringido por la DDSTI.
- Se generan claves de acceso al centro de cómputo previa solicitud y análisis de la misma para la activación de accesos, las cuales tienen una duración máxima de 6 meses, la cual debe renovarse al finalizar este periodo.
- El control de acceso en puerta al SITE, se tiene por cerradura electromagnética administrada por control biométrico.
- El control biométrico de autorización de acceso al centro de cómputo trabaja en doble factor, biométrico (huella digital) y contraseña.
- Se cuenta con rondas de vigilancia al centro de cómputo por parte del personal de Policía Federal durante los horarios inhábiles para los empleados del instituto.
-Se tiene video vigilancia con monitoreo vía intranet e internet en7 x 24 x 365.
- Oficinas mobiliario destinado al almacenamiento (gavetas, lockers y escritorios) cuentan con cerraduras y llaves, además de tiene el servicio continuo de cerrajería para reparaciones.

Se cuenta con:

Claves de acceso personalizadas
Puntos de revisión estratégicos
Circuito Cerrado de video.
Procedimiento para la denuncia de intrusiones
Infraestructura adecuada (Sistemas)
Señalización
Acceso electrónico y restringido a las áreas del Instituto

17. Perfiles de usuario y contraseña

Indicar en este rubro el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.

1. Modelo de control de acceso
Es obligatorio, basado en roles (perfiles) y discrecional (matriz de control de acceso) para acceso a equipos de cómputo, sistemas de gestión y servicios informáticos.

2. Perfiles de usuario y contraseñas en el sistema operativo de red:
a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
Se cuenta con sistema operativo de red y administrado por aplicativo nativo al mismo

b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
Si, se hace administran bajo uso de Directorio Activo y se tiene control de los perfiles de usuario, así como control en las contraseñas en cuanto a composición y tiempos de cambio de la misma.

c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Si, se hace administran bajo uso de Directorio Activo.

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de datos personales:
a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
Si, se hace administran bajo uso de Directorio Activo y se tiene control de los perfiles de usuario, así como control en las contraseñas en cuanto a composición y tiempos de cambio de la misma.

b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Si, se hace administran bajo uso de Directorio Activo

4. Administración de perfiles de usuario y contraseñas:
a) ¿Quién da de alta nuevos perfiles?
La DDSTI a petición expresa de la Dirección Divisional responsable.

b) ¿Quién autoriza la creación de nuevos perfiles?
La Dirección Divisional responsable.

c) ¿Se lleva registro de la creación de nuevos perfiles?
Si

5. Acceso remoto al sistema de datos personales:
a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
No

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
No aplica

c) ¿Cómo se evita el acceso remoto no autorizado?
- Mediante las reglas de control de acceso de negación vía firewall a puertos y aplicativos no autorizados

Por otro lado, aun cuando los equipos de cómputo cuentan con claves de acceso, también cuentan con distintos perfiles según el nivel jerárquico y/o atribuciones de los usuarios; de forma que no todo el personal que tiene acceso al sistema puede hacer modificaciones o alteraciones en el sistema.

18. Bitácoras de acceso y operación cotidiana, seguridad aplicable (señalar con una X, según corresponda)

	Soporte físico	Se cuenta con documentos de comprobación inmediata, relaciones de expedientes y promociones y oficios.
X	Soporte electrónico	a) Log de eventos a nivel de Sistema Operativo, cortafuegos y detector de intrusos. b) Se guarda un registro histórico de cada movimiento generado en los sistemas. c) Se guarda un registro histórico de cada movimiento generado en los sistemas. d) No Se encuentra en soporte electrónico y viven en los dispositivos y servidores del instituto.

19. Lugar de almacenamiento de las bitácoras y tiempo de conservación y conservación de integridad

De acuerdo a lo dispuesto por el Artículo 18 del Reglamento de la Ley de la Propiedad Industrial, los expedientes podrán consultarse y permanecerán en el archivo del Instituto durante la vigencia de los derechos de propiedad industrial a que se refieran, salvo aquellos casos en los que el Instituto considere que deberán permanecer por más tiempo.
El soporte electrónico, vive en los dispositivos y servidores del instituto y se generan en tiempo real de acuerdo a la operación de los mismos. Se cuenta con un servicio que proporciona una herramienta que se encarga del análisis automatizado de los logs de detector de intrusos (correlacionador de eventos).

Los documentos de comprobación inmediata (relaciones de expedientes y promociones y oficios) se resguardan por un periodo de un año. No hay área especial de resguardo.

20. Registro de incidentes

El sistema SAGPAT es el medio electrónico de todos los documentos que gestiona la Dirección Divisional de Patentes, es un sistema que solamente puede ser consultado por usuarios que pertenecen a la Dirección Divisional, sin embargo, en el caso de los datos personales que se publican a través de los diferentes portales electrónicos del Instituto, el usuario de los datos personales podrá ejercer sus derechos ARCO.

En la Coordinación de Archivo de Patentes son resguardados los expedientes, en caso de incidentes como goteras, fugas de agua, se envían correos electrónicos al área de servicios generales para que atienda el incidente a la brevedad.

21. Procedimiento de respaldo y recuperación de datos

A fin de mitigar el riesgo por perdida de datos, se realizan respaldo de estos en cintas magnéticas las cuales son enviadas a bóveda de seguridad externa al instituto conservando roles que permitan la recuperación hasta de un mes hacia atrás.

Se mantiene un proceso de administración de servicios (procesamiento de computo central, Servidores físicos y virtuales, administración de las bases de datos respaldos de información y restauración de información)

(Disponible en el portal MAAGTICSI del Instituto) el cual incluye lo siguiente:

Programa de Capacidad
Programa de Continuidad
Programa de Disponibilidad

En la Coordinación Departamental de Archivo de Patentes, en caso de un incidente por virtud del cual se afecte un expediente, se procede a la restauración de la documentación original como el caso de poderes, contratos, los demás documentos se reimprimen utilizando el sistema de SAGPAT.
22. Plan de contingencia
No se cuenta con un sitio de contingencia alterno. No se cuenta con plan de contingencia, sin embargo, la Coordinación Departamental de Archivo de Patentes cuenta con medidas preventivas, como son revisión de las instalaciones. Sistemas para sofocar incendios sistema VESDA.

23. Encargado de datos (señalar con una X, según corresponda)				
Existe un prestador de servicios, persona física o moral, pública o privada ajena al IMPI que sola o conjuntamente, trate datos personales a nombre y por cuenta de este Instituto	SI	**X**	NO	

SE SECRETARÍA DE ECONOMÍA | IMPI

DIRECCIÓN DIVISIONAL DE PROTECCIÓN A LA PROPIEDAD INTELECTUAL
DDPPI.2019.488

0. NÚMERO Y NOMBRE DEL ÁREA O UNIDAD ADMINISTRATIVA	400 Dirección Divisional de Protección a la Propiedad Intelectual		
1. Nombre del Sistema	Sistema Integral de Gestión de Asuntos de Protección a la Propiedad Intelectual (SIGAPPI)		
2. Objetivo	Tener una base de datos de la sustanciación de los procedimientos de observancia en materia de propiedad intelectual.		
3. Fundamento Legal	Títulos Sexto y Séptimo de la Ley de la Propiedad Industrial publicada en el Diario Oficial de la Federación el 27 de junio de 1991 (reformada, adicionada y derogada, según corresponda, mediante decretos publicados los días 2 de agosto de 1994, 25 de octubre de 1996, 26 de diciembre de 1997, 17 de mayo de 1999, 26 de enero del 2004, 16 de junio del 2005, 25 de enero del 2006, 6 de mayo de 2009, 6 de enero de 2010, 18 y 28 de junio de 2010, 27 de enero y 9 de abril de 2012, 1° de junio de 2016, 13 de marzo y 18 de mayo de 2018 en dicho medio informativo).		
4. DATOS PERSONALES QUE CONTIENE EL SISTEMA (señalar con una X, según corresponda)			
Dato personal	Idoneidad (informar para que se recaba el dato)		
Nombre de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros).	Los datos personales que son obtenidos y almacenados por la Dirección Divisional de Protección a la Propiedad Intelectual, son para realizar las facultades de inspección y vigilancia que conforme a la Ley de la Propiedad Industrial son competencia de la referida unidad administrativa.		
Datos personales contenidos en documento para acreditar personalidad del representante.			
Datos personales contenidos en la descripción del trámite a realizar o solicitud de derecho a ejercer.			
Datos personales contenidos en la identificación oficial presentada por la persona física.			
Domicilio para oír y recibir notificaciones			
Firma			
5. FORMA DE OBTENCIÓN DE LOS DATOS PERSONALES (señalar con una X, según corresponda)			
Directa		**Indirecta** (obtenida, creada, generada en algún otro sistema)	NA
Formulario físico		**Descripción:**	
Formulario electrónico			
Texto físico	x		
Texto electrónico			
Vía telefónica			
Otro			
6. Responsable del Sistema			
Nombre	Aldo Arturo Fragoso Pastrana		
Cargo	Director Divisional de Protección a la Propiedad Intelectual		
Teléfono	(55) 53340737		
Correo electrónico	aldo.fragoso@impi.gob.mx		
Función	Instruir para obtener y almacenar los datos personales que por disposición de Ley son requisitos para la procedibilidad de los trámites competencia de la Dirección Divisional de Protección a la Propiedad Intelectual.		
Obligación	Informar a la unidad administrativa competente las solicitudes para el ejercicio de los derechos ARCO.		
7. Administrador del Sistema			
Nombre	Juan Manuel Hernández García / Javier Raúl Romero García		
Cargo	Coordinador Departamental		
Teléfono	53340700 extensión 10043 / 10110		
Correo electrónico	juan.hernandez@impi.gob.mx / javier.romero@impi.gob.mx		
Función	Monitorear la operación y funcionabilidad del sistema.		
Obligación	Guardar debida secrecía de la información.		
8. Usuarios u Operador del Sistema			
Nombre	Se anexa relación de usuarios.		

Cargo					
Teléfono					
Correo electrónico					
Función					
Obligación					
9. Tipo de soporte (señalar con una X, según corresponda)					
*Electrónico		*Físico		*Ambos	x
*Descripción: Físico y electrónico					
10. Transferencias o transmisiones de datos personales (señalar con una X, según corresponda)					
*SI		NO	x		
*Describir en que consiste la transferencia o transmisión No aplica.					
11. Portabilidad de datos (señalar con una X, según corresponda)					
SI		NO	x		
12. Nivel de protección que requieren los datos					
Básico					
13. Actualización de la información contenida en el sistema					
La actualización de la información se lleva a cabo diariamente.					
14. Plazo de conservación de los datos personales					
En el archivo de trámite y de concentración de las unidades administrativas 7 años.					
15. Medidas de Seguridad					
Físicas	Identificación oficial del solicitante externo de los expedientes. **SOPORTE ELECTRÓNICO.** Los elementos de seguridad con que cuenta el Instituto, están basados en el marco del Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones, y de Seguridad de la Información (MAAGTICSI) así como del estándar ISO/IEC 27001 e ISO/IEC 27002, ambos en sus versiones vigentes. Para el caso de la DDSTI, el uso y tratamiento de datos personales corresponde al resguardo de estos bajo la figura de custodio y su manipulación únicamente en el alcance del ejercicio sus facultades. Resguardo de datos electrónicos en equipos de cómputo con acceso por personal con rol autorizado. Control de acceso perimetral en primera línea al acceso a instalaciones. Personal de Policía Federal custodian el acceso al inmueble del Instituto. Se exige portabilidad de credencial de identificación oficial del Instituto a todo empleado y de gafetes de acceso a todo personal externo. Control de acceso perimetral en segunda línea al acceso a las instalaciones de resguardo. Equipos de resguardo de información hospedados en sitio con acceso controlado y restringido a personal autorizado con monitoreo de vigilancia 7x24x365. El acceso al sitio de hospedaje, posee triple factor de autenticación (listado de personal autorizado, acceso biométrico dactilar, así como el uso de usuario y contraseña. Registro en bitácora electrónica del acceso al sitio. **SOPORTE FISICO** Control de acceso perimetral en primera línea al acceso a instalaciones. Personal de Policía Federal custodian el acceso al inmueble del Instituto. Se exige portabilidad de credencial de identificación oficial del Instituto a todo empleado y de gafetes de acceso a todo personal externo. Control de acceso perimetral en segunda línea al acceso a las instalaciones de resguardo. Préstamo de expedientes físicos únicamente a personas autorizadas en el procedimiento.				
Administrativas	**Política de seguridad.**				

	- Se cuenta con Políticas de Seguridad para protección de la información. - Se cuenta con una Guía de Responsabilidades en Materia de Seguridad de la Información del empleado del instituto, la cual se da a conocer a los empleados en su proceso de contratación y se pone a la disposición en la intranet Institucional. **Cumplimiento de la normatividad.** - La adopción de medidas necesarias para garantizar la integridad, confidencialidad y disponibilidad; se realiza a través del cumplimiento de los controles mínimos de seguridad de la información como lo requisita el MAAGTICSI en el proceso ASI 6 en su factor crítico 1 - Se cuenta con cartas de aceptación de riesgos en las cuales se mencionan los controles a implementar por cada dominio tecnológico bajo el marco de MAAGTICSI e ISO/IEC27001 y 27002. **Organización de la seguridad de la información.** - Existencia de Grupos de trabajo para evaluación e implementación de seguridad de la información. - Cartas de Responsables de Dominios Tecnológicos. - Designación del RSI - Designación del ERISC ante el CNI. - Identificación de riesgos a la información mediante mapas de operación. - Tratamiento de los riegos mediante análisis y SOA de los mismos. - Implementación de controles mínimos y basados en análisis de los mismos. - Revisión periódica de los controles implementados. **Clasificación y control de activos.** - Se cuenta con catálogos de activos e infraestructuras críticas del Instituto que pueden resguardar información de datos personales. - Se cuenta con análisis de riegos de activos e infraestructuras críticas del Instituto que pueden resguardar información de datos personales. **Seguridad relacionada a los recursos humanos.** Responsivas para el uso de claves privilegiadas y tratamiento de información. - Se cuenta con cartas de uso de claves y equipo de cómputo, los cuales permiten acceso a aplicativos con información que pudiesen contener datos personales, las cartas son entregadas a todos los empleados del Instituto y firmadas por los mismos. - Se cuenta con cartas de confidencialidad y responsabilidad de uso de claves, las cuales permiten acceso a aplicativos con información almacenada que pudiesen contener datos personales, las cartas son firmadas por los administradores de los dominios tecnológicos. - Asignaciones de personal responsables de los activos de resguardo de información. **Administración de incidentes.** - Administración de incidentes de seguridad, gestión y tratamiento - Evaluación de pruebas de penetración y vulnerabilidad a los aplicativos informáticos. - Base de datos de conocimiento sobre incidentes para tratamiento de brechas. **Continuidad de las operaciones.** - Se cuenta con respaldo de información en cinta, las cuales se encuentran alojadas en bóveda externa de seguridad, para su uso en caso de caídas en la operación. **SOPORTE FISICO** **Política de seguridad.** Conforme a la Ley Federal de Procedimiento Administrativo. **Cumplimiento de la normatividad.** Controles mínimos de seguridad de la información como lo establece la LFPA. **Organización de la seguridad de la información.** Existe un archivo en el cual se identifican los expedientes y que impiden el acceso a terceros. **Clasificación y control de activos.** Se cuenta con un catálogo de control archivístico. **Seguridad relacionada a los recursos humanos.** - Se cuenta con cartas de uso de claves y equipo de cómputo. **Administración de incidentes.** Conforme a la legislación aplicable **Continuidad de las operaciones.** - Se cuenta con respaldo de información.

Técnicas	La adopción de medidas necesarias para garantizar la integridad, confidencialidad y disponibilidad; se realiza a través del cumplimiento de los controles mínimos de seguridad de la información como lo requisita el MAAGTICSI en el proceso ASI 6 en su factor crítico 1 Todo acceso físico y lógico a donde se resguarda información que incluye datos personales requiere autenticación con usuario y clave para poder ingresar a los mismos. • Gestión de comunicaciones y operaciones. - A fin de mitigar el riesgo por perdida de datos, se realizan respaldo encriptado de estos en cintas magnéticas las cuales son enviadas a bóveda externa de seguridad externa al instituto conservando roles que permitan, recuperación hasta de un mes hacia atrás. - Uso de protección contra virus y malware en equipos de cómputo y buzones de correo electrónico, así como en la navegación en internet. - Uso en encriptación en la transmisión de datos dentro de la infraestructura del instituto. - Almacenamiento cifrado de la información. - Uso de aplicativos en infraestructura para monitorear y prevenir ataques automatizados - Monitoreo perimetral para contención de posibles ataques a la información • Control de acceso. - Resguardo de los equipos que funcionan como repositorio en área especial dedicada (centro de cómputo) con acceso restringido y vigilancia 7x24x365. - El acceso al centro de cómputo es controlado y restringido por la DDSTI. - El control de acceso en puerta al SITE, se realiza por doble factor, biométrico (huella digital) y password. - Se cuenta con registro en bitácora manual y electrónica sobre los accesos al centro de cómputo. -Se tiene video vigilancia con monitoreo vía intranet e internet. - Los accesos a los activos e información son controlados por el dominio tecnológico a cargo del mismo, generando las listas autorizadas de acceso. - El acceso a aplicativos que puedan resguarden información personal es controlado y restringido usuarios autorizados, mediante validación por usuario y contraseña y basada en roles el acceso. • Adquisición, desarrollo, uso y mantenimiento de sistemas de información: Integración de controles de seguridad a los sistemas de información, desde su adquisición o desarrollo, durante su uso y mantenimiento, hasta su cancelación o baja definitiva. Considera procesamiento adecuado en las aplicaciones, controles criptográficos y seguridad de los archivos de sistema, entre otros. - Acceso restringido a la información con uso de cuenta personal. (Sistemas operativos, Bases de Datos, aplicativos de gestión y resguardo) - Acceso restringido a la información con base en roles.

16. Acceso a instalaciones

SOPORTE FISICO

Seguridad perimetral exterior.
Bitácora de acceso que se valida con la identificación oficial del solicitante de los expedientes.
Seguridad perimetral interior.
Conforme a la Ley Federal de Procedimiento Administrativo.
Con claves de acceso al sistema primario.
- Resguardo de los equipos que funcionan como repositorio en área especial dedicada (centro de cómputo) con acceso controlado y restringido.
- El acceso al centro de cómputo es controlado y restringido por la DDSTI.
- Se generan claves de acceso al centro de cómputo previa solicitud y análisis de la misma para la activación de accesos, las cuales tienen una duración máxima de 6 meses, la cual debe renovarse al finalizar este periodo.
- El control de acceso en puerta al SITE, se tiene por cerradura electromagnética administrada por control biométrico.
- El control biométrico de autorización de acceso al centro de cómputo trabaja en doble factor, biométrico (huella digital) y contraseña.
- Se cuenta con rondas de vigilancia al centro de cómputo por parte del personal de Policía Federal durante los horarios inhábiles para los empleados del instituto.
-Se tiene video vigilancia con monitoreo vía intranet e internet en7 x 24 x 365.
- Oficinas mobiliario destinado al almacenamiento (gavetas, lockers y escritorios) cuentan con cerraduras y llaves, además de tiene el servicio continuo de cerrajería para reparaciones.

SOPORTE ELECTRÓNICO

- Resguardo de los equipos que funcionan como repositorio en área especial dedicada (centro de cómputo) con acceso controlado y restringido.
- El acceso al centro de cómputo es controlado y restringido por la DDSTI.
- Se generan claves de acceso al centro de cómputo previa solicitud y análisis de la misma para la activación de accesos, las cuales tienen una duración máxima de 6 meses, la cual debe renovarse al finalizar este periodo.
- El control de acceso en puerta al SITE, se tiene por cerradura electromagnética administrada por control biométrico.
- El control biométrico de autorización de acceso al centro de cómputo trabaja en doble factor, biométrico (huella digital) y contraseña.
- Se cuenta con rondas de vigilancia al centro de cómputo por parte del personal de Policía Federal durante los horarios inhábiles para los empleados del instituto.
-Se tiene video vigilancia con monitoreo vía intranet e internet en7 x 24 x 365.

17. Perfiles de usuario y contraseña

1. Modelo de control de acceso
Es obligatorio, basado en roles (perfiles) y discrecional (matriz de control de acceso) para acceso a equipos de cómputo, sistemas de gestión y servicios informáticos.

2. Perfiles de usuario y contraseñas en el sistema operativo de red:
a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
Se cuenta con sistema operativo de red y administrado por aplicativo nativo al mismo
b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
Si, se hace administran bajo uso de Directorio Activo y se tiene control de los perfiles de usuario así como control en las contraseñas en cuanto a composición y tiempos de cambio de la misma.
c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Si, se hace administran bajo uso de Directorio Activo.
3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de datos personales:
a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
Si, se hace administran bajo uso de Directorio Activo y se tiene control de los perfiles de usuario así como control en las contraseñas en cuanto a composición y tiempos de cambio de la misma.
b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Si, se hace administran bajo uso de Directorio Activo
4. Administración de perfiles de usuario y contraseñas:
a) ¿Quién da de alta nuevos perfiles?
La DDSTI a petición expresa de la Dirección Divisional responsable.
b) ¿Quién autoriza la creación de nuevos perfiles?
La Dirección Divisional responsable.
c) ¿Se lleva registro de la creación de nuevos perfiles?
Si
5. Acceso remoto al sistema de datos personales:
a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
No
b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
N/A
c) ¿Cómo se evita el acceso remoto no autorizado?
- Mediante las reglas de control de acceso de negación vía firewall a puertos y aplicativos no autorizados

18. Bitácoras de acceso y operación cotidiana, seguridad aplicable (señalar con una X, según corresponda)

x	Soporte físico	Las bitácoras se encuentran resguardas en archiveros con llaves designadas a los usuarios Conforme a la Ley Federal de Procedimiento Administrativo, los solicitantes se identifican como autorizados en el soporte físico a consultar.



18. Bitácoras de acceso y operación cotidiana, seguridad aplicable (señalar con una X, según corresponda)

x	Soporte electrónico	a) Log de eventos a nivel de Sistema Operativo, cortafuegos y detector de intrusos. b) Se guarda un registro histórico de cada movimiento generado en los sistemas. c) Se guarda un registro histórico de cada movimiento generado en los sistemas. d) No Se encuentra en soporte electrónico y viven en los dispositivos y servidores del instituto.

19. Lugar de almacenamiento de las bitácoras y tiempo de conservación y conservación de integridad

El soporte electrónico, vive en los dispositivos y servidores del instituto y se generan en tiempo real de acuerdo a la operación de los mismos. Se cuenta con un servicio que proporciona una herramienta que se encarga del análisis automatizado de los logs de detector de intrusos (correlacionador de eventos).

El soporte físico. El lugar de almacenamiento de las bitácoras es la Coordinación Departamental de Control y Procesamiento de Documentos y su conservación es por dos años.

20. Registro de incidentes

A la fecha del presente no se han presentado incidentes físicos o electrónicos que impliquen la pérdida o alteración no autorizada de expedientes.

1. Los datos que deberá registrar son:
a) La persona que resolvió el incidente;
No aplica
b) La metodología aplicada;
La establecida en la Legislación aplicable.
c) Para soportes físicos:
Denuncia ante la autoridad competente y recuperar la información del soporte electrónico.
d) Para soportes electrónicos:
Denuncia ante la autoridad competente y recuperar la información del soporte físico para generar el electrónico.
2. Si el registro está en soporte físico o en soporte electrónico;
No aplica
3. Cómo asegura la integridad de dicho registro, y
Conforme a las constancias
4. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos.
La DDPPI.

21. Procedimiento de respaldo y recuperación de datos

A fin de mitigar el riesgo por perdida de datos, la DDSTI realiza respaldos completos de estos en cintas magnéticas las cuales son enviadas a bóveda de seguridad externa al instituto conservando roles que permitan la recuperación hasta de un mes hacia atrás.

Se mantiene un proceso de administración de servicios (procesamiento de computo central, Servidores físicos y virtuales, administración de las bases de datos respaldos de información y restauración de información)

(Disponible en el portal MAAGTICSI del Instituto) el cual incluye lo siguiente:

Programa de Capacidad
Programa de Continuidad
Programa de Disponibilidad

22. Plan de contingencia

No se cuenta con un sitio de contingencia alterno.

23. Encargado de datos (señalar con una X, según corresponda)

Existe un prestador de servicios, persona física o moral, pública o privada ajena al IMPI que sola o conjuntamente, trate datos personales a nombre y por cuenta de este Instituto	SI	X Firma cláusula de confidencialidad	NO	x
22. Plazo de conservación de los datos personales	En el archivo de trámite y de concentración de las unidades administrativas 7 años.			

0. NÚMERO Y NOMBRE DEL ÁREA O UNIDAD ADMINISTRATIVA:	600 – Dirección Divisional de Administración		
1. Nombre del Sistema	**SAP (Contabilidad).**		
2. Objetivo	Guarda y conservación de documentación comprobatoria.		
3. Fundamento Legal	Reglamento del Instituto Mexicano de la Propiedad Industrial, Artículo 19, Fracción II, IV y V		
4. DATOS PERSONALES QUE CONTIENE EL SISTEMA (señalar con una X, según corresponda)			
Nombre	Para identificar a la persona		
Domicilio	Para localizar a la persona, proveedor o promovente en caso de ser necesario.		
Teléfono	Para localizar a la persona fuera del Instituto en caso de ser necesario..		
RFC	Para identificar como contribuyentes a las personas físicas o morales.		
5. FORMA DE OBTENCIÓN DE LOS DATOS PERSONALES (señalar con una X, según corresponda)			
Directa		**Indirecta** (obtenida, creada, generada en algún otro sistema)	
Formulario físico	X	**Descripción:**	
Formulario electrónico	X		
Texto físico			
Texto electrónico			
Vía telefónica			
Otro			
6. Responsable del Sistema			
Nombre	Víctor Manuel Terán Arista		
Cargo	Director Divisional de Administración		
Teléfono	5556240400 extensión 11018		
Correo electrónico	victor.teran@impi.gob.mx		
Función	Administrar los Recursos Humanos, Materiales y Financieros del Instituto conforme a normatividad establecida.		
Obligación	Administrar información dentro de un entorno para la administración y control de los recursos humanos, financieros y materiales del Instituto.		
7. Administrador del Sistema			
Nombre	Agustín Fernando Bello Vázquez		
Cargo	Director Divisional de Sistemas y Tecnología de la Información		
Teléfono	5553340700 extensión 10000		
Correo electrónico	agustin.bello@impi.gob.mx		
Función	Administrar la Información del Sistema		
Obligación	Resguardar información		
8. Usuarios u Operador del Sistema			
Nombre	Patricio Santos Martínez		
Cargo	Coordinador Departamental de Contabilidad		
Teléfono	5556240400 extensión 11171		
Correo electrónico	patricio.santos@impi.gob.mx		
Función	Vigilar y supervisar la recepción, otorgamiento, registro y control de datos		
Obligación	Resguardar información		
Nombre	Francisco Benitez Ramírez		
Cargo	Especialista "A" en Propiedad Industrial		
Teléfono	5556240400 extensión 11171		
Correo electrónico	francisco.benitez@impi.gob.mx		
Función	Recepción, registro y control de datos		
Obligación	Resguardar información		
Nombre	Dora Rosario López Colorado		
Cargo	Especialista "A" en Propiedad Industrial		
Teléfono	5556240400 extensión 11171		
Correo electrónico	dora.lopez@impi.gob.mx		
Función	Cargar y/o alimentar de datos al sistema y/o actualizar los mismos.		
Obligación	Resguardar información		
Nombre	Juan Reyes Sánchez		
Cargo	Especialista "A" en Propiedad Industrial		
Teléfono	5556240400 extensión 11268		
Correo electrónico	juan.reyes@impi.gob.mx		
Función	Cargar y/o alimentar de datos al sistema y/o actualizar los mismos.		
Obligación	Resguardar información		
Nombre	Diego Ivan Ramos Manrique		
Cargo	Auxiliar Técnico "A"		
Teléfono	5556240400 extensión 11171		
Correo electrónico	diego.ramos@impi.gob.mx		
Función	Cargar y/o alimentar de datos al sistema y/o actualizar los mismos.		
Obligación	Resguardar información		
Nombre	Carlos David Castañeda Murillo		
Cargo	Especialista "B" en Propiedad Industrial		

Teléfono	
Correo electrónico	carlos.castañeda@impi.gob.mx
Función	Cargar y/o alimentar de datos al sistema y/o actualizar los mismos.
Obligación	Resguardar información
Nombre	Rosario Sánchez Torres
Cargo	Ayudante especializado en servicios "C"
Teléfono	5556240400 extensión 11281
Correo electrónico	rosario.sanchez@impi.gob.mx
Función	Cargar y/o alimentar de datos al sistema y/o actualizar los mismos.
Obligación	Resguardar información
Nombre	Fernando Tomé Flores
Cargo	Ayudante especializado en servicios "C"
Teléfono	5556240400 extensión 11171
Correo electrónico	fernando.tome@impi.gob.mx
Función	Cargar y/o alimentar de datos al sistema y/o actualizar los mismos.
Obligación	Resguardar información

9. Tipo de soporte (señalar con una X, según corresponda)

*Electrónico		*Físico		*Ambos	X

*Descripción: Servidor y Expedientes de Personal

10. Transferencias o transmisiones de datos personales (señalar con una X, según corresponda)

*SI		NO	X

*Describir en que consiste la transferencia o transmisión

11. Portabilidad de datos (señalar con una X, según corresponda)

SI		NO	X

12. Nivel de protección que requieren los datos

Bajo

13. Actualización de la información contenida en el sistema

Quincenalmente en los datos que requieran actualización.

14. Plazo de conservación de los datos personales

Histórico en Servidor y 30 años en papel

15. Medidas de Seguridad

Físicas	Se cuenta con un servicio de seguridad que es proporcionado por el Servicio de Protección Federal. El Instituto cuenta con sistemas de video-vigilancia en cada los inmuebles de Arenal y Pedregal, operando al 50% de su capacidad. Los servidores públicos deben portar en todo momento su credencial institucional, así como hacer uso del hand-punch al ingreso y salida diaria. El personal externo debe registrarse, dejar una identificación oficial, así como portar en todo momento el gafete de visita que le sea proporcionado en recepción. La autorización de los accesos es proporcionada por cada área, mediante mesa de ayuda o correo electrónico. Asimismo, con el fin de garantizar la integridad de la información del Instituto, se lleva a cabo una revisión del interior de mochilas, portafolios, bolsas grandes, maletas de equipaje, etc., registros en caso de ingreso con equipo de cómputo, así como del interior de las cajuelas de los vehículos que ingresan a las instalaciones. Para el acceso a los expedientes, éstos se encuentran debidamente resguardados en archiveros bajo llave y los responsables de los archivos de cada Coordinación son quienes tienen el control de estas llaves.
Administrativas	La información que se recaba en la Subdirección es en cumplimiento a la normatividad establecida en materia de contrataciones, por lo que está debidamente justificada la finalidad por la cual se recaban.
Técnicas	Clave de usuario y password para acceso a sistemas.

16. Acceso a instalaciones

Con credencial de empleado y/o Identificación oficial.

Se cuenta con un servicio de seguridad que es proporcionado por el Servicio de Protección Federal.
El Instituto cuenta con sistemas de video-vigilancia en cada los inmuebles de Arenal y Pedregal, operando al 50% de su capacidad.
Los servidores públicos deben portar en todo momento su credencial institucional, así como hacer uso del hand-punch al ingreso y salida diaria.
El personal externo debe registrarse, dejar una identificación oficial, así como portar en todo momento el gafete de visita que le sea proporcionado en recepción.
La autorización de los accesos es proporcionada por cada área, mediante mesa de ayuda o correo electrónico

Asimismo, con el fin de garantizar la integridad de la información del Instituto, se lleva a cabo una revisión del interior de mochilas, portafolios, bolsas grandes, maletas de equipaje, etc., así como del interior de las cajuelas de los vehículos que ingresan a las instalaciones.
Para el acceso a los expedientes, éstos se encuentran debidamente resguardados en archiveros bajo llave y los responsables de los archivos de cada Coordinación son quienes tienen el control de estas llaves.

17. Perfiles de usuario y contraseña

Para el acceso al sistema SAP, cada usuario tiene una cuenta de acceso con una contraseña personal, administrada por la Dirección Divisional de Sistemas y Tecnología de la Información y para el acceso a los expedientes de personal, éstos se encuentran debidamente resguardados con acceso restringido solo para personal autorizado en archiveros bajo llave y los responsables de los archivos de cada Coordinación son quienes tienen el control de estas llaves.

18. Bitácoras de acceso y operación cotidiana, seguridad aplicable (señalar con una X, según corresponda)

	Soporte físico	No se cuenta con bitácoras, en virtud de que, en caso de préstamos de expedientes, son solicitados por medio de oficio con la información y/o documentación que soporte el motivo de la solicitud, ya sea por autoridad competente ajena al IMPI o por el Órgano Interno de Control o algún otro.
	Soporte electrónico	No se cuenta con soporte electrónico de los expedientes físicos del personal, en cuanto al SAP la información se alberga en el Servidor Institucional que se encuentra y es administrado por la Dirección Divisional de Sistemas y Tecnología de la Información.

19. Lugar de almacenamiento de las bitácoras y tiempo de conservación y conservación de integridad

N/A

20. Registro de incidentes

No se tiene registro de incidentes, en virtud de que ningún expediente sale del archivo sin el debido oficio por medio del cual la autoridad competente lo solicite.

21. Procedimiento de respaldo y recuperación de datos

Servidores en el área de Sistemas.

22. Plan de contingencia

No se tiene implementado como tal un plan de contingencia.

23. Encargado de datos (señalar con una X, según corresponda)

Existe un prestador de servicios, persona física o moral, pública o privada ajena al IMPI que sola o conjuntamente, trate datos personales a nombre y por cuenta de este Instituto	SI		NO	X
22. Plazo de conservación de los datos personales				

0. NÚMERO Y NOMBRE DEL ÁREA O UNIDAD ADMINISTRATIVA:	600 – Dirección Divisional de Administración
1. Nombre del Sistema	**SAP (Tesorería / Viáticos).**
2. Objetivo	Guarda y conservación de información comprobatoria.
3. Fundamento Legal	Reglamento del Instituto Mexicano de la Propiedad Industrial, Artículo 19, Fracción IV
4. DATOS PERSONALES QUE CONTIENE EL SISTEMA (señalar con una X, según corresponda)	
Nombre	Para identificar a la persona
Domicilio	Para localizar a la persona fuera del Instituto en caso de ser necesario.
RFC	Para identificar como contribuyentes a las personas físicas o morales.

5. FORMA DE OBTENCIÓN DE LOS DATOS PERSONALES (señalar con una X, según corresponda)			
Directa		**Indirecta** (obtenida, creada, generada en algún otro sistema)	
Formulario físico		**Descripción:**	
Formulario electrónico	X		
Texto físico			
Texto electrónico			
Vía telefónica			
Otro			

6. Responsable del Sistema	
Nombre	Víctor Manuel Terán Arista
Cargo	Director Divisional de Administración
Teléfono	5556240400 extensión 11018
Correo electrónico	victor.teran@impi.gob.mx
Función	Administrar los Recursos Humanos, Materiales y Financieros del Instituto conforme a normatividad establecida.
Obligación	Administrar información dentro de un entorno para la administración y control de los recursos humanos, financieros y materiales del Instituto.
7. Administrador del Sistema	
Nombre	Agustín Fernando Bello Vázquez
Cargo	Director Divisional de Sistemas y Tecnología de la Información
Teléfono	5553340700 extensión 10000
Correo electrónico	agustin.bello@impi.gob.mx
Función	Administrar la Información del Sistema
Obligación	Resguardar información
8. Usuarios u Operador del Sistema	
Nombre	José Antonio Vázquez Torres
Cargo	Coordinador Departamental de Tesorería
Teléfono	5556240400 extensión 11271
Correo electrónico	jose.vazquezt@impi.gob.mx
Función	Vigilar y supervisar la recepción, otorgamiento, registro y control de datos
Obligación	Resguardar información
Nombre	Rosalba Herlinda Rodríguez Sánchez
Cargo	Supervisor Analista
Teléfono	5556240400 extensión 11035
Correo electrónico	rosalba.rodriguez@impi.gob.mx
Función	Recepción, registro y control de datos
Obligación	Resguardar información
Nombre	María Teresa Lozano Hernández
Cargo	Supervisor Analista
Teléfono	5556240400 extensión 11279
Correo electrónico	teresa.lozano@impi.gob.mx
Función	Cargar y/o alimentar de datos al sistema y/o actualizar los mismos.
Obligación	Resguardar información
Nombre	Federico Sánchez Rodríguez
Cargo	Especialista "A" en Propiedad Industrial
Teléfono	5556240400 extensión 11099
Correo electrónico	federico.sanchez@impi.gob.mx
Función	Cargar y/o alimentar de datos al sistema y/o actualizar los mismos.
Obligación	Resguardar información
Nombre	Juan Carlos Martínez Eleno
Cargo	Especialista "A" en Propiedad Industrial
Teléfono	5556240400 extensión 11022
Correo electrónico	juan.martinez@impi.gob.mx
Función	Cargar y/o alimentar de datos al sistema
Obligación	Resguardar información
Nombre	Fernando Santamaría Morales
Cargo	Especialista "B" en Propiedad Industrial
Teléfono	

Correo electrónico	fernando.santamaria@impi.gob.mx
Función	Cargar y/o alimentar de datos al sistema y/o actualizar los mismos.
Obligación	Resguardar información
Nombre	Raymundo Ramírez Jiménez
Cargo	Especialista "B" en Propiedad Industrial
Teléfono	5556240400 extensión 11271
Correo electrónico	raymundo.ramirez@impi.gob.mx
Función	Cargar y/o alimentar de datos al sistema y/o actualizar los mismos.
Obligación	Resguardar información
Nombre	Miguel Angel Reséndiz Piña
Cargo	Especialista "B" en Propiedad Industrial
Teléfono	5556240400 extensión 11271
Correo electrónico	miguel.resendiz@impi.gob.mx
Función	Cargar y/o alimentar de datos al sistema y/o actualizar los mismos.
Obligación	Resguardar información
Nombre	María de los Angeles Mariles Gutiérrez
Cargo	Ayudante Especializado en Servicios "B"
Teléfono	5556240400 extensión 11271
Correo electrónico	maria.mariles@impi.gob.mx
Función	Cargar y/o alimentar de datos al sistema y/o actualizar los mismos.
Obligación	Resguardar información
Nombre	Victor Hugo Adauto Esquivel
Cargo	Ayudante Especializado en Servicios "B"
Teléfono	5556240400 extensión 11271
Correo electrónico	victor.adauto@impi.gob.mx
Función	Cargar y/o alimentar de datos al sistema y/o actualizar los mismos.
Obligación	*Resguardar información
Nombre	Jose Carlos Vargas Morales
Cargo	Ayudante Especializado en Servicios "C"
Teléfono	5556240400 extensión 11271
Correo electrónico	jose.vargasm@impi.gob.mx
Función	Cargar y/o alimentar de datos al sistema y/o actualizar los mismos.
Obligación	Resguardar información
Nombre	Karina Ivette Cortes López
Cargo	Ayudante Especializado en Servicios "D"
Teléfono	5556240400 extensión 11271
Correo electrónico	Karina.cortes@impi.gob.mx
Función	Cargar y/o alimentar de datos al sistema y/o actualizar los mismos.
Obligación	Resguardar información

9. Tipo de soporte (señalar con una X, según corresponda)

*Electrónico		*Físico		*Ambos	X

*Descripción: Servidor y Expedientes de Personal

10. Transferencias o transmisiones de datos personales (señalar con una X, según corresponda)

*SI		NO	X

*Describir en que consiste la transferencia o transmisión

11. Portabilidad de datos (señalar con una X, según corresponda)

SI		NO	X

12. Nivel de protección que requieren los datos

Bajo

13. Actualización de la información contenida en el sistema

Eventualmente

14. Plazo de conservación de los datos personales

Histórico en Servidor

15. Medidas de Seguridad

Físicas	Se cuenta con un servicio de seguridad que es proporcionado por el Servicio de Protección Federal. El Instituto cuenta con sistemas de video-vigilancia en cada los inmuebles de Arenal y Pedregal, operando al 50% de su capacidad. Los servidores públicos deben portar en todo momento su credencial institucional, así como hacer uso del hand-punch al ingreso y salida diaria. El personal externo debe registrarse, dejar una identificación oficial, así como portar en todo

	momento el gafete de visita que le sea proporcionado en recepción. La autorización de los accesos es proporcionada por cada área, mediante mesa de ayuda o correo electrónico. Asimismo, con el fin de garantizar la integridad de la información del Instituto, se lleva a cabo una revisión del interior de mochilas, portafolios, bolsas grandes, maletas de equipaje, etc., registros en caso de ingreso con equipo de cómputo, así como del interior de las cajuelas de los vehículos que ingresan a las instalaciones. Para el acceso a los expedientes, éstos se encuentran debidamente resguardados en archiveros bajo llave y los responsables de los archivos de cada Coordinación son quienes tienen el control de estas llaves.
Administrativas	La información que se recaba en la Subdirección es en cumplimiento a la normatividad establecida en materia de contrataciones, por lo que está debidamente justificada la finalidad por la cual se recaban.
Técnicas	Clave de usuario y password para acceso a sistemas.

16. Acceso a instalaciones

Con credencial de empleado y/o Identificación oficial.

Se cuenta con un servicio de seguridad que es proporcionado por el Servicio de Protección Federal.
El Instituto cuenta con sistemas de video-vigilancia en cada los inmuebles de Arenal y Pedregal, operando al 50% de su capacidad.
Los servidores públicos deben portar en todo momento su credencial institucional, así como hacer uso del hand-punch al ingreso y salida diaria.
El personal externo debe registrarse, dejar una identificación oficial, así como portar en todo momento el gafete de visita que le sea proporcionado en recepción.
La autorización de los accesos es proporcionada por cada área, mediante mesa de ayuda o correo electrónico.
Asimismo, con el fin de garantizar la integridad de la información del Instituto, se lleva a cabo una revisión del interior de mochilas, portafolios, bolsas grandes, maletas de equipaje, etc., así como del interior de las cajuelas de los vehículos que ingresan a las instalaciones.
Para el acceso a los expedientes, éstos se encuentran debidamente resguardados en archiveros bajo llave y los responsables de los archivos de cada Coordinación son quienes tienen el control de estas llaves.

17. Perfiles de usuario y contraseña

Para el acceso al sistema SAP, cada usuario tiene una cuenta de acceso con una contraseña personal, administrada por la Dirección Divisional de Sistemas y Tecnología de la Información y para el acceso a los expedientes de personal, éstos se encuentran debidamente resguardados con acceso restringido solo para personal autorizado en archiveros bajo llave y los responsables de los archivos de cada Coordinación son quienes tienen el control de estas llaves.

18. Bitácoras de acceso y operación cotidiana, seguridad aplicable (señalar con una X, según corresponda)

	Soporte físico	No se cuenta con bitácoras, en virtud de que, en caso de préstamos de expedientes, son solicitados por medio de oficio con la información y/o documentación que soporte el motivo de la solicitud, ya sea por autoridad competente ajena al IMPI o por el Órgano Interno de Control o algún otro.
	Soporte electrónico	No se cuenta con soporte electrónico de los expedientes físicos del personal, en cuanto al SAP la información se alberga en el Servidor Institucional que se encuentra y es administrado por la Dirección Divisional de Sistemas y Tecnología de la Información.

19. Lugar de almacenamiento de las bitácoras y tiempo de conservación y conservación de integridad

N/A

20. Registro de incidentes

No se tiene registro de incidentes, en virtud de que ningún expediente sale del archivo sin el debido oficio por medio del cual la autoridad competente lo solicite.

21. Procedimiento de respaldo y recuperación de datos

Servidores en el área de Sistemas.

22. Plan de contingencia

No se tiene implementado como tal un plan de contingencia.

23. Encargado de datos (señalar con una X, según corresponda)

Existe un prestador de servicios, persona física o moral, pública o privada ajena al IMPI que sola o conjuntamente, trate datos personales a nombre y por cuenta de este Instituto	SI		NO	X
22. Plazo de conservación de los datos personales				

0. NÚMERO Y NOMBRE DEL ÁREA O UNIDAD ADMINISTRATIVA			
1. Nombre del Sistema	SAP / Expedientes de Contratación		
2. Objetivo	Documentar los procesos de contratación que se llevan a cabo en el Instituto		
3. Fundamento Legal	Artículos: 19 del Reglamento del IMPI; 23 de la LGTAIPG; 1 de la LGPDPPSO		
4. DATOS PERSONALES QUE CONTIENE EL SISTEMA (señalar con una X, según corresponda)			
Dato personal	Idoneidad (informar para que se recaba el dato)		
Datos personales contenidos en la identificación oficial presentada por la persona física (CURP, Clave de elector, número de pasaporte, etc.)	Para identificar a la persona		
Datos personales contenidos en documento para acreditar personalidad del representante (CURP, Clave de elector, número de pasaporte, etc.)	Para identificar a la persona		
Títulos o constancias profesionales	Para acreditar nivel de estudios, en aquellos casos en que el tipo de contratación lo requiera		
Datos patrimoniales (Cuentas bancarias, información fiscal, ingresos, etc.)	Para llevar a cabo pagos en caso de que se formalice algún contrato; acreditar ingresos, en aquellos casos en que el tipo de contratación lo requiera; etc.		
Datos personales contenidos en Acta de nacimiento (Fecha y lugar de nacimiento, nacionalidad, etc.)	Para integrar la documentación necesaria para la formalización de los contratos. Para acreditar nacionalidad, en aquellos casos en que el tipo de contratación lo requiera		
5. FORMA DE OBTENCIÓN DE LOS DATOS PERSONALES (señalar con una X, según corresponda)			
Directa		**Indirecta** (obtenida, creada, generada en algún otro sistema)	
Formulario físico		**Descripción:** La documentación en la que se contienen los datos personales también es recibida por medio del Sistema Electrónico CompraNet, a través del cual las personas físicas o morales que participan en los procesos de contratación envían su información	
Formulario electrónico			
Texto físico	X		
Texto electrónico	X		
Vía telefónica			
Otro			
6. Responsable del Sistema			
Nombre	**Víctor Manuel Terán Arista**		
Cargo	**Director Divisional de Administración**		
Teléfono	5556240400 ext. 11018		
Correo electrónico	**victor.teran@impi.gob.mx**		
Función	Realizar las adquisiciones, arrendamientos y la contratación de servicios del Instituto		
Obligación	Transparentar y permitir el acceso a su información y proteger los datos personales que obren en su poder		
7. Administrador del Sistema			
Nombre	**Jaime Arturo Olivares Lamadrid**		
Cargo	**Subdirector Divisional de Recursos Materiales y Servicios Generales**		
Teléfono	5556240400 ext. 11021		
Correo electrónico	**Jaime.olivares@impi.gob.mx**		
Función	Llevar a cabo los procesos de contratación en el Instituto		
Obligación	Resguardo de la información contenida en los expedientes de contratación, así como transparentar y permitir el acceso a ésta, protegiendo los datos personales que obren en su poder		
8. Usuarios u Operador del Sistema			
Nombre	**Alejandro Gabriel Tovar Guzmán**		
Cargo	**Coordinador Departamental de Adquisiciones**		
Teléfono	5556240400 ext. 11023		
Correo electrónico	**alejandro.tovar@impi.gob.mx**		
Función	Llevar a cabo los procesos de contratación en el Instituto		
Obligación	Recabar la información necesaria para llevar a cabo los procesos de contratación asignados, así como el resguardo de la información contenida en los expedientes de contratación.		
Nombre	**Albany Sosa Salas**		
Cargo	**Coordinadora Departamental de Servicios Generales**		
Teléfono	5556240400 ext. 11024		
Correo electrónico	**albany.sosa@impi.gob.mx**		

Función	Participación en los procesos de contratación en materia de servicios generales en el Instituto
Obligación	Recabar y/o analizar la información necesaria para llevar a cabo los procesos de contratación en materia de servicios generales
Nombre	**Clara Soler Aguilar**
Cargo	**Especialista "A" en Propiedad Industrial**
Teléfono	56240400 ext. 11788
Correo electrónico	**clara.soler@impi.gob.mx**
Función	Llevar a cabo los procesos de contratación que le son asignados
Obligación	Recabar la información necesaria para llevar a cabo los procesos de contratación asignados
Nombre	**Ma. De los Ángeles Torres Herrera**
Cargo	**Especialista "A" en Propiedad Industrial**
Teléfono	56240400 ext. 11275
Correo electrónico	**angeles.torres@impi.gob.mx**
Función	Llevar a cabo los procesos de contratación que le son asignados
Obligación	Recabar la información necesaria para llevar a cabo los procesos de contratación asignados
Nombre	**Samanta Valderrama Burgos**
Cargo	**Especialista "A" en Propiedad Industrial**
Teléfono	56240400 ext. 11701
Correo electrónico	**samanta.valderrama@impi.gob.mx**
Función	Llevar a cabo los procesos de contratación que le son asignados
Obligación	Recabar la información necesaria para llevar a cabo los procesos de contratación asignados
Nombre	**César Huerta Gómez**
Cargo	**Especialista "A" en Propiedad Industrial**
Teléfono	56240400 ext. 11277
Correo electrónico	**cesar.huerta@impi.gob.mx**
Función	Llevar a cabo los procesos de contratación que le son asignados
Obligación	Recabar la información necesaria para llevar a cabo los procesos de contratación asignados
Nombre	**Leticia Calderón Fuentes**
Cargo	**Especialista "A" en Propiedad Industrial**
Teléfono	56240400 ext. 11275
Correo electrónico	**leticia.calderon@impi.gob.mx**
Función	Llevar a cabo los procesos de contratación que le son asignados
Obligación	Recabar la información necesaria para llevar a cabo los procesos de contratación asignados
Nombre	**María Elena López Jiménez**
Cargo	**Especialista "B" en Propiedad Industrial**
Teléfono	56240400 ext. 11788
Correo electrónico	**maria.lopez@impi.gob.mx**
Función	Llevar a cabo los procesos de contratación que le son asignados
Obligación	Recabar la información necesaria para llevar a cabo los procesos de contratación asignados
Nombre	**Jorge Vilchis Esquivel**
Cargo	**Especialista "A" en Propiedad Industrial**
Teléfono	56240400 ext. 11275
Correo electrónico	**jorge.vilchis@impi.gob.mx**
Función	Resguardo de la documentación relativa a los procesos de contratación
Obligación	Resguardar la documentación que obra en los expedientes de los procesos de contratación

9. Tipo de soporte (señalar con una X, según corresponda)

*Electrónico		*Físico		*Ambos	**X**

*Descripción: Los documentos en los que se contienen los datos personales obran en los expedientes de contratación y se reciben tanto de manera física como electrónica a través de correos electrónicos o mediante el sistema CompraNet

10. Transferencias o transmisiones de datos personales (señalar con una X, según corresponda)

*SI		NO	X

*Describir en que consiste la transferencia o transmisión

11. Portabilidad de datos (señalar con una X, según corresponda)

SI		NO	X

12. Nivel de protección que requieren los datos

En los expedientes de contratación se cuenta con documentos que contienen datos personales tanto de nivel básico como de nivel medio

13. Actualización de la información contenida en el sistema

No se tiene como tal establecido un periodo de actualización de la información tanto en el SAP como en los expedientes, ya que la información se va integrando conforme se recibe, de acuerdo a los procesos de contratación que se realizan

14. Plazo de conservación de los datos personales

Los expedientes de contratación tienen una vigencia de 6 años establecida en el Catálogo de Disposición Documental

15. Medidas de Seguridad

Físicas	Se cuenta con un servicio de seguridad que es proporcionado por el Servicio de Protección Federal. El Instituto cuenta con sistemas de video-vigilancia en cada los inmuebles de Arenal y Pedregal, operando al 50% de su capacidad. Los servidores públicos deben portar en todo momento su credencial institucional, así como hacer uso del hand-punch al ingreso y salida diaria. El personal externo debe registrarse, dejar una identificación oficial, así como portar en todo momento el gafete de visita que le sea proporcionado en recepción. La autorización de los accesos es proporcionada por cada área, mediante mesa de ayuda o correo electrónico. Asimismo, con el fin de garantizar la integridad de la información del Instituto, se lleva a cabo una revisión del interior de mochilas, portafolios, bolsas grandes, maletas de equipaje, etc., registros en caso de ingreso con equipo de cómputo, así como del interior de las cajuelas de los vehículos que ingresan a las instalaciones. Para el acceso a los expedientes, éstos se encuentran debidamente resguardados en archiveros bajo llave y los responsables de los archivos de cada Coordinación son quienes tienen el control de estas llaves.
Administrativas	La información que se recaba en la Subdirección es en cumplimiento a la normatividad establecida en materia de contrataciones, por lo que está debidamente justificada la finalidad por la cual se recaban.
Técnicas	Clave de usuario y password para acceso a sistemas.

16. Acceso a instalaciones

Se cuenta con un servicio de seguridad que es proporcionado por el Servicio de Protección Federal.
El Instituto cuenta con sistemas de video-vigilancia en cada los inmuebles de Arenal y Pedregal, operando al 50% de su capacidad.
Los servidores públicos deben portar en todo momento su credencial institucional, así como hacer uso del hand-punch al ingreso y salida diaria.
El personal externo debe registrarse, dejar una identificación oficial, así como portar en todo momento el gafete de visita que le sea proporcionado en recepción.
La autorización de los accesos es proporcionada por cada área, mediante mesa de ayuda o correo electrónico.
Asimismo, con el fin de garantizar la integridad de la información del Instituto, se lleva a cabo una revisión del interior de mochilas, portafolios, bolsas grandes, maletas de equipaje, etc., así como del interior de las cajuelas de los vehículos que ingresan a las instalaciones.

Para el acceso a los expedientes, éstos se encuentran debidamente resguardados en archiveros bajo llave y los responsables de los archivos de cada Coordinación son quienes tienen el control de estas llaves.

17. Perfiles de usuario y contraseña

Para el acceso al sistema SAP, cada usuario tiene una cuenta de acceso con una contraseña personal, y para el acceso a los expedientes, éstos se encuentran debidamente resguardados en archiveros bajo llave y los responsables de los archivos de cada Coordinación son quienes tienen el control de estas llaves.

18. Bitácoras de acceso y operación cotidiana, seguridad aplicable (señalar con una X, según corresponda)

	Soporte físico	No se cuenta con bitácoras, sin embargo, si los expedientes son solicitados por alguna persona ajena a la Subdirección, generalmente se realiza a través de oficio y se entregan de la misma forma.
	Soporte electrónico	Servidores en el área de Sistemas.

19. Lugar de almacenamiento de las bitácoras y tiempo de conservación y conservación de integridad

No se cuenta con bitácoras

20. Registro de incidentes

Los incidentes en cuestión del soporte físico, se registrarán mediante actas administrativas, en caso de pérdida o destrucción de expedientes.

21. Procedimiento de respaldo y recuperación de datos

Como respaldo de la información que obra en los expedientes, se tienen escaneados en soporte electrónico los contratos y sus anexos de cada uno de los expedientes, así como los documentos que fueron recibidos mediante correo electrónico o a través del Sistema Electrónico CompraNet.				
22. Plan de contingencia				
No se tiene implementado como tal un plan de contingencia.				
23. Encargado de datos (señalar con una X, según corresponda)				
Existe un prestador de servicios, persona física o moral, pública o privada ajena al IMPI que sola o conjuntamente, trate datos personales a nombre y por cuenta de este Instituto	SI		NO	**X**
22. Plazo de conservación de los datos personales				

0. NÚMERO Y NOMBRE DEL ÁREA O UNIDAD ADMINISTRATIVA:	600 – Dirección Divisional de Administración
1. Nombre del Sistema	**SAP (presupuesto)**
2. Objetivo	Guarda y conservación de información de registros en el sistema SAP.
3. Fundamento Legal	Reglamento del Instituto Mexicano de la Propiedad Industrial, Artículo 19, Fracción II, IV y V

4. DATOS PERSONALES QUE CONTIENE EL SISTEMA (señalar con una X, según corresponda)	
Nombre	Para identificar a la persona

5. FORMA DE OBTENCIÓN DE LOS DATOS PERSONALES (señalar con una X, según corresponda)			
Directa		**Indirecta** (obtenida, creada, generada en algún otro sistema)	
Formulario físico		**Descripción:**	
Formulario electrónico	**X**		
Texto físico			
Texto electrónico			
Vía telefónica			
Otro			

6. Responsable del Sistema	
Nombre	Víctor Manuel Terán Arista
Cargo	Director Divisional de Administración
Teléfono	5556240400 extensión 11018
Correo electrónico	victor.teran@impi.gob.mx
Función	Administrar los Recursos Humanos, Materiales y Financieros del Instituto conforme a normatividad establecida.
Obligación	Administrar información dentro de un entorno para la administración y control de los recursos humanos, financieros y materiales del Instituto.

7. Administrador del Sistema	
Nombre	Agustín Fernando Bello Vázquez
Cargo	Director Divisional de Sistemas y Tecnología de la Información
Teléfono	5553340700 extensión 10000
Correo electrónico	agustin.bello@impi.gob.mx
Función	Administrar la Información del Sistema
Obligación	Resguardar información

8. Usuarios u Operador del Sistema	
Nombre	Marco Aurelio Torres Moreno
Cargo	Coordinador Departamental de Presupuesto
Teléfono	5556240400 extensión 11034
Correo electrónico	marco.torres@impi.gob.mx
Función	Vigilar y supervisar la recepción, otorgamiento, registro y control de datos
Obligación	Resguardar información
Nombre	Rodrigo Armando Guerrero Castro
Cargo	Especialista "A" en Propiedad Industrial
Teléfono	5556240400 extensión 11272
Correo electrónico	rodrigo.guerrero@impi.gob.mx
Función	Recepción, registro y control de datos
Obligación	Resguardar información
Nombre	Miguel Angel Reséndiz Piña
Cargo	Especialista "B" en Propiedad Industrial
Teléfono	5556240400 extensión 11034
Correo electrónico	miguel.resendiz@impi.gob.mx
Función	Cargar y/o alimentar de datos al sistema y/o actualizar los mismos.
Obligación	Resguardar información
Nombre	Jose Carlos Vargas Morales
Cargo	Ayudante Especializado en Servicios "C"
Teléfono	5556240400 extensión 11034
Correo electrónico	jose.vargasm@impi.gob.mx
Función	Cargar y/o alimentar de datos al sistema y/o actualizar los mismos.
Obligación	Resguardar información

9. Tipo de soporte (señalar con una X, según corresponda)					
*Electrónico	**X**	*Físico		*Ambos	
*Descripción: Servidor y Expedientes de Personal					

10. Transferencias o transmisiones de datos personales (señalar con una X, según corresponda)			
*SI		NO	**X**
*Describir en que consiste la transferencia o transmisión			

11. Portabilidad de datos (señalar con una X, según corresponda)			
SI		NO	**X**

12. Nivel de protección que requieren los datos

Bajo

13. Actualización de la información contenida en el sistema

Quincenalmente en los datos que requieran actualización.

14. Plazo de conservación de los datos personales

Histórico en Servidor

15. Medidas de Seguridad

Físicas	Se cuenta con un servicio de seguridad que es proporcionado por el Servicio de Protección Federal. El Instituto cuenta con sistemas de video-vigilancia en cada los inmuebles de Arenal y Pedregal, operando al 50% de su capacidad. Los servidores públicos deben portar en todo momento su credencial institucional, así como hacer uso del hand-punch al ingreso y salida diaria. El personal externo debe registrarse, dejar una identificación oficial, así como portar en todo momento el gafete de visita que le sea proporcionado en recepción. La autorización de los accesos es proporcionada por cada área, mediante mesa de ayuda o correo electrónico. Asimismo, con el fin de garantizar la integridad de la información del Instituto, se lleva a cabo una revisión del interior de mochilas, portafolios, bolsas grandes, maletas de equipaje, etc., registros en caso de ingreso con equipo de cómputo, así como del interior de las cajuelas de los vehículos que ingresan a las instalaciones. Para el acceso a los expedientes, éstos se encuentran debidamente resguardados en archiveros bajo llave y los responsables de los archivos de cada Coordinación son quienes tienen el control de estas llaves.
Administrativas	La información que se recaba en la Subdirección es en cumplimiento a la normatividad establecida en materia de contrataciones, por lo que está debidamente justificada la finalidad por la cual se recaban.
Técnicas	Clave de usuario y password para acceso a sistemas.

16. Acceso a instalaciones

Con credencial de empleado y/o Identificación oficial.
Se cuenta con un servicio de seguridad que es proporcionado por el Servicio de Protección Federal.
El Instituto cuenta con sistemas de video-vigilancia en cada los inmuebles de Arenal y Pedregal, operando al 50% de su capacidad.
Los servidores públicos deben portar en todo momento su credencial institucional, así como hacer uso del hand-punch al ingreso y salida diaria.
El personal externo debe registrarse, dejar una identificación oficial, así como portar en todo momento el gafete de visita que le sea proporcionado en recepción.
La autorización de los accesos es proporcionada por cada área, mediante mesa de ayuda o correo electrónico.
Asimismo, con el fin de garantizar la integridad de la información del Instituto, se lleva a cabo una revisión del interior de mochilas, portafolios, bolsas grandes, maletas de equipaje, etc., así como del interior de las cajuelas de los vehículos que ingresan a las instalaciones.
Para el acceso a los expedientes, éstos se encuentran debidamente resguardados en archiveros bajo llave y los responsables de los archivos de cada Coordinación son quienes tienen el control de estas llaves.

17. Perfiles de usuario y contraseña

Para el acceso al sistema SAP, cada usuario tiene una cuenta de acceso con una contraseña personal, administrada por la Dirección Divisional de Sistemas y Tecnología de la Información y para el acceso a los expedientes de personal, éstos se encuentran debidamente resguardados con acceso restringido solo para personal autorizado en archiveros bajo llave y los responsables de los archivos de cada Coordinación son quienes tienen el control de estas llaves.

18. Bitácoras de acceso y operación cotidiana, seguridad aplicable (señalar con una X, según corresponda)

	Soporte físico	No se cuenta con bitácoras, en virtud de que, en caso de préstamos de expedientes, son solicitados por medio de oficio con la información y/o documentación que soporte el motivo de la solicitud, ya sea por autoridad competente ajena al IMPI o por el Órgano Interno de Control o algún otro.
	Soporte electrónico	No se cuenta con soporte electrónico de los expedientes físicos del personal, en cuanto al SAP la información se alberga en el Servidor Institucional que se encuentra y es administrado por la Dirección Divisional de Sistemas y Tecnología de la Información.

19. Lugar de almacenamiento de las bitácoras y tiempo de conservación y conservación de integridad

N/A

20. Registro de incidentes

No se tiene registro de incidentes, en virtud de que ningún expediente sale del archivo sin el debido oficio por medio del cual la autoridad competente lo solicite.

21. Procedimiento de respaldo y recuperación de datos

Servidores en el área de Sistemas.				
22. Plan de contingencia				
No se tiene implementado como tal un plan de contingencia.				
23. Encargado de datos (señalar con una X, según corresponda)				
Existe un prestador de servicios, persona física o moral, pública o privada ajena al IMPI que sola o conjuntamente, trate datos personales a nombre y por cuenta de este Instituto	SI		NO	**X**
22. Plazo de conservación de los datos personales				

0. NÚMERO Y NOMBRE DEL ÁREA O UNIDAD ADMINISTRATIVA:	600 – Dirección Divisional de Administración
1. Nombre del Sistema	**SAP**
2. Objetivo	Administración de Recursos Humanos, Materiales y Financieros.
3. Fundamento Legal	Artículo 19 del Reglamento del Instituto Mexicano de la Propiedad Industrial.
4. DATOS PERSONALES QUE CONTIENE EL SISTEMA (señalar con una X, según corresponda)	
Nombre	Para identificar a la persona
Titulo (Nivel de estudios)	Para conocer nivel de estudios
Fotografía	Para identificar a la persona
Domicilio	Para localizar a la persona fuera del Instituto en caso de ser necesario.
Teléfono	Para localizar a la persona fuera del Instituto en caso de ser necesario..
RFC	Para identificar como contribuyentes a las personas físicas o morales.
CURP	Para identificar oficialmente tanto a residentes como a ciudadanos mexicanos de todo el país.
Fecha de Nacimiento	Para conocer edad de la personal.
Lugar de Nacimiento	Para conocer lugar de nacimiento.
País de Nacimiento	Para conocer país de naciimienr.to.
Nacionalidad	Para en caso de extranjeros solicitar documentos migratorios
Estado Civil	Para fines estadísticos
Huella dactilar	Para registrar entrada y salida de horario de labores
Tipo de sangre	Dato necesario en caso de urgencias médicas.
Peso	Para conocer estado de salud.
Estatura	Para conocer estado de salud.
Temperatura	Para conocer estado de salud.
Presión arterial	Para conocer estado de salud.
Frecuencia cardiaca	Para conocer estado de salud.

5. FORMA DE OBTENCIÓN DE LOS DATOS PERSONALES (señalar con una X, según corresponda)			
Directa		**Indirecta** (obtenida, creada, generada en algún otro sistema)	
Formulario físico	X	**Descripción:**	
Formulario electrónico			
Texto físico	X		
Texto electrónico			
Vía telefónica			
Otro			

6. Responsable del Sistema	
Nombre	Víctor Manuel Terán Arista
Cargo	Director Divisional de Administración
Teléfono	5556240400 extensión 11018
Correo electrónico	victor.teran@impi.gob.mx
Función	Administrar los Recursos Humanos, Materiales y Financieros del Instituto conforme a normatividad establecida.
Obligación	Administrar información dentro de un entorno para la administración y control de los recursos humanos, financieros y materiales del Instituto.
7. Administrador del Sistema	
Nombre	Agustín Fernando Bello Vázquez
Cargo	Director Divisional de Sistemas y Tecnología de la Información
Teléfono	5553340700 extensión 10000
Correo electrónico	agustin.bello@impi.gob.mx
Función	Administrar la Información del Sistema
Obligación	Resguardar información
8. Usuarios u Operador del Sistema	
Nombre	Carlos Jesús Oviedo Laguna
Cargo	Subdirector Divisional de Recursos Humanos
Teléfono	5556240400 extensión 11113
Correo electrónico	carlos.oviedo@impi.gob.mx
Función	Vigilar la recepción, registro y control de datos
Obligación	Resguardar información
Nombre	Saúl Javier Ríos Marmolejo
Cargo	Coordinador Departamental de Nómina
Teléfono	5556240400 extensión 11037
Correo electrónico	saul.rios@impi.gob.mx
Función	Coordinar la recepción, registro y control de datos
Obligación	Resguardar información
Nombre	Miguel Ángel Arredondo Huerta
Cargo	Especialista "A" en Propiedad Industrial
Teléfono	5556240400 extensión 11896
Correo electrónico	miguel.arredondo@impi.gob.mx
Función	Cargar y/o alimentar de datos al sistema y/o actualizar los mismos.

Obligación	Soporte Técnico
Nombre	Benjamín Rivera Lorenzo
Cargo	Especialista "B" en Propiedad Industrial
Teléfono	5556240400 extensión 11896
Correo electrónico	benjamin.rivera@impi.gob.mx
Función	Cargar y/o alimentar de datos al sistema y/o actualizar los mismos.
Obligación	Soporte Técnico
Nombre	Gloria Del Razo Contreras
Cargo	Especialista "A" en Propiedad Industrial
Teléfono	5556240400 extensión 11264
Correo electrónico	gloria.delrazo@impi.gob.mx
Función	Cargar y/o alimentar de datos al sistema
Obligación	Cargar y/o alimentar de datos al sistema y/o actualizar los mismos.
Nombre	María De Los Ángeles Perez Cárdenas
Cargo	Especialista "B" en Propiedad Industrial
Teléfono	5556240400 extensión 11264
Correo electrónico	maria.perez@impi.gob.mx
Función	Cargar y/o alimentar de datos al sistema y/o actualizar los mismos.
Obligación	Concentrar información
Nombre	Melo Luis Enrique Rossell Rivera
Cargo	Especialista "B" en Propiedad Industrial
Teléfono	5556240400 extensión 11036
Correo electrónico	melo.rossell@impi.gob.mx
Función	Cargar y/o alimentar de datos al sistema y/o actualizar los mismos.
Obligación	Concentrar información
Nombre	Luz Del Carmen Ramírez Palacios
Cargo	Ayudante Especializado en Servicios "A"
Teléfono	5556240400 extensión 11036
Correo electrónico	luz.ramirez@impi.gob.mx
Función	Cargar y/o alimentar de datos al sistema y/o actualizar los mismos.
Obligación	Concentrar información
Nombre	David Rivera Fuentes
Cargo	Especialista "A" en Propiedad Industrial
Teléfono	5556240400 extensión 11033
Correo electrónico	david.rivera@impi.gob.mx
Función	Cargar y/o alimentar de datos al sistema
Obligación	Cargar y/o alimentar de datos al sistema y/o actualizar los mismos.
Nombre	Alejandro Ibarra Martínez
Cargo	Especialista "B" en Propiedad Industrial
Teléfono	5553340700 extensión 10409
Correo electrónico	alejandro.ibarra@impi.gob.mx
Función	Cargar y/o alimentar de datos al sistema y/o actualizar los mismos.
Obligación	Concentrar información
Nombre	Nury Alba González
Cargo	Secretaria Ejecutiva
Teléfono	5553340700 extensión 10409
Correo electrónico	nury.alba@impi.gob.mx
Función	Cargar y/o alimentar de datos al sistema y/o actualizar los mismos.
Obligación	Concentrar información
Nombre	Mara Erika Vega Ibarra
Cargo	Coordinador Departamental de Selección, Reclutamiento y Capacitación
Teléfono	5556240400 extensión 11016
Correo electrónico	mara.vega@impi.gob.mx
Función	Coordinar la recepción, registro y control de datos
Obligación	Resguardar información
Nombre	Ana Lilia Carmona Serrano
Cargo	Especialista "A" en Propiedad Industrial
Teléfono	5556240400 extensión 11847
Correo electrónico	ana.carmona@impi.gob.mx
Función	Cargar y/o alimentar de datos al sistema
Obligación	Cargar y/o alimentar de datos al sistema y/o actualizar los mismos.
Nombre	Alma Lilia Morales Guzmán
Cargo	Especialista "B" en Propiedad Industrial
Teléfono	5556240400 extensión 11847
Correo electrónico	alma.morales@impi.gob.mx
Función	Cargar y/o alimentar de datos al sistema y/o actualizar los mismos.
Obligación	Concentrar información

Nombre	Alfonso Morales Huerta
Cargo	Ayudante Especializado en Servicios "A"
Teléfono	5556240400 extensión 11847
Correo electrónico	alfonso.morales@impi.gob.mx
Función	Cargar y/o alimentar de datos al sistema
Obligación	Cargar y/o alimentar de datos al sistema y/o actualizar los mismos.
Nombre	Gloria Ruiz Rangel
Cargo	Especialista "A" en Propiedad Industrial
Teléfono	5556240400 extensión 11258
Correo electrónico	gloria.ruiz@impi.gob.mx
Función	Cargar y/o alimentar de datos al sistema
Obligación	Cargar y/o alimentar de datos al sistema y/o actualizar los mismos.

9. Tipo de soporte (señalar con una X, según corresponda)

*Electrónico		*Físico		*Ambos	X

*Descripción: Servidor y Expedientes de Personal

10. Transferencias o transmisiones de datos personales (señalar con una X, según corresponda)

*SI		NO	X

*Describir en que consiste la transferencia o transmisión

11. Portabilidad de datos (señalar con una X, según corresponda)

SI		NO	X

12. Nivel de protección que requieren los datos

Bajo en datos personales y alto en datos de salud.

13. Actualización de la información contenida en el sistema

Quincenalmente en los datos que requieran actualización.

14. Plazo de conservación de los datos personales

Histórico en Servidor y 30 años en papel. (Expedientes de Personal)

15. Medidas de Seguridad

Físicas	Se cuenta con un servicio de seguridad que es proporcionado por el Servicio de Protección Federal. El Instituto cuenta con sistemas de video-vigilancia en cada los inmuebles de Arenal y Pedregal, operando al 50% de su capacidad. Los servidores públicos deben portar en todo momento su credencial institucional, así como hacer uso del hand-punch al ingreso y salida diaria. El personal externo debe registrarse, dejar una identificación oficial, así como portar en todo momento el gafete de visita que le sea proporcionado en recepción. La autorización de los accesos es proporcionada por cada área, mediante mesa de ayuda o correo electrónico. Asimismo, con el fin de garantizar la integridad de la información del Instituto, se lleva a cabo una revisión del interior de mochilas, portafolios, bolsas grandes, maletas de equipaje, etc., registros en caso de ingreso con equipo de cómputo, así como del interior de las cajuelas de los vehículos que ingresan a las instalaciones. Para el acceso a los expedientes, éstos se encuentran debidamente resguardados en archiveros bajo llave y los responsables de los archivos de cada Coordinación son quienes tienen el control de estas llaves.
Administrativas	La información que se recaba en cumplimiento a la normatividad establecida en materia de Recursos Humanos, por lo que está debidamente justificada la finalidad por la cual se recaban.
Técnicas	Clave de usuario y password para acceso a sistemas.

16. Acceso a instalaciones

Con credencial de empleado y/o Identificación oficial.

Se cuenta con un servicio de seguridad que es proporcionado por el Servicio de Protección Federal.
El Instituto cuenta con sistemas de video-vigilancia en cada los inmuebles de Arenal y Pedregal, operando al 50% de su capacidad.
Los servidores públicos deben portar en todo momento su credencial institucional, así como hacer uso del hand-punch al ingreso y salida diaria.
El personal externo debe registrarse, dejar una identificación oficial, así como portar en todo momento el gafete de visita que le sea proporcionado en recepción.
La autorización de los accesos es proporcionada por cada área, mediante mesa de ayuda o correo electrónico.
Asimismo, con el fin de garantizar la integridad de la información del Instituto, se lleva a cabo una revisión del interior de mochilas, portafolios, bolsas grandes, maletas de equipaje, etc., así como del interior de las cajuelas de los vehículos que ingresan a las instalaciones.
Para el acceso a los expedientes, éstos se encuentran debidamente resguardados en archiveros bajo llave y los responsables de los archivos de cada Coordinación son quienes tienen el control de estas llaves.

17. Perfiles de usuario y contraseña

Para el acceso al sistema SAP, cada usuario tiene una cuenta de acceso con una contraseña personal, administrada por la Dirección Divisional de Sistemas y Tecnología de la Información y para el acceso a los expedientes de personal, éstos se encuentran debidamente resguardados con acceso restringido solo para personal autorizado en archiveros bajo llave y los responsables de los archivos de cada Coordinación son quienes tienen el control de estas llaves.		
18. Bitácoras de acceso y operación cotidiana, seguridad aplicable (señalar con una X, según corresponda)		
	Soporte físico	No se cuenta con bitácoras, en virtud de que, en caso de préstamos de expedientes de personal, son solicitados por medio de oficio con la información y/o documentación que soporte el motivo de la solicitud, ya sea por autoridad competente ajena al IMPI o por el Órgano Interno de Control o algún otro.
	Soporte electrónico	No se cuenta con soporte electrónico de los expedientes físicos del personal, en cuanto al SAP la información se alberga en el Servidor Institucional que se encuentra y es administrado por la Dirección Divisional de Sistemas y Tecnología de la Información.
19. Lugar de almacenamiento de las bitácoras y tiempo de conservación y conservación de integridad		
N/A		
20. Registro de incidentes		
No se tiene registro de incidentes, en virtud de que ningún expediente sale del archivo sin el debido oficio por medio del cual la autoridad competente lo solicite.		
21. Procedimiento de respaldo y recuperación de datos		
Servidores en el área de Sistemas.		
22. Plan de contingencia		
No se tiene implementado como tal un plan de contingencia.		

23. Encargado de datos (señalar con una X, según corresponda)				
Existe un prestador de servicios, persona física o moral, pública o privada ajena al IMPI que sola o conjuntamente, trate datos personales a nombre y por cuenta de este Instituto	SI		NO	**X**
22. Plazo de conservación de los datos personales				

0. NÚMERO Y NOMBRE DEL ÁREA O UNIDAD ADMINISTRATIVA:	600 – Dirección Divisional de Administración		
1. Nombre del Sistema	**SAP (Nomina)**		
2. Objetivo	Administración de la Nomina		
3. Fundamento Legal	Artículo 19 del Reglamento del Instituto Mexicano de la Propiedad Industrial		
4. DATOS PERSONALES QUE CONTIENE EL SISTEMA (señalar con una X, según corresponda)			
Nombre	Para identificar a la persona		
Titulo (Nivel de estudios)	Para conocer nivel de estudios		
Fotografía	Para identificar a la persona		
Domicilio	Para localizar a la persona fuera del Instituto en caso de ser necesario.		
Teléfono	Para localizar a la persona fuera del Instituto en caso de ser necesario..		
RFC	Para identificar como contribuyentes a las personas físicas o morales.		
CURP	Para identificar oficialmente tanto a residentes como a ciudadanos mexicanos de todo el país.		
Fecha de Nacimiento	Para conocer edad de la personal.		
Lugar de Nacimiento	Para conocer lugar de nacimiento.		
País de Nacimiento	Para conocer país de naciimienr.to.		
Nacionalidad	Para en caso de extranjeros solicitar documentos migratorios		
Estado Civil	Para fines estadísticos		
5. FORMA DE OBTENCIÓN DE LOS DATOS PERSONALES (señalar con una X, según corresponda)			
Directa		**Indirecta** (obtenida, creada, generada en algún otro sistema)	
Formulario físico	X	**Descripción:**	
Formulario electrónico			
Texto físico	X		
Texto electrónico			
Vía telefónica			
Otro			
6. Responsable del Sistema			
Nombre	Víctor Manuel Terán Arista		
Cargo	Director Divisional de Administración		
Teléfono	5556240400 extensión 11018		
Correo electrónico	victor.teran@impi.gob.mx		
Función	Administrar los Recursos Humanos, Materiales y Financieros del Instituto conforme a normatividad establecida.		
Obligación	Administrar información dentro de un entorno para la administración y control de los recursos humanos, financieros y materiales del Instituto.		
7. Administrador del Sistema			
Nombre	Agustín Fernando Bello Vázquez		
Cargo	Director Divisional de Sistemas y Tecnología de la Información		
Teléfono	5553340700 extensión 10000		
Correo electrónico	agustin.bello@impi.gob.mx		
Función	Administrar la Información del Sistema		
Obligación	Resguardar información		
8. Usuarios u Operador del Sistema			
Nombre	Carlos Jesús Oviedo Laguna		
Cargo	Subdirector Divisional de Recursos Humanos		
Teléfono	5556240400 extensión 11113		
Correo electrónico	carlos.oviedo@impi.gob.mx		
Función	Vigilar la recepción, registro y control de datos		
Obligación	Resguardar información		
Nombre	Saúl Javier Ríos Marmolejo		
Cargo	Coordinador Departamental de Nómina		
Teléfono	5556240400 extensión 11037		
Correo electrónico	saul.rios@impi.gob.mx		
Función	Coordinar la recepción, registro y control de datos		
Obligación	Resguardar información		
Nombre	Miguel Ángel Arredondo Huerta		
Cargo	Especialista "A" en Propiedad Industrial		
Teléfono	5556240400 extensión 11896		
Correo electrónico	miguel.arredondo@impi.gob.mx		
Función	Cargar y/o alimentar de datos al sistema y/o actualizar los mismos.		
Obligación	Soporte Técnico		
Nombre	Benjamín Rivera Lorenzo		
Cargo	Especialista "B" en Propiedad Industrial		
Teléfono	5556240400 extensión 11896		
Correo electrónico	benjamin.rivera@impi.gob.mx		
Función	Cargar y/o alimentar de datos al sistema y/o actualizar los mismos.		
Obligación	Soporte Técnico		

Nombre	Gloria Del Razo Contreras
Cargo	Especialista "A" en Propiedad Industrial
Teléfono	5556240400 extensión 11264
Correo electrónico	gloria.delrazo@impi.gob.mx
Función	Cargar y/o alimentar de datos al sistema
Obligación	Cargar y/o alimentar de datos al sistema y/o actualizar los mismos.
Nombre	María De Los Ángeles Perez Cárdenas
Cargo	Especialista "B" en Propiedad Industrial
Teléfono	5556240400 extensión 11264
Correo electrónico	maria.perez@impi.gob.mx
Función	Cargar y/o alimentar de datos al sistema y/o actualizar los mismos.
Obligación	Concentrar información
Nombre	Melo Luis Enrique Rossell Rivera
Cargo	Especialista "B" en Propiedad Industrial
Teléfono	5556240400 extensión 11036
Correo electrónico	melo.rossell@impi.gob.mx
Función	Cargar y/o alimentar de datos al sistema y/o actualizar los mismos.
Obligación	Concentrar información
Nombre	Luz Del Carmen Ramírez Palacios
Cargo	Ayudante Especializado en Servicios "A"
Teléfono	5556240400 extensión 11036
Correo electrónico	luz.ramirez@impi.gob.mx
Función	Cargar y/o alimentar de datos al sistema y/o actualizar los mismos.
Obligación	Concentrar información

9. Tipo de soporte (señalar con una X, según corresponda)

*Electrónico		*Físico		*Ambos	X

*Descripción: Servidor y Expedientes de Personal

10. Transferencias o transmisiones de datos personales (señalar con una X, según corresponda)

*SI		NO	X

*Describir en que consiste la transferencia o transmisión

11. Portabilidad de datos (señalar con una X, según corresponda)

SI		NO	X

12. Nivel de protección que requieren los datos

Bajo en datos personales y alto en datos de salud.

13. Actualización de la información contenida en el sistema

Quincenalmente en los datos que requieran actualización.

14. Plazo de conservación de los datos personales

Histórico en Servidor y 30 años en papel. (Expedientes de Personal)

15. Medidas de Seguridad

Físicas	Se cuenta con un servicio de seguridad que es proporcionado por el Servicio de Protección Federal. El Instituto cuenta con sistemas de video-vigilancia en cada los inmuebles de Arenal y Pedregal, operando al 50% de su capacidad. Los servidores públicos deben portar en todo momento su credencial institucional, así como hacer uso del hand-punch al ingreso y salida diaria. El personal externo debe registrarse, dejar una identificación oficial, así como portar en todo momento el gafete de visita que le sea proporcionado en recepción. La autorización de los accesos es proporcionada por cada área, mediante mesa de ayuda o correo electrónico. Asimismo, con el fin de garantizar la integridad de la información del Instituto, se lleva a cabo una revisión del interior de mochilas, portafolios, bolsas grandes, maletas de equipaje, etc., registros en caso de ingreso con equipo de cómputo, así como del interior de las cajuelas de los vehículos que ingresan a las instalaciones. Para el acceso a los expedientes, éstos se encuentran debidamente resguardados en archiveros bajo llave y los responsables de los archivos de cada Coordinación son quienes tienen el control de estas llaves.
Administrativas	La información que se recaba en cumplimiento a la normatividad establecida en materia de Recursos Humanos, por lo que está debidamente justificada la finalidad por la cual se recaban.
Técnicas	Clave de usuario y password para acceso a sistemas.

16. Acceso a instalaciones

Con credencial de empleado y/o Identificación oficial.
Se cuenta con un servicio de seguridad que es proporcionado por el Servicio de Protección Federal.

El Instituto cuenta con sistemas de video-vigilancia en cada los inmuebles de Arenal y Pedregal, operando al 50% de su capacidad. Los servidores públicos deben portar en todo momento su credencial institucional, así como hacer uso del hand-punch al ingreso y salida diaria. El personal externo debe registrarse, dejar una identificación oficial, así como portar en todo momento el gafete de visita que le sea proporcionado en recepción. La autorización de los accesos es proporcionada por cada área, mediante mesa de ayuda o correo electrónico. Asimismo, con el fin de garantizar la integridad de la información del Instituto, se lleva a cabo una revisión del interior de mochilas, portafolios, bolsas grandes, maletas de equipaje, etc., así como del interior de las cajuelas de los vehículos que ingresan a las instalaciones. Para el acceso a los expedientes, éstos se encuentran debidamente resguardados en archiveros bajo llave y los responsables de los archivos de cada Coordinación son quienes tienen el control de estas llaves.
17. Perfiles de usuario y contraseña
Para el acceso al sistema SAP, cada usuario tiene una cuenta de acceso con una contraseña personal, administrada por la Dirección Divisional de Sistemas y Tecnología de la Información y para el acceso a los expedientes de personal, éstos se encuentran debidamente resguardados con acceso restringido solo para personal autorizado en archiveros bajo llave y los responsables de los archivos de cada Coordinación son quienes tienen el control de estas llaves.
18. Bitácoras de acceso y operación cotidiana, seguridad aplicable (señalar con una X, según corresponda)

	Soporte físico	No se cuenta con bitácoras, en virtud de que, en caso de préstamos de expedientes de personal, son solicitados por medio de oficio con la información y/o documentación que soporte el motivo de la solicitud, ya sea por autoridad competente ajena al IMPI o por el Órgano Interno de Control o algún otro.
	Soporte electrónico	No se cuenta con soporte electrónico de los expedientes físicos del personal, en cuanto al SAP la información se alberga en el Servidor Institucional que se encuentra y es administrado por la Dirección Divisional de Sistemas y Tecnología de la Información.

19. Lugar de almacenamiento de las bitácoras y tiempo de conservación y conservación de integridad
N/A
20. Registro de incidentes
No se tiene registro de incidentes, en virtud de que ningún expediente sale del archivo sin el debido oficio por medio del cual la autoridad competente lo solicite.
21. Procedimiento de respaldo y recuperación de datos
Servidores en el área de Sistemas.
22. Plan de contingencia
No se tiene implementado como tal un plan de contingencia.
23. Encargado de datos (señalar con una X, según corresponda)

Existe un prestador de servicios, persona física o moral, pública o privada ajena al IMPI que sola o conjuntamente, trate datos personales a nombre y por cuenta de este Instituto	SI		NO	X
22. Plan de conservación de los datos personales				

0. NÚMERO Y NOMBRE DEL ÁREA O UNIDAD ADMINISTRATIVA:	600 – Dirección Divisional de Administración		
1. Nombre del Sistema	**SAP (Control de Asistencia)**		
2. Objetivo	Administración de entrada y salida a labores y/o administración de incidencias.		
3. Fundamento Legal	Artículo 19 del Reglamento del Instituto Mexicano de la Propiedad Industrial		
4. DATOS PERSONALES QUE CONTIENE EL SISTEMA (señalar con una X, según corresponda)			
Numero de empleado	Para identificar a la persona		
5. FORMA DE OBTENCIÓN DE LOS DATOS PERSONALES (señalar con una X, según corresponda)			
Directa		**Indirecta** (obtenida, creada, generada en algún otro sistema)	
Formulario físico	X	**Descripción:**	
Formulario electrónico			
Texto físico	X		
Texto electrónico			
Vía telefónica			
Otro			
6. Responsable del Sistema			
Nombre	Víctor Manuel Terán Arista		
Cargo	Director Divisional de Administración		
Teléfono	5556240400 extensión 11018		
Correo electrónico	victor.teran@impi.gob.mx		
Función	Administrar los Recursos Humanos, Materiales y Financieros del Instituto conforme a normatividad establecida.		

Obligación	Administrar información dentro de un entorno para la administración y control de los recursos humanos, financieros y materiales del Instituto.
7. Administrador del Sistema	
Nombre	Agustín Fernando Bello Vázquez
Cargo	Director Divisional de Sistemas y Tecnología de la Información
Teléfono	5553340700 extensión 10000
Correo electrónico	agustin.bello@impi.gob.mx
Función	Administrar la Información del Sistema
Obligación	Resguardar información
8. Usuarios u Operador del Sistema	
Nombre	Carlos Jesús Oviedo Laguna
Cargo	Subdirector Divisional de Recursos Humanos
Teléfono	5556240400 extensión 11113
Correo electrónico	carlos.oviedo@impi.gob.mx
Función	Vigilar la recepción, registro y control de datos
Obligación	Resguardar información
Nombre	Saúl Javier Ríos Marmolejo
Cargo	Coordinador Departamental de Nómina
Teléfono	5556240400 extensión 11037
Correo electrónico	saul.rios@impi.gob.mx
Función	Coordinar la recepción, registro y control de datos
Obligación	Resguardar información
Nombre	David Rivera Fuentes
Cargo	Especialista "A" en Propiedad Industrial
Teléfono	5556240400 extensión 11033
Correo electrónico	david.rivera@impi.gob.mx
Función	Cargar y/o alimentar de datos al sistema
Obligación	Cargar y/o alimentar de datos al sistema y/o actualizar los mismos.
Nombre	Alejandro Ibarra Martínez
Cargo	Especialista "B" en Propiedad Industrial
Teléfono	5553340700 extensión 10409
Correo electrónico	alejandro.ibarra@impi.gob.mx
Función	Cargar y/o alimentar de datos al sistema y/o actualizar los mismos.
Obligación	Concentrar información
Nombre	Nury Alba González
Cargo	Secretaria Ejecutiva
Teléfono	5553340700 extensión 10409
Correo electrónico	nury.alba@impi.gob.mx
Función	Cargar y/o alimentar de datos al sistema y/o actualizar los mismos.
Obligación	Concentrar información

9. Tipo de soporte (señalar con una X, según corresponda)					
*Electrónico		*Físico		*Ambos	X
*Descripción: Servidor y Expedientes de Personal					

10. Transferencias o transmisiones de datos personales (señalar con una X, según corresponda)			
*SI		NO	X
*Describir en que consiste la transferencia o transmisión			

11. Portabilidad de datos (señalar con una X, según corresponda)			
SI		NO	X

12. Nivel de protección que requieren los datos	
Bajo en datos personales y alto en datos de salud.	
13. Actualización de la información contenida en el sistema	
Quincenalmente en los datos que requieran actualización.	
14. Plazo de conservación de los datos personales	
Histórico en Servidor y 30 años en papel. (Expedientes de Personal Incidencias)	
15. Medidas de Seguridad	
Físicas	Se cuenta con un servicio de seguridad que es proporcionado por el Servicio de Protección Federal. El Instituto cuenta con sistemas de video-vigilancia en cada los inmuebles de Arenal y Pedregal, operando al 50% de su capacidad. Los servidores públicos deben portar en todo momento su credencial institucional, así como hacer uso del hand-punch al ingreso y salida diaria. El personal externo debe registrarse, dejar una identificación oficial, así como portar en todo momento el gafete de visita que le sea proporcionado en recepción.

	La autorización de los accesos es proporcionada por cada área, mediante mesa de ayuda o correo electrónico. Asimismo, con el fin de garantizar la integridad de la información del Instituto, se lleva a cabo una revisión del interior de mochilas, portafolios, bolsas grandes, maletas de equipaje, etc., registros en caso de ingreso con equipo de cómputo, así como del interior de las cajuelas de los vehículos que ingresan a las instalaciones. Para el acceso a los expedientes, éstos se encuentran debidamente resguardados en archiveros bajo llave y los responsables de los archivos de cada Coordinación son quienes tienen el control de estas llaves.
Administrativas	La información que se recaba en cumplimiento a la normatividad establecida en materia de Recursos Humanos, por lo que está debidamente justificada la finalidad por la cual se recaban.
Técnicas	Clave de usuario y password para acceso a sistemas.

16. Acceso a instalaciones

Con credencial de empleado y/o Identificación oficial.
Se cuenta con un servicio de seguridad que es proporcionado por el Servicio de Protección Federal.
El Instituto cuenta con sistemas de video-vigilancia en cada los inmuebles de Arenal y Pedregal, operando al 50% de su capacidad.
Los servidores públicos deben portar en todo momento su credencial institucional, así como hacer uso del hand-punch al ingreso y salida diaria.
El personal externo debe registrarse, dejar una identificación oficial, así como portar en todo momento el gafete de visita que le sea proporcionado en recepción.
La autorización de los accesos es proporcionada por cada área, mediante mesa de ayuda o correo electrónico.
Asimismo, con el fin de garantizar la integridad de la información del Instituto, se lleva a cabo una revisión del interior de mochilas, portafolios, bolsas grandes, maletas de equipaje, etc., así como del interior de las cajuelas de los vehículos que ingresan a las instalaciones.
Para el acceso a los expedientes, éstos se encuentran debidamente resguardados en archiveros bajo llave y los responsables de los archivos de cada Coordinación son quienes tienen el control de estas llaves.

17. Perfiles de usuario y contraseña

Para el acceso al sistema SAP, cada usuario tiene una cuenta de acceso con una contraseña personal, administrada por la Dirección Divisional de Sistemas y Tecnología de la Información y para el acceso a los expedientes de personal, éstos se encuentran debidamente resguardados con acceso restringido solo para personal autorizado en archiveros bajo llave y los responsables de los archivos de cada Coordinación son quienes tienen el control de estas llaves.

18. Bitácoras de acceso y operación cotidiana, seguridad aplicable (señalar con una X, según corresponda)

	Soporte físico	No se cuenta con bitácoras, en virtud de que, en caso de préstamos de expedientes de personal, son solicitados por medio de oficio con la información y/o documentación que soporte el motivo de la solicitud, ya sea por autoridad competente ajena al IMPI o por el Órgano Interno de Control o algún otro.
	Soporte electrónico	No se cuenta con soporte electrónico de los expedientes físicos del personal, en cuanto al SAP la información se alberga en el Servidor Institucional que se encuentra y es administrado por la Dirección Divisional de Sistemas y Tecnología de la Información.

19. Lugar de almacenamiento de las bitácoras y tiempo de conservación y conservación de integridad

N/A

20. Registro de incidentes

No se tiene registro de incidentes, en virtud de que ningún expediente sale del archivo sin el debido oficio por medio del cual la autoridad competente lo solicite.

21. Procedimiento de respaldo y recuperación de datos

Servidores en el área de Sistemas.

22. Plan de contingencia

No se tiene implementado como tal un plan de contingencia.

23. Encargado de datos (señalar con una X, según corresponda)

Existe un prestador de servicios, persona física o moral, pública o privada ajena al IMPI que sola o conjuntamente, trate datos personales a nombre y por cuenta de este Instituto	SI		NO	**X**
22. Plazo de conservación de los datos personales				

0. NÚMERO Y NOMBRE DEL ÁREA O UNIDAD ADMINISTRATIVA:	600 – Dirección Divisional de Administración
1. Nombre del Sistema	**SAP (Expedientes de Personal)**
2. Objetivo	Administración de Expedientes de Personal
3. Fundamento Legal	Artículo 19 del Reglamento del Instituto Mexicano de la Propiedad Industrial
4. DATOS PERSONALES QUE CONTIENE EL SISTEMA (señalar con una X, según corresponda)	
Nombre	Para identificar a la persona
Titulo (Nivel de estudios)	Para conocer nivel de estudios

Fotografía	Para identificar a la persona
Domicilio	Para localizar a la persona fuera del Instituto en caso de ser necesario.
Teléfono	Para localizar a la persona fuera del Instituto en caso de ser necesario..
RFC	Para identificar como contribuyentes a las personas físicas o morales.
CURP	Para identificar oficialmente tanto a residentes como a ciudadanos mexicanos de todo el país.
Fecha de Nacimiento	Para conocer edad de la personal.
Lugar de Nacimiento	Para conocer lugar de nacimiento.
País de Nacimiento	Para conocer país de naciimienr.to.
Nacionalidad	Para en caso de extranjeros solicitar documentos migratorios
Estado Civil	Para fines estadísticos

5. FORMA DE OBTENCIÓN DE LOS DATOS PERSONALES (señalar con una X, según corresponda)

Directa		**Indirecta** (obtenida, creada, generada en algún otro sistema)	
Formulario físico	X	**Descripción:**	
Formulario electrónico			
Texto físico	X		
Texto electrónico			
Vía telefónica			
Otro			

6. Responsable del Sistema	
Nombre	Víctor Manuel Terán Arista
Cargo	Director Divisional de Administración
Teléfono	5556240400 extensión 11018
Correo electrónico	victor.teran@impi.gob.mx
Función	Administrar los Recursos Humanos, Materiales y Financieros del Instituto conforme a normatividad establecida.
Obligación	Administrar información dentro de un entorno para la administración y control de los recursos humanos, financieros y materiales del Instituto.
7. Administrador del Sistema	
Nombre	Agustín Fernando Bello Vázquez
Cargo	Director Divisional de Sistemas y Tecnología de la Información
Teléfono	5553340700 extensión 10000
Correo electrónico	agustin.bello@impi.gob.mx
Función	Administrar la Información del Sistema
Obligación	Resguardar información
8. Usuarios u Operador del Sistema	
Nombre	Carlos Jesús Oviedo Laguna
Cargo	Subdirector Divisional de Recursos Humanos
Teléfono	5556240400 extensión 11113
Correo electrónico	carlos.oviedo@impi.gob.mx
Función	Vigilar la recepción, registro y control de datos
Obligación	Resguardar información
Nombre	Mara Erika Vega Ibarra
Cargo	Coordinador Departamental de Selección, Reclutamiento y Capacitación
Teléfono	5556240400 extensión 11016
Correo electrónico	mara.vega@impi.gob.mx
Función	Coordinar la recepción, registro y control de datos
Obligación	Resguardar información
Nombre	Ana Lilia Carmona Serrano
Cargo	Especialista "A" en Propiedad Industrial
Teléfono	5556240400 extensión 11847
Correo electrónico	ana.carmona@impi.gob.mx
Función	Cargar y/o alimentar de datos al sistema
Obligación	Cargar y/o alimentar de datos al sistema y/o actualizar los mismos.
Nombre	Alma Lilia Morales Guzmán
Cargo	Especialista "B" en Propiedad Industrial
Teléfono	5556240400 extensión 11847
Correo electrónico	alma.morales@impi.gob.mx
Función	Cargar y/o alimentar de datos al sistema y/o actualizar los mismos.
Obligación	Concentrar información

9. Tipo de soporte (señalar con una X, según corresponda)

*Electrónico		*Físico		*Ambos	X

*Descripción: Servidor y Expedientes de Personal

10. Transferencias o transmisiones de datos personales (señalar con una X, según corresponda)

*SI		NO	X

*Describir en que consiste la transferencia o transmisión

11. Portabilidad de datos (señalar con una X, según corresponda)			
SI		NO	X
12. Nivel de protección que requieren los datos			
Bajo en datos personales y alto en datos de salud.			
13. Actualización de la información contenida en el sistema			
Quincenalmente en los datos que requieran actualización.			
14. Plazo de conservación de los datos personales			
Histórico en Servidor y 30 años en papel. (Expedientes de Personal)			
15. Medidas de Seguridad			
Físicas	Se cuenta con un servicio de seguridad que es proporcionado por el Servicio de Protección Federal. El Instituto cuenta con sistemas de video-vigilancia en cada los inmuebles de Arenal y Pedregal, operando al 50% de su capacidad. Los servidores públicos deben portar en todo momento su credencial institucional, así como hacer uso del hand-punch al ingreso y salida diaria. El personal externo debe registrarse, dejar una identificación oficial, así como portar en todo momento el gafete de visita que le sea proporcionado en recepción. La autorización de los accesos es proporcionada por cada área, mediante mesa de ayuda o correo electrónico. Asimismo, con el fin de garantizar la integridad de la información del Instituto, se lleva a cabo una revisión del interior de mochilas, portafolios, bolsas grandes, maletas de equipaje, etc., registros en caso de ingreso con equipo de cómputo, así como del interior de las cajuelas de los vehículos que ingresan a las instalaciones. Para el acceso a los expedientes, éstos se encuentran debidamente resguardados en archiveros bajo llave y los responsables de los archivos de cada Coordinación son quienes tienen el control de estas llaves.		
Administrativas	La información que se recaba en cumplimiento a la normatividad establecida en materia de Recursos Humanos, por lo que está debidamente justificada la finalidad por la cual se recaban.		
Técnicas	Clave de usuario y password para acceso a sistemas.		
16. Acceso a instalaciones			
Con credencial de empleado y/o Identificación oficial. Se cuenta con un servicio de seguridad que es proporcionado por el Servicio de Protección Federal. El Instituto cuenta con sistemas de video-vigilancia en cada los inmuebles de Arenal y Pedregal, operando al 50% de su capacidad. Los servidores públicos deben portar en todo momento su credencial institucional, así como hacer uso del hand-punch al ingreso y salida diaria. El personal externo debe registrarse, dejar una identificación oficial, así como portar en todo momento el gafete de visita que le sea proporcionado en recepción. La autorización de los accesos es proporcionada por cada área, mediante mesa de ayuda o correo electrónico. Asimismo, con el fin de garantizar la integridad de la información del Instituto, se lleva a cabo una revisión del interior de mochilas, portafolios, bolsas grandes, maletas de equipaje, etc., así como del interior de las cajuelas de los vehículos que ingresan a las instalaciones. Para el acceso a los expedientes, éstos se encuentran debidamente resguardados en archiveros bajo llave y los responsables de los archivos de cada Coordinación son quienes tienen el control de estas llaves.			
17. Perfiles de usuario y contraseña			
Para el acceso al sistema SAP, cada usuario tiene una cuenta de acceso con una contraseña personal, administrada por la Dirección Divisional de Sistemas y Tecnología de la Información y para el acceso a los expedientes de personal, éstos se encuentran debidamente resguardados con acceso restringido solo para personal autorizado en archiveros bajo llave y los responsables de los archivos de cada Coordinación son quienes tienen el control de estas llaves.			
18. Bitácoras de acceso y operación cotidiana, seguridad aplicable (señalar con una X, según corresponda)			
	Soporte físico	No se cuenta con bitácoras, en virtud de que, en caso de préstamos de expedientes de personal, son solicitados por medio de oficio con la información y/o documentación que soporte el motivo de la solicitud, ya sea por autoridad competente ajena al IMPI o por el Órgano Interno de Control o algún otro.	
	Soporte electrónico	No se cuenta con soporte electrónico de los expedientes físicos del personal, en cuanto al SAP la información se alberga en el Servidor Institucional que se encuentra y es administrado por la Dirección Divisional de Sistemas y Tecnología de la Información.	
19. Lugar de almacenamiento de las bitácoras y tiempo de conservación y conservación de integridad			
N/A			
20. Registro de incidentes			
No se tiene registro de incidentes, en virtud de que ningún expediente sale del archivo sin el debido oficio por medio del cual la autoridad competente lo solicite.			
21. Procedimiento de respaldo y recuperación de datos			

Servidores en el área de Sistemas.					
22. Plan de contingencia					
No se tiene implementado como tal un plan de contingencia.					
23. Encargado de datos (señalar con una X, según corresponda)					
Existe un prestador de servicios, persona física o moral, pública o privada ajena al IMPI que sola o conjuntamente, trate datos personales a nombre y por cuenta de este Instituto	SI		NO	X	
22. Plazo de conservación de los datos personales					

0. NÚMERO Y NOMBRE DEL ÁREA O UNIDAD ADMINISTRATIVA:	600 – Dirección Divisional de Administración		
1. Nombre del Sistema	**SAP (Servicio Social y Practicas Profesionales)**		
2. Objetivo	Administración de Expedientes		
3. Fundamento Legal	Artículo 19 del Reglamento del Instituto Mexicano de la Propiedad Industrial		
4. DATOS PERSONALES QUE CONTIENE EL SISTEMA (señalar con una X, según corresponda)			
Nombre	Para identificar a la persona		
Titulo (Nivel de estudios)	Para conocer nivel de estudios		
Fotografía	Para identificar a la persona		
Domicilio	Para localizar a la persona fuera del Instituto en caso de ser necesario.		
Teléfono	Para localizar a la persona fuera del Instituto en caso de ser necesario..		
RFC	Para identificar como contribuyentes a las personas físicas o morales.		
CURP	Para identificar oficialmente tanto a residentes como a ciudadanos mexicanos de todo el país.		
Fecha de Nacimiento	Para conocer edad de la personal.		
Lugar de Nacimiento	Para conocer lugar de nacimiento.		
País de Nacimiento	Para conocer país de naciimienr.to.		
Nacionalidad	Para en caso de extranjeros solicitar documentos migratorios		
Estado Civil	Para fines estadísticos		
5. FORMA DE OBTENCIÓN DE LOS DATOS PERSONALES (señalar con una X, según corresponda)			
Directa		**Indirecta** (obtenida, creada, generada en algún otro sistema)	
Formulario físico	X	**Descripción:**	
Formulario electrónico			
Texto físico	X		
Texto electrónico			
Vía telefónica			
Otro			
6. Responsable del Sistema			
Nombre	Víctor Manuel Terán Arista		
Cargo	Director Divisional de Administración		
Teléfono	5556240400 extensión 11018		
Correo electrónico	victor.teran@impi.gob.mx		
Función	Administrar los Recursos Humanos, Materiales y Financieros del Instituto conforme a normatividad establecida.		
Obligación	Administrar información dentro de un entorno para la administración y control de los recursos humanos, financieros y materiales del Instituto.		
7. Administrador del Sistema			
Nombre	Agustín Fernando Bello Vázquez		
Cargo	Director Divisional de Sistemas y Tecnología de la Información		
Teléfono	5553340700 extensión 10000		
Correo electrónico	agustin.bello@impi.gob.mx		
Función	Administrar la Información del Sistema		
Obligación	Resguardar información		
8. Usuarios u Operador del Sistema			
Nombre	Carlos Jesús Oviedo Laguna		
Cargo	Subdirector Divisional de Recursos Humanos		
Teléfono	5556240400 extensión 11113		
Correo electrónico	carlos.oviedo@impi.gob.mx		
Función	Vigilar la recepción, registro y control de datos		
Obligación	Resguardar información		
Nombre	Mara Erika Vega Ibarra		
Cargo	Coordinador Departamental de Selección, Reclutamiento y Capacitación		
Teléfono	5556240400 extensión 11016		
Correo electrónico	mara.vega@impi.gob.mx		

Función	Coordinar la recepción, registro y control de datos
Obligación	Resguardar información
Nombre	Alfonso Morales Huerta
Cargo	Ayudante Especializado en Servicios "A"
Teléfono	5556240400 extensión 11847
Correo electrónico	alfonso.morales@impi.gob.mx
Función	Cargar y/o alimentar de datos al sistema
Obligación	Cargar y/o alimentar de datos al sistema y/o actualizar los mismos.

9. Tipo de soporte (señalar con una X, según corresponda)

*Electrónico		*Físico		*Ambos	X

*Descripción: Servidor y Expedientes de Personal

10. Transferencias o transmisiones de datos personales (señalar con una X, según corresponda)

*SI		NO	X

*Describir en que consiste la transferencia o transmisión

11. Portabilidad de datos (señalar con una X, según corresponda)

SI		NO	X

12. Nivel de protección que requieren los datos

Bajo en datos personales y alto en datos de salud.

13. Actualización de la información contenida en el sistema

Quincenalmente en los datos que requieran actualización.

14. Plazo de conservación de los datos personales

Histórico en Servidor y 30 años en papel. (Expedientes de Personal)

15. Medidas de Seguridad

Físicas	Se cuenta con un servicio de seguridad que es proporcionado por el Servicio de Protección Federal. El Instituto cuenta con sistemas de video-vigilancia en cada los inmuebles de Arenal y Pedregal, operando al 50% de su capacidad. Los servidores públicos deben portar en todo momento su credencial institucional, así como hacer uso del hand-punch al ingreso y salida diaria. El personal externo debe registrarse, dejar una identificación oficial, así como portar en todo momento el gafete de visita que le sea proporcionado en recepción. La autorización de los accesos es proporcionada por cada área, mediante mesa de ayuda o correo electrónico. Asimismo, con el fin de garantizar la integridad de la información del Instituto, se lleva a cabo una revisión del interior de mochilas, portafolios, bolsas grandes, maletas de equipaje, etc., registros en caso de ingreso con equipo de cómputo, así como del interior de las cajuelas de los vehículos que ingresan a las instalaciones. Para el acceso a los expedientes, éstos se encuentran debidamente resguardados en archiveros bajo llave y los responsables de los archivos de cada Coordinación son quienes tienen el control de estas llaves.
Administrativas	La información que se recaba en cumplimiento a la normatividad establecida en materia de Recursos Humanos, por lo que está debidamente justificada la finalidad por la cual se recaban.
Técnicas	Clave de usuario y password para acceso a sistemas.

16. Acceso a instalaciones

Con credencial de empleado y/o Identificación oficial.

Se cuenta con un servicio de seguridad que es proporcionado por el Servicio de Protección Federal.
El Instituto cuenta con sistemas de video-vigilancia en cada los inmuebles de Arenal y Pedregal, operando al 50% de su capacidad.
Los servidores públicos deben portar en todo momento su credencial institucional, así como hacer uso del hand-punch al ingreso y salida diaria.
El personal externo debe registrarse, dejar una identificación oficial, así como portar en todo momento el gafete de visita que le sea proporcionado en recepción.
La autorización de los accesos es proporcionada por cada área, mediante mesa de ayuda o correo electrónico.
Asimismo, con el fin de garantizar la integridad de la información del Instituto, se lleva a cabo una revisión del interior de mochilas, portafolios, bolsas grandes, maletas de equipaje, etc., así como del interior de las cajuelas de los vehículos que ingresan a las instalaciones.
Para el acceso a los expedientes, éstos se encuentran debidamente resguardados en archiveros bajo llave y los responsables de los archivos de cada Coordinación son quienes tienen el control de estas llaves.

17. Perfiles de usuario y contraseña

Para el acceso al sistema SAP, cada usuario tiene una cuenta de acceso con una contraseña personal, administrada por la Dirección Divisional de Sistemas y Tecnología de la Información y para el acceso a los expedientes de personal, éstos se encuentran debidamente resguardados con acceso restringido solo para personal autorizado en archiveros bajo llave y los responsables de los archivos de cada Coordinación son quienes tienen el control de estas llaves.

18. Bitácoras de acceso y operación cotidiana, seguridad aplicable (señalar con una X, según corresponda)

	Soporte físico	No se cuenta con bitácoras, en virtud de que, en caso de préstamos de expedientes de personal, son solicitados por medio de oficio con la información y/o documentación que soporte el motivo de la solicitud, ya sea por autoridad competente ajena al IMPI o por el Órgano Interno de Control o algún otro.
	Soporte electrónico	No se cuenta con soporte electrónico de los expedientes físicos del personal, en cuanto al SAP la información se alberga en el Servidor Institucional que se encuentra y es administrado por la Dirección Divisional de Sistemas y Tecnología de la Información.

19. Lugar de almacenamiento de las bitácoras y tiempo de conservación y conservación de integridad
N/A
20. Registro de incidentes
No se tiene registro de incidentes, en virtud de que ningún expediente sale del archivo sin el debido oficio por medio del cual la autoridad competente lo solicite.
21. Procedimiento de respaldo y recuperación de datos
Servidores en el área de Sistemas.
22. Plan de contingencia
No se tiene implementado como tal un plan de contingencia.

23. Encargado de datos (señalar con una X, según corresponda)				
Existe un prestador de servicios, persona física o moral, pública o privada ajena al IMPI que sola o conjuntamente, trate datos personales a nombre y por cuenta de este Instituto	SI		NO	**X**
22. Plazo de conservación de los datos personales				

0. NÚMERO Y NOMBRE DEL ÁREA O UNIDAD ADMINISTRATIVA:	600 – Dirección Divisional de Administración		
1. Nombre del Sistema	**SAP (Historia Clínica)**		
2. Objetivo	Conocer el estado de salud del personal del Instituto		
3. Fundamento Legal	Artículo 19 del Reglamento del Instituto Mexicano de la Propiedad Industrial		
4. DATOS PERSONALES QUE CONTIENE EL SISTEMA (señalar con una X, según corresponda)			
Nombre	Para identificar a la persona		
Fotografía	Para identificar a la persona		
Tipo de sangre	Dato necesario en caso de urgencias médicas.		
Peso	Para conocer estado de salud.		
Estatura	Para conocer estado de salud.		
Temperatura	Para conocer estado de salud.		
Presión arterial	Para conocer estado de salud.		
Frecuencia cardiaca	Para conocer estado de salud.		
5. FORMA DE OBTENCIÓN DE LOS DATOS PERSONALES (señalar con una X, según corresponda)			
Directa		**Indirecta** (obtenida, creada, generada en algún otro sistema)	
Formulario físico	**X**	**Descripción:**	
Formulario electrónico			
Texto físico	**X**		
Texto electrónico			
Vía telefónica			
Otro			
6. Responsable del Sistema			
Nombre	Víctor Manuel Terán Arista		
Cargo	Director Divisional de Administración		
Teléfono	5556240400 extensión 11018		
Correo electrónico	victor.teran@impi.gob.mx		
Función	Administrar los Recursos Humanos, Materiales y Financieros del Instituto conforme a normatividad establecida.		
Obligación	Administrar información dentro de un entorno para la administración y control de los recursos humanos, financieros y materiales del Instituto.		
7. Administrador del Sistema			
Nombre	Agustín Fernando Bello Vázquez		
Cargo	Director Divisional de Sistemas y Tecnología de la Información		
Teléfono	5553340700 extensión 10000		
Correo electrónico	agustin.bello@impi.gob.mx		
Función	Administrar la Información del Sistema		
Obligación	Resguardar información		
8. Usuarios u Operador del Sistema			

Nombre	Carlos Jesús Oviedo Laguna
Cargo	Subdirector Divisional de Recursos Humanos
Teléfono	5556240400 extensión 11113
Correo electrónico	carlos.oviedo@impi.gob.mx
Función	Vigilar la recepción, registro y control de datos
Obligación	Resguardar información
Nombre	Mara Erika Vega Ibarra
Cargo	Coordinador Departamental de Selección, Reclutamiento y Capacitación
Teléfono	5556240400 extensión 11016
Correo electrónico	mara.vega@impi.gob.mx
Función	Coordinar la recepción, registro y control de datos
Obligación	Resguardar información
Nombre	Gloria Ruiz Rangel
Cargo	Especialista "A" en Propiedad Industrial
Teléfono	5556240400 extensión 11258
Correo electrónico	gloria.ruiz@impi.gob.mx
Función	Cargar y/o alimentar de datos al sistema
Obligación	Cargar y/o alimentar de datos al sistema y/o actualizar los mismos.

9. Tipo de soporte (señalar con una X, según corresponda)

*Electrónico		*Físico		*Ambos	X

*Descripción: Servidor y Expedientes de Personal

10. Transferencias o transmisiones de datos personales (señalar con una X, según corresponda)

*SI		NO	X

*Describir en que consiste la transferencia o transmisión

11. Portabilidad de datos (señalar con una X, según corresponda)

SI		NO	X

12. Nivel de protección que requieren los datos

Bajo en datos personales y alto en datos de salud.

13. Actualización de la información contenida en el sistema

Quincenalmente en los datos que requieran actualización.

14. Plazo de conservación de los datos personales

Histórico en Servidor y 30 años en papel. (Expedientes de Personal)

15. Medidas de Seguridad

Físicas	Se cuenta con un servicio de seguridad que es proporcionado por el Servicio de Protección Federal. El Instituto cuenta con sistemas de video-vigilancia en cada los inmuebles de Arenal y Pedregal, operando al 50% de su capacidad. Los servidores públicos deben portar en todo momento su credencial institucional, así como hacer uso del hand-punch al ingreso y salida diaria. El personal externo debe registrarse, dejar una identificación oficial, así como portar en todo momento el gafete de visita que le sea proporcionado en recepción. La autorización de los accesos es proporcionada por cada área, mediante mesa de ayuda o correo electrónico. Asimismo, con el fin de garantizar la integridad de la información del Instituto, se lleva a cabo una revisión del interior de mochilas, portafolios, bolsas grandes, maletas de equipaje, etc., registros en caso de ingreso con equipo de cómputo, así como del interior de las cajuelas de los vehículos que ingresan a las instalaciones. Para el acceso a los expedientes, éstos se encuentran debidamente resguardados en archiveros bajo llave y los responsables de los archivos de cada Coordinación son quienes tienen el control de estas llaves.
Administrativas	La información que se recaba en cumplimiento a la normatividad establecida en materia de Recursos Humanos, por lo que está debidamente justificada la finalidad por la cual se recaban.
Técnicas	Clave de usuario y password para acceso a sistemas.

16. Acceso a instalaciones

Con credencial de empleado y/o Identificación oficial.

Se cuenta con un servicio de seguridad que es proporcionado por el Servicio de Protección Federal.
El Instituto cuenta con sistemas de video-vigilancia en cada los inmuebles de Arenal y Pedregal, operando al 50% de su capacidad.
Los servidores públicos deben portar en todo momento su credencial institucional, así como hacer uso del hand-punch al ingreso y salida diaria.
El personal externo debe registrarse, dejar una identificación oficial, así como portar en todo momento el gafete de visita que le sea proporcionado en recepción.
La autorización de los accesos es proporcionada por cada área, mediante mesa de ayuda o correo electrónico.

Asimismo, con el fin de garantizar la integridad de la información del Instituto, se lleva a cabo una revisión del interior de mochilas, portafolios, bolsas grandes, maletas de equipaje, etc., así como del interior de las cajuelas de los vehículos que ingresan a las instalaciones. Para el acceso a los expedientes, éstos se encuentran debidamente resguardados en archiveros bajo llave y los responsables de los archivos de cada Coordinación son quienes tienen el control de estas llaves.					
17. Perfiles de usuario y contraseña					
Para el acceso al sistema SAP, cada usuario tiene una cuenta de acceso con una contraseña personal, administrada por la Dirección Divisional de Sistemas y Tecnología de la Información y para el acceso a los expedientes de personal, éstos se encuentran debidamente resguardados con acceso restringido solo para personal autorizado en archiveros bajo llave y los responsables de los archivos de cada Coordinación son quienes tienen el control de estas llaves.					
18. Bitácoras de acceso y operación cotidiana, seguridad aplicable (señalar con una X, según corresponda)					
	Soporte físico	No se cuenta con bitácoras, en virtud de que, en caso de préstamos de expedientes de personal, son solicitados por medio de oficio con la información y/o documentación que soporte el motivo de la solicitud, ya sea por autoridad competente ajena al IMPI o por el Órgano Interno de Control o algún otro.			
	Soporte electrónico	No se cuenta con soporte electrónico de los expedientes físicos del personal, en cuanto al SAP la información se alberga en el Servidor Institucional que se encuentra y es administrado por la Dirección Divisional de Sistemas y Tecnología de la Información.			
19. Lugar de almacenamiento de las bitácoras y tiempo de conservación y conservación de integridad					
N/A					
20. Registro de incidentes					
No se tiene registro de incidentes, en virtud de que ningún expediente sale del archivo sin el debido oficio por medio del cual la autoridad competente lo solicite.					
21. Procedimiento de respaldo y recuperación de datos					
Servidores en el área de Sistemas.					
22. Plan de contingencia					
No se tiene implementado como tal un plan de contingencia.					
23. Encargado de datos (señalar con una X, según corresponda)					
Existe un prestador de servicios, persona física o moral, pública o privada ajena al IMPI que sola o conjuntamente, trate datos personales a nombre y por cuenta de este Instituto		SI		NO	**X**
22. Plazo de conservación de los datos personales					

1000 DIRECCIÓN DIVISIONAL DE PROMOCIÓN Y SERVICIOS DE INFORMACIÓN TECNOLÓGICA			
1. Nombre del Sistema	SISTEMA DE BÚSQUEDA DE PATENTES EN LÍNEA		
2. Objetivo	Resolución a las solicitudes de búsqueda de información tecnológica y de vigilancias y alertas tecnológicas		
3. Fundamento Legal	Estatuto Orgánico del Instituto Mexicano de la Propiedad Industrial Artículo 20 fracciones IV y VII (D.O.F. 27/12/1999 última reforma 5/01/2018) ; Reglamento de Instituto Mexicano de la Propiedad Industrial Artículo 16 fracciones IV y VII (D.O.F. 14/12/1999 última reforma 15/12/2017); Acuerdo que Delega Facultades en los Directores Generales Adjuntos, Coordinador, Directores Divisionales, Titulares de las Oficinas Regionales, Subdirectores Divisionales, Coordinadores Departamentales y otros subalternos de Instituto Mexicano de la Propiedad Industrial Artículo 9 (D.O.F. 15/12/1999 última reforma 20/01/2018)		
4. DATOS PERSONALES QUE CONTIENE EL SISTEMA (señalar con una X, según corresponda)			
Dato personal	Idoneidad (informar para que se recaba el dato)		
Nombre	Para atender las solicitudes de búsquedas de información tecnológica y de vigilancias y alertas tecnológicas y alertas tecnológicas complementarias.		
Teléfono	Para contactar al usuario en caso de ser necesario.		
Correo electrónico	Para el envío de avisos relacionados con la solicitud de usuario.		
Domicilio	Fines estadísticos. Para conocer el número de solicitudes de búsqueda que se presentan por Entidad Federativa.		
5. FORMA DE OBTENCIÓN DE LOS DATOS PERSONALES (señalar con una X, según corresponda)			
Directa	X	**Indirecta** (obtenida, creada, generada en algún otro sistema)	
Formulario físico	X	**Descripción:**	
Formulario electrónico	X		
Texto físico			
Texto electrónico			
Vía telefónica			
Otro			
6. Responsable del Sistema			
Nombre	Viviana Huerta García		
Cargo	Directora Divisional de Promoción y Servicios de Información Tecnológica		
Teléfono	5624-0400 Ext. 11110		
Correo electrónico	viviana.huerta@impi.gob.mx		
Función	Para generación de reportes.		
Obligación	Supervisar la prestación de las solicitudes de búsquedas de información tecnológica y de vigilancias y alertas tecnológicas		
7. Administrador del Sistema			
Nombre	Alberto Olguín Nava		
Cargo	Subdirector Divisional de Servicios de Información Tecnológica		
Teléfono	5624-0400 Ext. 11079		
Correo electrónico	alberto.olguin@impi.gob.mx		
Función	Para generación de reportes.		
Obligación	Supervisar la prestación de las solicitudes de búsquedas de información tecnológica y de vigilancias y alertas tecnológicas		
8. Usuarios u Operador del Sistema			
Nombre	Leonardo Gómez Bautista		
Cargo	Coordinador Departamental del Centro de Información Tecnológica		
Teléfono	5334 07 00 Ext. 10106		
Correo electrónico	leonardo.gómez@impi.gob.mx		
Función	Operar la atención de los servicios de solicitudes de búsquedas de información tecnológica y de vigilancias y alertas tecnológicas		
Obligación	Atender las solicitudes de búsquedas de información tecnológica y de vigilancias y alertas tecnológicas		
Observaciones:	Personal autorizado adscrito a la Dirección Divisional de Promoción y Servicios de Información Tecnológica.		
9. Tipo de soporte (señalar con una X, según corresponda)			
*Electrónico		*Físico		*Ambos	X
*Descripción: Los usuarios ingresan su solicitud capturando sus datos en formato físico o electrónico			
10. Transferencias o transmisiones de datos personales (señalar con una X, según corresponda)			
*SI		NO X	
*Describir en que consiste la transferencia o transmisión NA			

11. Portabilidad de datos (señalar con una X, según corresponda)			
SI		NO	X
12. Nivel de protección que requieren los datos			
Nivel Básico			
13. Actualización de la información contenida en el sistema			
Diaria			
14. Plazo de conservación de los datos personales			
1 año**			
15. Medidas de Seguridad			
Físicas	Acceso restringido a las instalaciones, portabilidad de la credencial. Personal de seguridad.		
Administrativas	Seguridad relacionada a los recursos humanos. Cumplimiento de la normatividad.		
Técnicas	Control de Acceso.		
16. Acceso a instalaciones			
Seguridad perimetral exterior: en la entrada de las instalaciones el personal de seguridad únicamente permite el acceso al personal que labora en el Instituto y en el caso de los usuarios que solicitan asesorías se les requiere un registro y que presenten una identificación oficial para proporcionarles un gafete de visitantes. Seguridad interior: únicamente se permite el acceso al área de asesoría a personas que porten gafete de visitante. El Instituto cuenta con un sistema de circuito cerrado.			
17. Perfiles de usuario y contraseña			
Modelo de control de acceso: Está basado en perfiles de usuario. **Perfiles de usuario y contraseña en el sistema operativo de red** El sistema sí cuenta con un sistema operativo de red instalado en los equipos. El sistema operativo si proporciona un manejo riguroso de perfiles de usuario y contraseñas. **Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de datos personales** El software realiza un cifrado al teclear la contraseña. **Administrador de perfiles de usuario y contraseñas** La Dirección Divisional de Sistemas y Tecnologías de la Información (DDSTI) se encarga de la creación de los perfiles a petición de la Dirección Divisional de Promoción y Servicios de Información Tecnológica (DDPSIT). DDPSIT se encarga de la autorización de nuevos perfiles. La DDSTI se encarga del registro de la creación de nuevos perfiles. **Acceso remoto al sistema de datos personales** Se puede ingresar al sistema únicamente desde los equipos instalados en el Instituto.			
18. Bitácoras de acceso y operación cotidiana, seguridad aplicable (señalar con una X, según corresponda)			
	Soporte físico	No se cuenta con bitácoras ya que el acceso a los datos está restringido al personal autorizado.	
	Soporte electrónico	No se cuenta con bitácoras ya que el acceso a los datos está restringido al personal autorizado.	
19. Lugar de almacenamiento de las bitácoras y tiempo de conservación y conservación de integridad			
N/A			
20. Registro de incidentes			
En el caso de los expedientes físicos se elabora un acta administrativa al día siguiente de haber identificado el incidente (extravío de expediente). Por lo que respecta a la plataforma, en caso de alguna incidencia esta se reporta a la DDSTI.			
21. Procedimiento de respaldo y recuperación de datos			
La Dirección Divisional de Promoción y Servicios de Información Tecnológica se encarga del resguardo físico de la información, las solicitudes que se reciben físicas se capturan en el sistema. La Dirección Divisional de Sistemas y Tecnología de la Información se encarga del resguardo de la información del sistema.			
22. Plan de contingencia			
No aplica			
23. Encargado de datos (señalar con una X, según corresponda)			

Existe un prestador de servicios, persona física o moral, pública o privada ajena al IMPI que sola o conjuntamente, trate datos personales a nombre y por cuenta de este Instituto	SI		NO	X
22. Plazo de conservación de los datos personales	1 año**			

***En cumplimiento a la Ley General de Archivos que entró en vigor el 15 de junio de 2019 y derivado de la reunión sostenida con la Coordinación de Archivos, el Órgano Interno de Control y la Unidad de Transparencia el pasado 2 de septiembre de 2019, la Dirección Divisional de Promoción y Servicios de Información Tecnológica, está realizando acciones para la clasificación y organización de sus archivos.
Derivado de lo anterior, se está en proceso de regularización.

1000 DIRECCIÓN DIVISIONAL DE PROMOCIÓN Y SERVICIOS DE INFORMACIÓN TECNOLÓGICA			
1. Nombre del Sistema	SISTEMA DE REGISTRO DE ACTIVIDADES DE PROMOCIÓN Y ASESORIAS		
2. Objetivo	Proporcionar asesoría en materia de propiedad industrial		
3. Fundamento Legal	Estatuto Orgánico del Instituto Mexicano de la Propiedad Industrial Artículo 20 fracciones II y V (D.O.F. 27/12/1999 última reforma 5/01/2018) ; Reglamento de Instituto Mexicano de la Propiedad Industrial Artículo 16 fracciones II y V (D.O.F. 14/12/1999 última reforma 15/12/2017).		
4. DATOS PERSONALES QUE CONTIENE EL SISTEMA (señalar con una X, según corresponda)			
Dato personal	Idoneidad (informar para que se recaba el dato)		
Nombre	Para personalizar la atención que se le brinda al usuario al darle asesoría.		
Sexo	Para fines estadísticos		
Dirección	Para fines estadísticos		
CURP	Responder dudas de los usuarios respecto a su cuenta de los servicios electrónicos del Instituto.		
RFC	Responder dudas de los usuarios respecto a sus pagos y facturas.		
Datos laborales (Institución)	Para fines estadísticos		
Teléfono	Contactar al usuario cuando la complejidad de la asesoría así lo requiera.		
Correo electrónico	Para responder dudas de los usuarios, orientarlos y asesorarlos en sus trámites ante el Instituto y para compartir material de apoyo relacionado con la asesoría.		
5. FORMA DE OBTENCIÓN DE LOS DATOS PERSONALES (señalar con una X, según corresponda)			
Directa	X	**Indirecta** (obtenida, creada, generada en algún otro sistema)	
Formulario físico	X	**Descripción:**	
Formulario electrónico			
Texto físico			
Texto electrónico	X		
Vía telefónica	X		
Otro			
6. Responsable del Sistema			
Nombre	Viviana Huerta García		
Cargo	Directora Divisional de Promoción y Servicios de Información Tecnológica		
Teléfono	5624-0400 Ext. 11110		
Correo electrónico	viviana.huerta@impi.gob.mx		
Función	Designar a su personal adscrito para la atención al usuario.		
Obligación	Supervisar la prestación del servicio de asesorías.		
7. Administrador del Sistema			
Nombre	Alberto Olguín Nava		
Cargo	Subdirector Divisional de Servicios de Información Tecnológica		
Teléfono	5624-0400 Ext. 11079		
Correo electrónico	alberto.olguin@impi.gob.mx		
Función	Designar a su personal adscrito para la atención al usuario.		
Obligación	Supervisar la prestación del servicio de asesorías.		
8. Usuarios u Operador del Sistema			
Nombre	Francisco Isaías Escutia Álvarez		
Cargo	Coordinador Departamental de Estudios de Difusión de la Propiedad Industrial		
Teléfono	5624-0400 Ext. 11912		
Correo electrónico	francisco.escutia@impi.gob.mx		
Función	Designar a su personal adscrito para la atención al usuario.		
Obligación	Supervisar la prestación del servicio de asesorías.		
Observaciones:	Otros usuarios del sistema son personal autorizado adscrito a la Dirección Divisional de Promoción y Servicios de Información Tecnológica.		

9. Tipo de soporte (señalar con una X, según corresponda)					
*Electrónico		*Físico		*Ambos	**X**

*Descripción:
Las asesorías se proporcionan de forma presencial a los usuarios que así lo requieran, éstos capturan sus datos en una cédula de asesorías. También se brindan asesorías mediante el correo electrónico buzon@impi.gob.mx a los usuarios que envíen sus peticiones por dicho medio. Se contacta vía telefónica al usuario cuando la complejidad de la asesoría así lo requiere.

10. Transferencias o transmisiones de datos personales (señalar con una X, según corresponda)			
*SI			NO **X**

*Describir en que consiste la transferencia o transmisión

NA

11. Portabilidad de datos (señalar con una X, según corresponda)			
SI		NO	X

12. Nivel de protección que requieren los datos
Nivel Básico

13. Actualización de la información contenida en el sistema
Diaria

14. Plazo de conservación de los datos personales
1 año **

15. Medidas de Seguridad	
Físicas	Acceso restringido a las instalaciones, portabilidad de la credencial. Personal de seguridad.
Administrativas	Seguridad relacionada a los recursos humanos. Cumplimiento de la normatividad.
Técnicas	Control de Acceso.

16. Acceso a instalaciones
Seguridad perimetral exterior: en la entrada de las instalaciones el personal de seguridad únicamente permite el acceso al personal que labora en el Instituto y en el caso de los usuarios que solicitan asesorías se les requiere un registro y que presenten una identificación oficial para proporcionarles un gafete de visitantes. Seguridad interior: únicamente se permite el acceso al área de asesoría a personas que porten gafete de visitante. El Instituto cuenta con un sistema de circuito cerrado.

17. Perfiles de usuario y contraseña
Modelo de control de acceso: Está basado en perfiles de usuario. **Perfiles de usuario y contraseña en el sistema operativo de red** El sistema sí cuenta con un sistema operativo de red instalado en los equipos. El sistema operativo si proporciona un manejo riguroso de perfiles de usuario y contraseñas. **Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de datos personales** El software realiza un cifrado al teclear la contraseña. **Administrador de perfiles de usuario y contraseñas** La Dirección Divisional de Sistemas y Tecnologías de la Información (DDSTI) se encarga de la creación de los perfiles a petición de la Dirección Divisional de Promoción y Servicios de Información Tecnológica (DDPSIT). DDPSIT se encarga de la autorización de nuevos perfiles. La DDSTI se encarga del registro de la creación de nuevos perfiles. **Acceso remoto al sistema de datos personales** Se puede ingresar al sistema únicamente desde los equipos instalados en el Instituto.

18. Bitácoras de acceso y operación cotidiana, seguridad aplicable (señalar con una X, según corresponda)		
	Soporte físico	No se cuenta con bitácoras ya que el acceso a los datos está restringido al personal autorizado.
	Soporte electrónico	No se cuenta con bitácoras ya que el acceso a los datos está restringido al personal autorizado.

19. Lugar de almacenamiento de las bitácoras y tiempo de conservación y conservación de integridad
N/A

20. Registro de incidentes
En el caso de los expedientes físicos se elabora un acta administrativa al día siguiente de haber identificado el incidente (extravío de expediente). Por lo que respecta a la plataforma electrónica, en caso de alguna incidencia esta se reporta a la DDSTI.

21. Procedimiento de respaldo y recuperación de datos
La Dirección Divisional de Promoción y Servicios de Información Tecnológica se encarga del resguardo físico de la información, la cual se escanea para contar con un repositorio electrónico de la información. La Dirección Divisional de Sistemas y Tecnología de la Información se encarga del resguardo de la información del sistema.

22. Plan de contingencia
No aplica

23. Encargado de datos (señalar con una X, según corresponda)				
Existe un prestador de servicios, persona física o moral, pública o privada ajena al IMPI que sola o conjuntamente, trate datos personales a nombre y por cuenta de este Instituto	SI		NO	**X**
22. Plazo de conservación de los datos personales	1 año*			

** En cumplimiento a la Ley General de Archivos que entró en vigor el 15 de junio de 2019 y derivado de la reunión sostenida con la Coordinación de Archivos, el Órgano Interno de Control y la Unidad de Transparencia el pasado 2 de septiembre de 2019, la Dirección Divisional de Promoción y Servicios de Información Tecnológica, está realizando acciones para la clasificación y organización de sus archivos.
Derivado de lo anterior, se está en proceso de regularización.

1000 DIRECCIÓN DIVISIONAL DE PROMOCIÓN Y SERVICIOS DE INFORMACIÓN TECNOLÓGICA					
1. Nombre del Sistema	FICHA DE INSCRIPCIÓN A CURSOS				
2. Objetivo	Proporcionar capacitación en materia de propiedad industrial				
3. Fundamento Legal	Estatuto Orgánico del Instituto Mexicano de la Propiedad Industrial Artículo 20 fracción I (D.O.F. 27/12/1999 última reforma 5/01/2018) ; Reglamento de Instituto Mexicano de la Propiedad Industrial Artículo 16 fracción I (D.O.F. 14/12/1999 última reforma 15/12/2017).				
4. DATOS PERSONALES QUE CONTIENE EL SISTEMA (señalar con una X, según corresponda)					
Dato personal	Idoneidad (informar para que se recaba el dato)				
Nombre y apellidos	Para su registro, verificar asistencia y emitir constancia.				
Edad (Rango)	Para fines estadísticos				
Sexo	Para fines estadísticos				
Profesión	Para fines estadísticos				
Institución / Empresa	Para fines estadísticos				
Teléfono fijo o celular	Para contactar al usuario en caso de ser necesario (cancelación, cambio de fecha u horario del curso).				
Correo electrónico	Contactar al usuario en caso de ser necesario (cancelación, cambio de fecha u horario y compartir material didáctico e informativo relativo con el curso).				
5. FORMA DE OBTENCIÓN DE LOS DATOS PERSONALES (señalar con una X, según corresponda)					
Directa	X	**Indirecta** (obtenida, creada, generada en algún otro sistema)			
Formulario físico	X	**Descripción:**			
Formulario electrónico	X				
Texto físico					
Texto electrónico					
Vía telefónica					
Otro					
6. Responsable del Sistema					
Nombre	Viviana Huerta García				
Cargo	Directora Divisional de Promoción y Servicios de Información Tecnológica				
Teléfono	5624-0400 Ext. 11110				
Correo electrónico	viviana.huerta@impi.gob.mx				
Función	Para generación de reportes.				
Obligación	Supervisar ejecución de los cursos.				
7. Administrador del Sistema					
Nombre	Alberto Olguín Nava				
Cargo	Subdirector Divisional de Servicios de Información Tecnológica				
Teléfono	5624-0400 Ext. 11079				
Correo electrónico	alberto.olguin@impi.gob.mx				
Función	Para generación de reportes. Elaboración de constancias.				
Obligación	Supervisar ejecución de los cursos.				
8. Usuarios u Operador del Sistema					
Nombre	Francisco Isaías Escutia Álvarez				
Cargo	Coordinador Departamental de Estudios de Difusión de la Propiedad Industrial				
Teléfono	5624-0400 Ext. 11912				
Correo electrónico	francisco.escutia@impi.gob.mx				
Función	Para generación de reportes. Elaboración de constancias. Designar expositores y dar seguimiento a la capacitación				
Obligación	Ejecución de los cursos.				
Observaciones:	Otros usuarios del sistema son personal autorizado adscrito a la Dirección Divisional de Promoción y Servicios de Información Tecnológica.				
9. Tipo de soporte (señalar con una X, según corresponda)					
*Electrónico		*Físico		*Ambos	X
*Descripción: La inscripción de los asistentes es a través del portal: https://cursosytalleres.impi.gob.mx/inscripcionCursos/Paginas/CursosPropiedadIntelectual.aspx (electrónico). Los asistentes que acuden sin haberse inscrito, capturan su nombre en la lista de asistencia a fin de que se emita su constancia (físico).					
10. Transferencias o transmisiones de datos personales (señalar con una X, según corresponda)					
*SI				NO X	
*Describir en que consiste la transferencia o transmisión NA					

11. Portabilidad de datos (señalar con una X, según corresponda)			
SI		NO	X
12. Nivel de protección que requieren los datos			
Nivel Básico			
13. Actualización de la información contenida en el sistema			
Semanal			
14. Plazo de conservación de los datos personales			
1 año **			
15. Medidas de Seguridad			
Físicas	Acceso restringido a las instalaciones, portabilidad de la credencial. Personal de seguridad.		
Administrativas	Seguridad relacionada a los recursos humanos. Cumplimiento de la normatividad.		
Técnicas	Control de Acceso.		
16. Acceso a instalaciones			
Seguridad perimetral exterior: en la entrada de las instalaciones el personal de seguridad únicamente permite el acceso al personal que labora en el Instituto y en el caso de los usuarios que solicitan asesorías se les requiere un registro y que presenten una identificación oficial para proporcionarles un gafete de visitantes. Seguridad interior: únicamente se permite el acceso al área de asesoría a personas que porten gafete de visitante. El Instituto cuenta con un sistema de circuito cerrado.			
17. Perfiles de usuario y contraseña			
Modelo de control de acceso: Está basado en perfiles de usuario. **Perfiles de usuario y contraseña en el sistema operativo de red** El sistema sí cuenta con un sistema operativo de red instalado en los equipos. El sistema operativo sí proporciona un manejo riguroso de perfiles de usuario y contraseñas. **Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de datos personales** El software realiza un cifrado al teclear la contraseña. **Administrador de perfiles de usuario y contraseñas** La Dirección Divisional de Sistemas y Tecnologías de la Información (DDSTI) se encarga de la creación de los perfiles a petición de la Dirección Divisional de Promoción y Servicios de Información Tecnológica (DDPSIT). DDPSIT se encarga de la autorización de nuevos perfiles. La DDSTI se encarga del registro de la creación de nuevos perfiles. **Acceso remoto al sistema de datos personales** Se puede ingresar al sistema únicamente desde los equipos instalados en el Instituto.			
18. Bitácoras de acceso y operación cotidiana, seguridad aplicable (señalar con una X, según corresponda)			
	Soporte físico	No se cuenta con bitácoras ya que el acceso a los datos está restringido al personal autorizado.	
	Soporte electrónico	No se cuenta con bitácoras ya que el acceso a los datos está restringido al personal autorizado.	
19. Lugar de almacenamiento de las bitácoras y tiempo de conservación y conservación de integridad			
N/A			
20. Registro de incidentes			
En el caso de los expedientes físicos se elabora un acta administrativa al día siguiente de haber identificado el incidente (extravío de expediente). Por lo que respecta a la plataforma electrónica, en caso de detectar alguna incidencia se reporta a la DDSTI.			
21. Procedimiento de respaldo y recuperación de datos			
La Dirección Divisional de Promoción y Servicios de Información Tecnológica se encarga del resguardo físico de la información, la cual se escanea para contar con un repositorio electrónico de la información. La Dirección Divisional de Sistemas y Tecnología de la Información se encarga del resguardo de la información del sistema.			
22. Plan de contingencia			
No aplica			
23. Encargado de datos (señalar con una X, según corresponda)			
Existe un prestador de servicios, persona física o moral, pública o privada ajena al IMPI que sola o conjuntamente, trate datos personales a nombre y por cuenta de este Instituto	SI		NO	**X**
22. Plazo de conservación de los datos personales	1 año**			

** En cumplimiento a la Ley General de Archivos que entró en vigor el 15 de junio de 2019 y derivado de la reunión sostenida con la Coordinación de Archivos, el Órgano Interno de Control y la Unidad de Transparencia el pasado 2 de septiembre de 2019, la Dirección Divisional de Promoción y Servicios de Información Tecnológica, está realizando acciones para la clasificación y organización de sus archivos.
Derivado de lo anterior, se está en proceso de regularización.

6. MEDIDAS DE SEGURIDAD

Las medidas de seguridad que fueran abordadas, se consideraron en tres vertientes: administrativas, físicas y técnicas.

Medidas de seguridad Físicas: Son el conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.

Medidas de seguridad Administrativas: Son las políticas y procedimientos que se implementan para la gestión, soporte y revisión de la seguridad de los recursos y de la información a nivel organizacional, mismos que se traducen en acciones para la identificación de información que involucre datos personales, identificación de riesgos y su prevención, clasificación de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales.

Medidas de seguridad Técnicas: Son el conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.

15. MEDIDAS DE SEGURIDAD GENERALIZADAS EN MATERIA DE TECNOLOGIAS DE LA INFORMACIÓN	
Físicas	La Dirección Divisional de Administración a través de la Subdirección Divisional de Recursos Materiales y Servicios Generales salvaguarda la integridad y seguridad de las personas, bienes, activos e instalaciones de la SFP, mediante procedimientos y mecanismos institucionales de identificación y prevención de riesgos de seguridad, como son: **Prevenir el acceso no autorizado al perímetro de la organización (SFP), sus instalaciones físicas, áreas críticas, recursos e información.** -Se cuenta con un contrato de prestación de servicios de seguridad y vigilancia con la Policía Bancaria e Industrial, que tiene por objeto la vigilancia protección a instalaciones, bienes y personas en los inmuebles que ocupa la Dependencia. Tiene capacidad de respuesta inmediata y se ejecutan medidas de prevención, contención, neutralización y mitigación de los efectos adversos en el interior y periferia de los inmuebles, es decir, resguardan las instalaciones físicas, áreas críticas, recursos e información las 24 horas, los 365 días del año, mediante: control de accesos y uso de gafetes, control en recepción. vigilancia en sótanos, control en estacionamientos y apoyo en vialidad periférica, adicionalmente de contar con bardas perimetrales y puertas con cerradura y candado que son vigiladas.

	II. Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas del IMPI así como a sus recursos e información. -Se cuenta con normas, procedimientos y medidas de seguridad contemplados en el Programa Interno de Protección Civil, que contienen el diseño y establecimiento de lineamientos de salvaguarda aplicables al interior de los inmuebles, considerando sus características y el tipo de actividad o servicio prestado, con el propósito de reducir al mínimo la incidencia de riesgos como: protocolo de acceso a las áreas estratégicas, protocolo de sismos y protocolo de incendio. **Proteger los recursos móviles. portátiles y cualquier soporte físico o electrónico** -Se cuenta con mecanismos para identificar y proteger equipos móviles y portátiles; mobiliarios, documentos y materiales mediante controles de entrada y salida, como son:' control en el uso de aparatos eléctricos y electrónicos, inspección ocular al ingreso y egreso de las instalaciones de los aparatos, equipos, mobiliario, documentos y materiales mediante pase de salida autorizado por el superior competente.
Técnicas	**Política de seguridad.** - Se cuenta con Políticas de Seguridad para protección de la información. - Se cuenta con una Guía de Responsabilidades en Materia de Seguridad de la Información del empleado del instituto, la cual se da a conocer a los empleados en su proceso de contratación y se pone a la disposición en la intranet Institucional. Se cuenta con políticas que establecen que cada servidorpúblico será responsable de los equipos, su uso y de la información y datos personales que son utilizados de los que son conocedores con motivo de su encargo Cumplimiento de la normatividad. - La adopción de medidas necesarias para garantizar la integridad, confidencialidad y disponibilidad; se realiza a través del cumplimiento de los controles mínimos de seguridad de la información como lo requisita el MAAGTICSI en el proceso ASI 6 en su factor crítico 1 - Se cuenta con cartas de aceptación de riesgos en las cuales se mencionan los controles a implementar por cada dominio tecnológico bajo el marco de MAAGTICSI e ISO/IEC27001 y 27002. **Control de acceso.** - Resguardo de los equipos que funcionan como repositorio en área especial dedicada (centro de cómputo) con acceso restringido y vigilancia 7x24x365. - El acceso al centro de cómputo es controlado y restringido por la DDSTI. - El control de acceso en puerta al SITE, se realiza por doble factor, biométrico (huella digital) y password. - Se cuenta con registro en bitácora manual y electrónica sobre los accesos al centro de

	cómputo. -Se tiene video vigilancia con monitoreo vía intranet e internet. - Los accesos a los activos e información son controlados por el dominio tecnológico a cargo del mismo, generando las listas autorizadas de acceso. - El acceso a aplicativos que puedan resguarden información personal es controlado y restringido usuarios autorizados, mediante validación por usuario y contraseña y basada en roles el acceso. **Adquisición, desarrollo, uso y mantenimiento de sistemas de información** Integración de controles de seguridad a los sistemas de información, desde su adquisición o desarrollo, durante su uso y mantenimiento, hasta su cancelación o baja definitiva. Considera procesamiento adecuado en las aplicaciones, controles criptográficos y seguridad de los archivos de sistema, entre otros. - Acceso restringido a la información con uso de cuenta personal. (Sistemas operativos, Bases de Datos, aplicativos de gestión y resguardo) - Acceso restringido a la información con base en roles. **Organización de la seguridad de la información.** - Existencia de Grupos de trabajo para evaluación e implementación de seguridad de la información. - Cartas de Responsables de Dominios Tecnológicos. - Designación del RSI - Designación del ERISC ante el CNI. - Identificación de riesgos a la información mediante mapas de operación. - Tratamiento de los riegos mediante análisis y SOA de los mismos. - Implementación de controles mínimos y basados en análisis de los mismos. - Revisión periódica de los controles implementados. **Clasificación y control de activos.** - Se cuenta con catálogos de activos e infraestructuras críticas del Instituto que pueden resguardar información de datos personales. - Se cuenta con análisis de riegos de activos e infraestructuras críticas del Instituto que pueden resguardar información de datos personales. **Seguridad relacionada a los recursos humanos.** Responsivas para el uso de claves privilegiadas y tratamiento de información. - Se cuenta con cartas de uso de claves y equipo de cómputo, los cuales permiten acceso a aplicativos con información que pudiesen contener datos personales, las cartas son entregadas a todos los empleados del Instituto y firmadas por los mismos. - Se cuenta con cartas de confidencialidad y responsabilidad de uso de claves, las cuales permiten acceso a aplicativos con información almacenada que pudiesen contener datos personales, las cartas son firmadas por los administradores de los dominios

	tecnológicos. - Asignaciones de personal responsables de los activos de resguardo de información. **Administración de incidentes.** - Administración de incidentes de seguridad, gestión y tratamiento - Evaluación de pruebas de penetración y vulnerabilidad a los aplicativos informáticos. - Base de datos de conocimiento sobre incidentes para tratamiento de brechas. **Continuidad de las operaciones.** - Se cuenta con respaldo de información en cinta, las cuales se encuentran alojadas en bóveda externa de seguridad, para su uso en caso de caídas en la operación.

7. MEDIDAS DE SEGURIDAD

8. ANÁLISIS DE RIESGOS

9. ANÁLISIS DE BRECHA

10. PLAN DE TRABAJO

11. MECANISMOS DE MONITOREO Y REVISION DE LAS MEDIDAS DE SEGURIDA

En este apartado deben incluirse las consideraciones sobre riesgos existentes y la posibilidad de mitigarlos, a través de un análisis cualitativo, sobre el impacto y la probabilidad de que una amenaza vulnere la seguridad, tanto en la información de los datos personales, como en los recursos involucrados. Para ello habrán de tomarse en cuenta los siguientes puntos :

Regulación (códigos de conducta o mejores prácticas en la materia)

Valor de los datos personales y su sensibilidad

Consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad

Desarrollo tecnológico

Consecuencias de una vulneración para los titulares;

Número de titulares;

Vulneraciones previas ocurridas;

LA INFORMACIÓN DE LOS APARTADOS 7, 8, 9,10 Y11 SE ENCUENTRA EN PROCESO DE ACTUALIZACIÓN, DERIVADO DE QUE LA LEY DE LA PROPIEDAD INDUSTRIAL PUBLICADA ORIGINALMENTR COMO LEY DE FOMENTOA LA PROTECCIÓN DE LA PROPIEDAD INDUSTRIAL EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 27 DE JUNIO DE 1991, SERA ABROGADA, CON LA ENTRADA EN VIGOR DE LA LEY FEDERAL DE PROTECCIÓN A LA PROPIEDAD INTELECTUAL PUBLICADA EL 01-07-2020 DE CONFORMIDAD CON LO DISPUESTO EN SUS TRANSITORIOS. SIENDO QUE DEBERÁ REDEFINIRSE EL IMPACTO DE LAS ESTRUCTURAS CRITICAS, ACTIVOS, COSTOS ASOCIADOS Y EXPOSCIÓN DE LA INFORMACIÓN GENERADA A PARITR DE LOS NUEVOS SISTEMAS EN LINEA QUE FUERAN DESARROLLADOS, ES ASÍ QUE LA INFORMACIÓN QUE EN SU MOMENTO SE GENERO YA NO SURTE EFECTOS.