DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE LOS DATOS PERSONALES

2024

Documento de Seguridad para la Protección de los Datos Personales

INDICE

INTRODUCCIÓN

En la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León se establecen las bases, principios, procedimientos y tratamiento que permite garantizar la protección de datos personales de los ciudadanos en posesión del Instituto de Innovación y Transferencia de Tecnología (I2T2), como sujeto obligado. Con base en dicha normatividad, y en cumplimiento a lo establecido en el artículo 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada en el Diario Oficial de la Federación el día 26 de enero de 2017; en relación al artículo 41 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León, publicada en el Periódico Oficial número 153, de fecha 11 de diciembre de 2019; se crea el presente documento de seguridad.

Desde la emisión de la Ley en referencia, el Instituto de Innovación y Transferencia de Tecnología (I2T2), en conjunto con los encargados de cada área generadora de información, se llevaron a cabo las acciones y actividades que tuvieron como finalidad establecer los principios para la creación de este documento.

Para recabar la información precisa, se aplicó un cuestionario a los Titulares de las Unidades Administrativas del I2T2, con la finalidad de detectar las medidas de seguridad con las que cuenta cada área y definir posibles riesgos.

Una vez contestado el cuestionario, se analizó la información recabada, lo que permitió la creación de las medidas de seguridad que integran el presentedocumento de seguridad, que tienen como objetivo propiciar la protección de los datos personales de la forma más completa, para alcanzar el adecuado tratamiento de los datos personales.

GLOSARIO

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

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.

Hardware: es el conjunto de componentes físicos de los que está hecho el equipo.

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

I2T2: Instituto de Innovación y Transferencia de Tecnología

INFONL: Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales.

JUT: Jefatura de Unidad de Transparencia

LGPDPPSO: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

LPDPPSONL: Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León.

Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permiten garantizar la protección, confidencialidad, disponibilidad e integridad de los datos personales.

Medidas de seguridad administrativas: Políticas y procedimiento para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional.

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.

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 recursos involucrados en su tratamiento.

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.

Respaldo: es una copia de la información que una organización genera, utiliza y actualiza a lo largo del tiempo; también este término se emplea para referirse a las copias de seguridad que se llevan a cabo en los sistemas de información, bases de datos, software de aplicación, sistemas operativos, utilerías, entre otros. El objetivo de un respaldo es garantizar la recuperación de la información, en caso de que haya sido eliminada, dañada o alterada al presentarse alguna contingencia.

Titular: Persona física a quien pertenecen los datos personales.

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

Tratamiento: De manera enunciativa más no limitativa cualquier operación o conjunto de operaciones efectuadas mediante procedimiento 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 los datos personales.

Sistema de Datos Personales: Todo conjunto organizado de archivos, registros, ficheros, bases o banco de datos personales de los entes públicos, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso.

Software: es el conjunto de programas o aplicaciones, instrucciones y reglas informáticas que hacen posible el funcionamiento del equipo.

Unidad administrativa: Son aquellas unidades creadas mediante alguna normatividad previamente establecida, con atribuciones específicas, que forman parte de la base orgánica de las dependencias y entidades que integran a la Administración Pública.

INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Se entiende por "inventario de sistemas de tratamiento de datos personales", al control de documentos y tratamiento de datos personales que realizan las unidades administrativas de Instituto de Innovación y Transferencia de Tecnología (I2T2), que se encuentran almacenados tanto física como electrónicamente.

Dichos sistemas de tratamiento de datos personales, se presentan por unidades administrativas previstas con base en la estructura orgánica y el Reglamento Interior del Instituto de Innovación y Transferencia de Tecnología de Nuevo León, mismas que cuentan o pueden contar, dar tratamiento, y ser responsables o encargados de los datos personales.

El inventario de datos personales se advierte en la LGPDPPSO en los artículos 33 fracción III y 35 fracción I; en relación a los artículos 38 fracción III y 41 fracción I de la LPDPPSONL.

Descripción y estructura de las bases de datos o sistemas de tratamiento de datos personales.

En la descripción de cada base o sistema de tratamiento de datos personales, se indica cuáles son los datos personales que se recaban, con qué finalidad se obtienen, así como su forma de obtención, el fundamento legal que faculta al área administrativa para el tratamiento de dichos datos personales, los medios de almacenamiento, sitios de resguardo, si existe un encargado que actúe a cuenta y nombre del I2T2 y el servidor público encargado de administrar la base o sistema de tratamiento de datos personales, así como los subordinados que tienen acceso a las mismas. (Ver anexo 1).

Es importante destacar que la Jefatura de Unidad de Transparencia**,** solicitó de manera oportuna a las unidades administrativas del I2T2 que informasen sobre los sistemas de

tratamiento con los que cuenta cada área, por lo tanto, el presente documento está integrado con la información brindada por las unidades administrativas, remitiéndoles la siguiente tabla:

Unidad Administrativa	Área administrativa del sujeto obligado que figura como responsable del tratamiento de datos personales
Base de datos o sistema de tratamiento	Denominación de la base o sistema de tratamiento de datos personales que utiliza el área administrativa de esta Contraloría
Categoría de los datos personales	Datos de identificación y contacto, Datos sobre características físicas, Datos laborales, Datos académicos,Datos patrimoniales y/o financieros, Datos biométricos, etc.
Datos personales que se recaban	Todos aquellos datos en específico que recaba el área administrativa.
Finalidad para la cual se obtuvieron (especificar si es finalidad principal o secundaria)	Todo tratamiento de datos personales que efectúe el responsable debe estar justificado por finalidades concretas,lícitas, explícitas y legítimas, relacionadas con las atribuciones que normatividad aplicable les confiera. **Finalidad principal**: Dan origen y son necesarias para la relación jurídica. **Finalidad secundaria:** No son necesarias para la relación jurídica (publicidad, mercadotécnica)
Fundamento legal que faculta para el tratamiento	El tratamiento de datos personales por parte del responsable deberá sujetarse a las facultades o atribuciones que la normatividad aplicable les confiera.
Formade obtención directa/indirectamente del titular medios físicos/electrónicos	Directamente del titular: • De manera personal, con la presencia física del titular de los datos personales o su representante, en su caso. • Vía telefónica. • Por correo electrónico. • Por Internet o sistema informático. • Por escrito presentado directamente en las oficinas del sujeto obligado. • Por escrito enviado por mensajería Mediante una transferencia: • Quién transfiere los datos personales y para qué fines • Medios por los que se realiza la transferencia De una fuente de acceso público: • Las páginas de Internet o medios remotos o locales de comunicación electrónica, óptica y de otra tecnología, siempre que el sitio donde se encuentren los datos personales esté concebido para facilitar información al público y este abierto a la consulta general; • Los directorios telefónicos en términos de la normativa específica; • Los diarios, gacetas o boletines oficiales de acuerdo con su

	normativa, • Los medios de comunicación social, y • Los registros públicos conforme a las disposiciones aplicables.
Medios de almacenamiento físicos/electrónicos	**Físico:** Todo recurso inteligible a simple vista y con el que se puede interactuar sin la necesidad de ningún apartado que procese su contenido para examinar, modificar o almacenar datos personales, por ejemplo, los expedientes de personal almacenados en un archivero. En este sentido hay que considerar cuantos especiales, muebles, cajones y cualquier espacio donde se guardenformatos físicos, o bien equipos de cómputo u otros medios de almacenamiento. **Electrónico:** Todo recurso al que se puede acceder sólo mediante el uso de equipo de cómputo (cualquier dispositivoelectrónico que permita el procesamiento de información, por ejemplo, computadoras de escritorio, laptops, tabletas,teléfonos inteligentes, entre otros) que procese su contenido para examinar, modificar o almacenar los datos personales. Podemos considerar, por ejemplo, discos duros (tanto propios del equipo de cómputo como los portátiles), memorias extraíbles como USB o CD's, entre otros. También podemos contemplar como medio de almacenamiento electrónico, el uso de servicios de almacenamiento en línea.
Sitios de resguardo	Toda locación donde se resguarden los medios dealmacenamiento, tanto físicos como electrónicos (ejemplo: casa, I2T2, instalaciones de un tercero).
Servidores públicos que tiene acceso a los sistemas de datos personales	Personal adscrito al I2T2cia de Tecnología autorizado para llevar a cabo el tratamiento de datos personales
Encargado	Servidor público designado para que solo o juntamente con otras trate datos personales a nombre y por cuenta del responsable.
Ciclo de vida y riesgo inherente de los datos personales	Es el tratamiento para los datos personales que son recabados y los cuales no deben ser excesivos. El ciclo de vida consiste en conservar, transferir, bloquear o suprimirse por haber cumplido con las finalidades por las que fue recabado.

En el caso de la sección de "*categoría de los datos personales"*, de la referida tabla, a continuación, se describen los tipos de datos personales que pueden estar sujetos a tratamiento de acuerdo con las atribuciones de cada unidad administrativa:

- Datos de identificación y contacto: nombre, estado civil, RFC, CURP, lugar de nacimiento, fecha de nacimiento, nacionalidad, domicilio, teléfono particular, teléfono celular, correo electrónico, firma autógrafa, edad, fotografía y referencias personales.
- Datos biométricos: huella dactilar.
- Datos laborales: puesto o cargo que desempeña, domicilio de trabajo, correo electrónico institucional, teléfono institucional, referencias laborales, información generada durante los procedimientos de reclutamiento, selección y contratación y experiencia/capacitación laboral.
- Datos académicos: trayectoria educativa, título, cédula profesional, certificados y reconocimientos.
- Datos patrimoniales y/o financieros: ingresos, egresos y cuentas bancarias.
- Datos legales: situación jurídica de la persona (juicios, amparos, procesos administrativos, entre otros)
- Datos personales de naturaleza pública: Datos que por mandato legal son de acceso público.

En el caso de la sección de "*forma de obtención directa / indirectamente del titular medios físicos / electrónicos"*, de la referida tabla, a continuación, se describen el tipo de personas de quienes se obtienen y cómo se recaban datos personales que pueden estar sujetos a tratamiento de acuerdo con las atribuciones de cada unidad administrativa:

- Personas que laboran en el I2T2.
- Personas externas que prestan algún servicio para el I2T2.
- Personas externas que participan en actividades que llevan a cabo las direcciones del I2T2. (capacitaciones y concursos)
- Los datos personales se recaban por medio de documentos presentados y/o por el llenado de formularios físicos y/o electrónicos por los titulares de los datos personales.

LAS FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATAN DATOS PERSONALES

Para la aplicación correcta de este sistema es necesario establecer los deberes de los servidores públicos del Instituto de Innovación y Transferencia de Tecnología, que participan en el tratamiento de los datos personales derivado de sus atribuciones.

Al momento de recibir los datos personales, el servidor público responsable de su recepción deberá:

1) Tener a la vista el Aviso de Privacidad.

2) Dar a conocer el aviso de privacidad al titular de los datos personales previo a la obtención de sus datos.

3) En caso de dudas o quejas de los titulares de los datos personales sobre el tratamiento de sus datos, orientar al ciudadano para que acuda a la Jefatura de Unidad de Transparencia del I2T2.

4) Al obtener los datos personales cerciorarse de que la información esté completa, actualizada, sea veraz, y comprensible.

5) Comunicar discrepancias de los datos personales recabados a su jefe inmediato o al administrador de los datos personales, ello cuando se dé cuenta.

6) Conocer y seguir las medidas de seguridad que le sean aplicables para el cuidado de los datos personales, durante el periodo en el que posea los datos personales.

7) Recabar los datos personales para la finalidad para la cual, estos fueron recabados según el trámite o el sistema de tratamiento que corresponda.

8) Tratar los datos personales de manera lícita siguiendo los principios establecidos en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Nuevo León.

9) Conocer, aplicar y sujetarse al Aviso de Privacidad y al Documento de Seguridad del Instituto de Innovación y Transferencia de Tecnología, en el tratamiento de datos personales.

10) Guardar estricta confidencialidad de los datos personales que conozca en el ejercicio de sus funciones.

11) Tomar por lo menos, una vez al año un curso, taller o capacitación sobre el tratamiento de datos personales.

12) Sujetarse a lo establecido en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León.

El servidor público involucrado en el tratamiento de datos personales deberá:

1) Conocer, aplicar y sujetarse al Aviso de Privacidad y al Documento de Seguridad del Instituto de Innovación y Transferencia de Tecnología, en el tratamiento de datos personales.

2) Aplicar las medidas de seguridad correspondientes a los datos personales tratados y/o el sistema de protección en el que participa.

3) Tratar los datos personales de manera lícita siguiendo los principios establecidos en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León.

4) En caso de dudas o quejas de los titulares de los datos personales sobre el tratamiento de sus datos, orientar al ciudadano para que acuda a la Jefatura de Unidad de Transparencia del

Instituto de Innovación y Transferencia de Tecnología.

5) Guardar estricta confidencialidad de los datos personales que conozca en el ejercicio de sus funciones.

6) Abstenerse de realizar transferencias de datos personales que no vayan de conformidad con la finalidad para la cual se obtuvieron los datos.

7) Tomar, una vez al año, un curso, taller o capacitación sobre el tratamiento de datos personales.

8) Sujetarse a lo establecido en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León.

El servidor público que administra los datos personales, conforme los sistemas de tratamiento vigentes deberán:

1) Conocer, aplicar y sujetarse al Aviso de Privacidad y al Documento de Seguridad del I2T2, en el tratamiento de datos personales.

2) Conocer e implementar las medidas de seguridad establecidas en el documento de seguridad.

3) Aplicar nuevas medidas de seguridad que resulten accesibles y viables para la protección de datos personales.

4) Supervisar a los servidores públicos que participan en la recepción y en el tratamiento de datos personales en cada trámite o sistema.

5) Tratar los datos personales para la finalidad para la cual estos fueron recabados según el trámite o el sistema de tratamiento que corresponda.

6) Tratar los datos personales de manera lícita siguiendo los principios establecidos en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León.

7) Guardar estricta confidencialidad de los datos personales que conozca en el ejercicio de sus funciones.

8) Tomar por lo menos, una vez al año, un curso, taller o capacitación sobre el tratamiento de datos personales.

9) Informar a los titulares de los datos sobre nuevas finalidades del tratamiento de datos personales o nuevas transferencias.

10) En caso de dudas o quejas de los titulares de los datos personales sobre el tratamiento de

sus datos, orientar al ciudadano para que acuda a la Jefatura de Unidad de Transparencia del I2T2.

9) Informar a la Jefatura de Unidad de Transparencia del I2T2, sobre los cambios que sufran sus trámites o sistemas de tratamiento dedatos personales, los riesgos y las vulneraciones que surjan en el tratamiento de los datos personales, las medidas correctivas implementadas y las transferencias nuevas que realicen de los datos personales.

10) Acudir a la Jefatura de Unidad de Transparencia del I2T2 en caso de requerir asesoría sobre el tratamiento de datos personales.

11) Monitorear de manera cotidiana la implementación de las medidas de seguridad y levantar actas circunstanciadas de hechos ante la reincidencia de un incumplimiento en la aplicación de las mismas.

12) Dar aviso al Comité de Transparencia, a través de la Jefatura de Unidad de Transparencia del I2T2, sobre las actas circunstanciadas de hechos levantadas por el incumplimiento del documento de seguridad y sobre el seguimiento de las mismas.

13) Sujetarse a lo establecido en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León.

El servidor público o el titular de la UnidadAdministrativa responsable de cada sistema, deberá:

1) Conocer, aplicar y sujetarse al Aviso de Privacidad y al Documento de Seguridad del Instituto de Innovación y Transferencia de Tecnología, en el tratamiento de datos personales.

2) Implementar las medidas de seguridad que establece el documento de seguridad.

3) Guardar estricta confidencialidad de los datos personales que conozca en el ejercicio de sus funciones.

4) Tomar por lo menos una vez al año un curso, taller o capacitación sobre el tratamiento de datos personales.

5) En caso de dudas o quejas de los titulares de los datos personales sobre el tratamiento de sus datos, orientar al ciudadano para que acuda a la Jefatura de Unidad de Transparencia del I2T2.

6) Aplicar medidas correctivas en caso de identificar incidentes, alteraciones o vulneraciones en el tratamiento de datos personales.

7) Informar a la Jefatura de Unidad de Transparencia del I2T2 sobre los cambios que sufran sus trámites o sistemas de tratamiento de datos personales, los riesgos y las vulneraciones que surjan en el tratamiento de los datos personales, las medidas correctivas implementadas y las transferencias nuevas que realicen de los datos personales.

8) Monitorear la implementación de las medidas de seguridad.

9) Monitorear de manera cotidiana la implementación de las medidas de seguridad y levantar actas circunstanciadas de hechos ante la reincidencia de un incumplimiento en la aplicación de estas.

10) Dar aviso al Comité de Transparencia, a la Jefatura de Unidad de Transparencia del I2T2 sobre las actas circunstanciadas de hechos levantadas por el incumplimiento del documento de seguridad y sobre el seguimiento de estas.

11) Presentar propuestas de mejora o modificación del documento de seguridad a través de la Jefatura de Unidad de Transparencia del Instituto de Innovación y Transferencia de Tecnología

12) Emitir reportes en relación con el tratamiento de los datos personales y la aplicación de medidas de seguridad, según sea requerido por el Comité de Transparencia a través de la Jefatura de Unidad de Transparencia del Instituto de Innovación y Transferencia de Tecnología.

13) Diseñar, desarrollar e implementar políticas públicas, procesos internos, y/o sistemas o plataformas tecnológicas necesarias para el ejercicio de sus funciones apegándose en todo momento al documento de seguridad, las políticas o lineamientos que para el tratamiento de datos personales emita el Comité de Transparencia, el INFO NL, INAI, así como a la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León.

14) Sujetarse a lo establecido en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León.

Son obligaciones del responsable de la Unidad de Transparencia en relación al tratamiento de datos personales, además de las previstas en el artículo 99 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León:

1) Difundir al interior los avisos de privacidad y el documento de seguridad.

2) Revisión física anual a dos unidades administrativas sobre el tratamiento de datos personales y la implementación de medidas de seguridad, mismas que serán sugeridas por el Comité de Transparencia.

3) Proponer al Comité de Transparencia actualizaciones o modificaciones al documento de seguridad.

4) Emitir un reporte anual al Comité de Transparencia sobre el ejercicio de estas funciones.

El Comité de Transparencia es la autoridad máxima en materia de protección de datos personales dentro del Instituto de Innovación y Transferencia de Tecnología.

Son obligaciones del Comité de Transparencia en relación con el tratamiento de datos personales, además de las previstas en el artículo 98 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León:

1) Revisar anualmente las políticas y/o lineamientos en materia de protección de datos personales establecidos en el presente documento.

2) Emitir o aprobar anualmente un programa de capacitaciones en materia de protección de datos personales.

3) Requerir anualmente a las áreas responsables que tratan datos personales, a través de la Jefatura de Unidad de Transparencia, informes sobre el tratamiento de los datos personales y la aplicación de medidas de seguridad, así como vulneraciones detectadas en el año.

ANÁLISIS DE RIESGOS

Debido a las circunstancias generales, tecnológicas como humanas, en las que se tratan datos personales, se identifican los posibles riesgos respecto a datos personales:

Origen de la amenaza	Causa	Posibles consecuencias
Acceso no autorizado a datos personales	Adquirir información o datos personales.	Divulgación de datos personales.Robo de información. Modificaciones no autorizadas.
Alteración o pérdida de datos personales no intencionada	Tratamiento inadecuado de la información.	Falta de disponibilidad íntegra dedatos personales
Daño físico	Agua, fuego, accidentes o corrosión.	Daño o pérdida de losdatos personales.
Eventos naturales	Fenómenos meteorológicos. Sismos. Cualquier eventualidad por causa natural.	Daño o pérdida de losdatos personales.
Fallas técnicas.	Pérdida de electricidad. Vulneraciones en sistemas, bases de datos, redes, correos electrónicos	Daño o pérdida de los datos personales. Divulgación y transferencia de datos personales. Modificaciones no autorizadas.

ANÁLISIS DE BRECHA

Para realizar el análisis de brecha, la Jefatura de Unidad de Transparencia del I2T2, elaboró y aplicó un cuestionario con el objetivo de efectuar un autodiagnóstico que determine el nivel de desempeño real esperado en cuanto a las medidas de seguridad del I2T2.

Una vez identificados los posibles riesgos a los que este Sujeto Obligado se encuentra susceptible de enfrentar, podemos realizar el análisis de brecha, utilizando como base las entrevistas que se hicieron con las diferentes unidades administrativas del I2T2.

Del resultado de las encuestas a los servidores públicos adscritos a las unidades administrativas reportaron las siguientes medidas de seguridad existentes:

- Quien recaba los datos personales, es un servidor público del área, asignado especialmente para recabar datos en general necesarios para cada trámite.
- Cuando los datos personales son recabados de forma digital, se realiza por medio de plataformas oficiales o correo electrónico oficial.
- Las llaves que se tienen de cada área se encuentran en manos de servidores públicos, autorizados por cada área.
- Una vez recabados los datos personales, el servidor público genera un expediente para cada trámite o servicio, del cual se obtuvieron los datos personales, ya sea físico o electrónico.
- Una vez recabados los datos personales, ya realizada la carpeta o expediente (electrónica, física, en plataformas, o cualquiera generada) y guardada está en archiveros o puesta en resguardo electrónico, solo tendrán acceso a estos los servidores públicos del área.
- Las llaves de los archiveros con las que se cuentan se encuentran en posesión de servidores públicos encargados del área.
- Una vez recabados los datos personales, en caso de que se les dé proceso electrónico, el servidor público guarda los mismos en carpeta electrónica, ya sea en su computadora, carpeta compartida, correo electrónico oficial o plataforma.
- Durante el desahogo del trámite del cual se obtuvieron los datos personales, los servidores públicos del área tienen acceso a los datos personales.
- Una vez concluido el trámite, los datos personales recabados se dejan intactos en la carpeta, archivo o expediente del trámite al que pertenecen.
- Cada carpeta de trámites o archivo, al terminar el proceso de cada uno, son resguardados en un archivo de cada área.

MEDIDAS DE SEGURIDAD EN EL I2T2

Medidas de seguridad físicas

El I2T2 deberá implementar como mínimo las siguientes medidas generales deseguridad física, para evitar daños, sustracciones o intromisiones no autorizadas en las instalaciones y archivos de información del sujeto obligado:

I. Asignar un espacio seguro y adecuado para el tratamiento de datos personales, que no se encuentre a la vista del público y que preferentemente no sea un área de paso frecuente por el personal de trabajo o ajeno al mismo.
II. Tener bajo llave o asegurados los archiveros, archivos, cajas y almacenes en donde se encuentre almacenada la información de datos personales.
III. Inventariar el contenido de cada archivo o caja en donde se encuentre información con datos personales y actualizarlo cotidianamente.
IV. Evitar que se dejen descuidados o sin la atención debida documentos que contengan datos personales.
V. Establecer un plan de contingencia con protocolos de seguridad, que incluya, cuando menos, la designación de responsables por piso, procedimientos de control, señalizaciones y medidas de protección física contra incendio, inundación, sismo, explosión y cualquier otra forma de desastre natural o humano.
VI. Verificar que en ningún caso los documentos que contengan datos personales se utilicen como papel reciclable ni de doble uso, ya que una vez transcurridos los plazos en que deban cancelarse o al tratarse de proyectos no utilizables, deberán ser destruidos.

El I2T2 deberá adoptar como mínimo las siguientes medidas de seguridad en el entorno, para evitar el acceso físico no autorizado a las instalaciones y a su información:

I. Registrar a visitantes que accedan a instalaciones y el motivo de su visita
II. Contar con un guardia de seguridad en la puerta de las instalaciones del I2T2
III. Identificar a los servidores públicos adscritos al sujeto obligado.

Medidas de seguridad administrativas

Medidas de seguridad administrativas relacionadas con el recurso humano: para asegurar que tanto los servidores públicos como terceros con quienes se tenga una relación contractual, sean aptos y de perfil idóneo para desarrollar sus responsabilidades, funciones u obligaciones contractuales, según corresponda, en el tratamiento y protección de datos personales, buscando reducir con ello el riesgo de robo, fraude, transmisiones no autorizadas o en general,

cualquier mal uso de esta información, se deberán implementar las siguientes acciones:

I. Definir adecuadamente el perfil del servidor público, empleado o contratista que realiza o realizará las funciones relacionadas con el tratamiento de datos personales;
II. Verificar los antecedentes de los candidatos al empleo en el servicio público, contratistas u otros terceros con que se inicie una relación contractual, cuyas labores estarán relacionadas con el tratamiento de datos personales en posesión de sujetos obligados;
III. Realizar cuando resulte pertinente, una reorganización interna, según los perfiles autorizados, de los servidores públicos que deberán dar tratamiento a la información de datos personales, sin afectación de derechos laborales;
IV. Capacitar de manera periódica a los servidores públicos que lleven a cabo el tratamiento de datos personales para que se especialicen, concienticen y actualicen en relación con las medidas que se deben adoptar, los procedimientos de seguridad y el uso correcto de los medios disponibles para el procesamiento de la información con el objeto de minimizar los posibles riesgos;
V. Suscribir acuerdos de confidencialidad con servidores públicos o terceros que actualmente estén relacionados con la seguridad de los servicios de procesamiento de la información y el tratamiento de datos personales en posesión de sujetos obligados, según resulte procedente o bien comunicarles las responsabilidades de tipo administrativo o penal en caso de incumplimiento a la normatividad aplicable.

Se deberán implementar las siguientes medidas de seguridad en la finalización o modificación de la relación laboral o contractual, para que una vez que concluya o se modifique la misma con los empleados base, sindicalizados o por honorarios, o bien, con contratistas o terceras personas, se adopten las medidas necesarias para la desvinculación organizada de funciones e información, reiterando la subsistencia del deber de respeto a los principios de confidencialidad, máxima privacidad y seguridad en términos de la legislación aplicable:

I. Establecer un procedimiento de devolución de activos y cualquier tipo de información que les haya sido remitida, que debe incluir el borrado efectivo de los datos, una vez que se desvinculen del personal respectivo o se produzca el cese del contrato o relación laboral correspondiente;
II. Retirar o modificar, según corresponda, los derechos de acceso del personal en estos supuestos, mediante un procedimiento de baja de usuarios en los sistemas de información y datos personales, que incluya la revocación de sus cuentas de acceso y privilegios;
III. Actualizar el documento de seguridad en lo relacionado con el padrón de servidores públicos Responsables y Encargados que sean designados;
IV. Identificar y revisar regularmente que los acuerdos de confidencialidad y protección de la información no pierdan vigencia y contemplen la no divulgación de los datos personales;
V. Establecer vías idóneas para recordar al personal que subsisten los deberes derespeto

a los principios de confidencialidad y secrecía en relación con la informaciónde datos personales a la que tuvieron conocimiento o acceso con motivo de suempleo, cargo o prestación de servicio, independientemente de que haya concluido ya su fase de acceso o cualquier otro tipo de tratamiento.

Medidas de seguridad técnicas

Las medidas de seguridad técnicas consisten en mecanismos que se valen de la tecnología, aseguran el acceso a las bases de datos relacionados con el software y hardware, es decir protegen el entorno digital de los datos personales.

El Instituto de Innovación y Transferencia de Tecnología, deberá implementar como mínimo las siguientes **medidas de seguridad en la administración y control de los soportes o Sistemas de Datos Personales**, para evitar daños, sustracciones o intromisiones no autorizadas:

I. Requerir el apoyo del área de tecnologías de la información para la implementación de medidas tecnológicas idóneas para proteger la información;

II. Inventariar el equipo tecnológico que tiene el Instituto de Innovación y Transferencia de Tecnología, tales como computadoras, impresoras, escáneres y copiadoras, para efectos de:
   a. Verificar que durante los mantenimientos y monitoreo que el personal internoo externo brinde al equipo, no se vulnere la seguridad de la información contenida en su disco duro o cualquiera de sus dispositivos de almacenamiento en la forma que adopten, debiendo estar acompañados por un servidor público autorizado para tal efecto;
   b. Eliminar por completo del disco duro del equipo o cualquiera de sus dispositivos de almacenamiento, previamente a su devolución, tras la terminación del contrato respectivo, tratándose de arrendamiento o similar, o encaso de que sean dados de baja, toda la información que obre del sujeto obligado, particularmente, la que corresponde a datos personales, para que solo quede bajo la custodia del I2T2.

III. Implementar los demás procedimientos y medidas de seguridad técnicas necesarias para el tratamiento y conservación de datos personales contenidos en sus archivos, registros, bancos y bases de datos, que deriven de lo dispuesto en la Ley y la demás normatividad aplicable.

La Dirección de Planeación y Gestión del Conocimiento del I2T2, implementará cuando menos las siguientes **medidas de seguridad en equipos computacionales que contengan**

documentos, archivos o sistemas de datos personales:

I. Contar con seguridad de acceso lógico a los equipos como contraseñas en el sistema operativo para el personal autorizado.
II. Establecer restricciones de acceso a Internet, a los sitios que pudieran resultar dañinos o maliciosos, o bien, que pudieran permitir la transmisión de información delos datos personales de forma no autorizada.
III. Limitar o restringir por completo el uso de internet en los equipos que se estime pertinente.
IV. Establecer acceso restringido a la red, únicamente a los archivos o carpetas necesarias para el desempeño de funciones.

Medidas de seguridad para prevenir accesos no autorizados en las instalaciones.

a) Para prevenir el acceso no autorizado de las personas ajenas a esta dependencia, el personal que labora en recepción deberá registrar al ciudadano y previa identificación,darle el acceso correspondiente.

Medidas de seguridad en caso de desastres naturales:

Tormentas eléctricas: En caso de interrupción de la energía eléctrica, cada computadora cuenta con un regulador de corriente para protección del equipo.

Incendios y humos: El Instituto de Innovación y Transferencia de Tecnología cuenta con extintores especiales para controlar los incendios en aparatos electrónicos, ya que el componente que tienen estos extintores (CO_2), es amigable con el material del que están fabricadas las computadoras.

Medidas de seguridad para prevenir accesos no autorizados a equipos de cómputo

Para evitar los accesos no autorizados a dichos equipos e imposibilitar que una persona no autorizada pueda acceder o modificar los datos contenidos en un sistema de cómputo se utilizan contraseñas, los servidores públicos que laboran en esta dependencia, al momento de ser dados de alta como trabajadores, son acreedores a un usuario y contraseña para acceder a los equipos de cómputo previamente designados para el desempeño de sus labores, considerándose una medida de seguridad ya que provee un acceso limitado al ordenador.

Medidas de seguridad con respecto a la infraestructura tecnológica

Con fundamento en el artículo 25 del Manual Integral de Organización del I2T2, es atribución de la Dirección de Planeación y Gestión del Conocimiento las siguientes medidas de seguridad:

- Gestionar de las Tecnologías de la Información y Comunicación del Instituto

- Llevar a cabo el mantenimiento y operación de la Infraestructura del Instituto
- Gestionar de incidentes por reporte de error o falla en la infraestructura del Instituto
- Atender solicitudes de cambio de contenido (alta, baja o modificación (sobre los sitios web y sobre las redes sociales
- Realizar y desarrollar de software y de sitios web para los programas y proyectos del Instituto

Como medida de seguridad contra pérdida o destrucción de documentos electrónicos, a criterio de cada uno de los servidores públicos se podrá realizar una copia o respaldo de los documentos que se encuentren resguardados en sus equipos de cómputo mediante la Disco duros de respaldos del Instituto de Innovación y Transferencia de Tecnología previa solicitud del servicio a la Dirección de Planeación y Gestión del Conocimiento.

Formas de supresión y borrado seguro de información, cuyo contenido se encuentran inmersos datos personales

Físicamente:

1.-Trituración mediante corte cruzado o en partículas, consiste en cortar el documento de forma vertical y horizontal generando fragmentos diminutos, denominados "partículas", lo cual hace prácticamente imposible que se puedan unir.
2.-Destrucción de los medios de almacenamiento electrónicos a través de la desintegración, a fin de que deje de existir la información que se desea eliminar, se separa, completa o parcialmente los elementos que la conforman.

Lógicamente:

1.-Sobre–escritura, esta consiste en sobre escribir todas las ubicaciones de almacenamiento utilizables en un medio de almacenamiento, es decir, se trata reescribir información, nueva en la superficie de almacenamiento, en el mismo lugar que los datos existentes, utilizando herramientas de software.

PLAN DE TRABAJO

La existencia del documento de seguridad busca enmarcar los deberes del I2T2 para la máxima protección de datos personales. Debido a la importancia y el contexto actual en materia de datos personales, se debe mantener actualizado el plan de trabajo, el cual permita alcanzar los objetivos del sistema de seguridad de protección de datos personales.

La finalidad de este plan de trabajo es plasmar de manera enunciativa, más no limitativa, las actividades que el I2T2 realizará para la aplicación del presente documento de seguridad.

Lo anterior se realizará con base en las atribuciones establecidas en la Ley General de Protección de Datos Personales en Posesión de sujetos Obligados y la Ley de Protección de Datos Personales en Posesión de sujetos Obligados del Estado de Nuevo León.

Para la ejecución del presente documento de seguridad, dentro de los 6 meses siguientes a la emisión del presente documento:

1. Se comunicará a los encargados, responsables y directores sobre la emisión del documento de seguridad, solicitando su apoyo para la difusión interna del mismo.

2. El Comité de Transparencia revisará de manera anual, a partir de la emisión del presente documento de seguridad.

3. La actualización de las medidas de Seguridad para la protección de datos personales.

.

4. Se emitirá un programa anual de capacitaciones y además se promoverá que el personal de este Sujeto Obligado se mantenga capacitado, no sólo por sus áreas internas, sino también mediante su asistencia a capacitaciones otorgadas por organismos competentes en la materia.

5. La actualización del plan de trabajo de acuerdo con las medidas y situaciones que se presenten.

EL PROGRAMA GENERAL DE CAPACITACIÓN 2024

Objetivo: Garantizar el cumplimiento de las regulaciones de protección de datos personales y promover practicas éticas y seguras en el manejo de la información.

Alcance: Los servidores públicos del I2T2 que, dentro de sus atribuciones y responsabilidades de su puesto, manejen información de datos personales tomaran al menos 1 curso por semestre dando un total de 2 cursos por año en materia de datos personales.

Legislación Vigente: Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León, Artículos 35 y 36

Las capacitaciones del I2T2 se manejarán de conformidad con las necesidades de las unidades obligadas en cuanto a la implementación y aplicación del sistema de manejo de datos personales, en posesión del sujeto obligado, trabajando de manera coordinada con el INFONL

Al ser cursos que imparte el INFONL de acuerdo con su calendario mensual, las fechas y los cursos se les notificaran a los encargados que sean designados con el menos una semana de anticipación, con la intención de que éstos difundan con los interesados en asistir a las capacitaciones.

Periodo	Servidor Público	Primer Apellido	Segundo Apellido	Cargo	Curso
1- Semestre	Jorge Enrique	Fernández	Salazar	Coordinador de Emprendimiento	Datos personales
1- Semestre	Jorge Eduardo	Rangel	Medrano	Jefe de la Unidad de Transparencia	Datos personales
1- Semestre	Endy-Judith	Méndez	Hernández	Analista de Cooperación Internacional y Proyectos Estratégicos	Datos personales
1- Semestre	Maura Isabel	Mendoza	Miranda	Directora de Administración y Finanzas	Datos personales
1- Semestre	Roberto	Sequera	Vargas	Coordinador Administrativa y Financiero	Datos personales
1- Semestre	Vanessa Zula-amath	Chávez	Rodríguez	Coordinador de Formación de Vocaciones y Capital Humano	Datos personales
1- Semestre	Adrián	Godines	González	Coordinador de Recursos Materiales, Servicios Generales y Archivo	Datos personales
1- Semestre	Saúl Román	Ruíz	Díaz	Coordinador de Incubadoras	Datos personales
1- Semestre	Oscar	Vázquez	Montiel	Director de Innovación, Emprendimiento e Infraestructura Tecnológica	Datos personales
1- Semestre	Emma Alejandra	Carlo	Guerrero	Directora de Planeación y Gestión del Conocimiento	Datos personales
1- Semestre	Manolo	Medina	De La Sota	Jefe de Archivos	Datos personales
1- Semestre	Ricardo Emmanuel	Alanís	Berlanga	Jefe de Logística	Datos personales
1- Semestre	Karla Cistina	Alanis	Estrada	Analista Técnico Nanoincubadora	Datos personales
1-Semestre	Victoria	De La Rosa	Valdez	Coordinador de Comunicación Pública de la CTI	Datos Personales
1-Semestre	Jesús Enrique	Cantú	Bustos	Analista Técnico Bioincubadora	Datos Personales
1-Semestre	María De Jesús	Rodríguez	Herrera	Coordinador de Planeación y Vinculación	Datos Personales

Periodo	Servidor Público	Primer Apellido	Segundo Apellido	Cargo	Curso
2- Semestre	Jorge Enrique	Fernández	Salazar	Coordinador de Emprendimiento	Datos personales
2- Semestre	Jorge Eduardo	Rangel	Medrano	Jefe de la Unidad de Transparencia	Datos personales
2- Semestre	Endy-Judith	Méndez	Hernández	Analista de Cooperación Internacional y Proyectos Estratégicos	Datos personales
2- Semestre	Maura Isabel	Mendoza	Miranda	Directora de Administración y Finanzas	Datos personales
2- Semestre	Roberto	Sequera	Vargas	Coordinador Administrativa y Financiero	Datos personales
2- Semestre	Vanessa Zula-amath	Chávez	Rodríguez	Coordinador de Formación de Vocaciones y Capital Humano	Datos personales
2- Semestre	Adrián	Godines	González	Coordinador de Recursos Materiales, Servicios Generales y Archivo	Datos personales
2- Semestre	Saúl Román	Ruíz	Díaz	Coordinador de Incubadoras	Datos personales
2- Semestre	Oscar	Vázquez	Montiel	Director de Innovación, Emprendimiento e Infraestructura Tecnológica	Datos personales
2- Semestre	Emma Alejandra	Carlo	Guerrero	Directora de Planeación y Gestión del Conocimiento	Datos personales
2- Semestre	Manolo	Medina	De La Sota	Jefe de Archivos	Datos personales
2- Semestre	Ricardo Emmanuel	Alanís	Berlanga	Jefe de Logística	Datos personales
2- Semestre	Karla Cristina	Alanis	Estrada	Analista Técnico Nanoincubadora	Datos personales
2- Semestre	Victoria	De La Rosa	Valdez	Coordinador de Comunicación Pública de la CTI	Datos Personales
2- Semestre	Jesús Enrique	Cantú	Bustos	Analista Técnico Bioincubadora	Datos Personales
2- Semestre	María De Jesús	Rodríguez	Herrera	Coordinador de Planeación y Vinculación	Datos Personales

ACTUALIZACIONES AL DOCUMENTO DE SEGURIDAD

El presente documento de seguridad se actualizará cuando sucedan los siguientes acontecimientos:

I. Se produzcan modificaciones fundamentales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;
II. Se modifiquen las medidas de seguridad, derivado de las recomendaciones del Comité de Transparencia**;**
III. Como resultado de un proceso de mejora continua para mitigar el impacto de una vulneración,
IV. Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.
V. Cuando surjan documentos, formatos, recomendaciones, por parte del INFO NL o del INAI para la mejora del presente documento de seguridad.
VI. Cuando este sujeto obligado sufra modificaciones en cuanto a su estructura orgánica y atribuciones de las áreas que lo componen.

ANEXO I

INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES DEL I2T2

- Dirección General: No cuenta con inventario (No maneja datos personales)
- Dirección de Administración y Finanzas : Si cuenta con inventario
    1. Integración de Expedientes de Personal
    2. Contrataciones de Servicios
    3. Adquisición de Bienes
- Dirección de Innovación Emprendimiento e infraestructura Tecnología: Si cuenta con inventario
    1. Ingreso de Emprendedores a las Incubadoras.
    2. Prestaciones de Servicios a las Incubadoras
- Dirección de Planeación y Gestión del Conocimiento: Si cuenta con inventario
    1. Ferias de Ciencias Nuevo León.
    2. Estancias Doctorales

3. Becas Conacyt- Regional Noreste
4. Verano de Investigación en el PIIT
5. Premio Estatal de Ciencia, Tecnología e Innovación

1.- Dirección Administrativa y Financiera

1.1.- Integración de Expedientes de Personal

1.1.1.- Servidor público responsable del sistema o base de tratamiento

Nombre	Puesto	Correo electrónico	Teléfono Institucional
Roberto Sequera Vargas	Coordinador Administrativa y Financiero	roberto.sequera @i2t2.gob.mx	8120331117

1.1.2.-Objeto de la base de datos o sistema de tratamiento:

Son requisitos necesarios que debe tener un expediente de personal y que son indispensables para su incorporación al sistema de nóminas.

1.1.3.-Datos personales que se recaban y su finalidad.

DATO PERSONAL	FINALIDAD
Nombre	Son requisitos necesarios que debe tener un expediente de personal y que son indispensables para su incorporación al sistema de Nóminas y al ISSTELEÓN o IMSS.
Domicilio	
RFC	
CURP	
Número telefónico	

Los datos que se recaban no son considerados como sensibles.

1.1.4.-Fundamento legal que lo faculta para el tratamiento.

Artículo 26 fracción XII del Reglamento Interior del Instituto de Innovación y Transferencia de Tecnología de Nuevo León, así como la Ley Federal de Protección de Datos Personales en Posesión de Particulares, la Ley Federal de Trabajo.

1.1.5.- Forma de obtención, directa o indirectamente del titular, y medios de almacenamiento físico o electrónico.

FORMA DE OBTENCIÓN	MEDIOS DE ALMACENAMIENTO
Directamente: Por el servidor público responsable del sistema.	**FÍSICO:** Los expedientes de personal almacenados en un archivero. **ELECTRÓNICO:** Mediante discos duros (tanto propios del equipo de cómputo como los portátiles), memorias extraíbles como USB.

1.1.6.-Sitios de resguardo

Se resguardan los datos personales en la Coordinación Administrativa y Financiera, tanto físicamente como en sus respaldos y almacenamientos digitales.

1.1.7.- Servidores públicos que tienen acceso a los sistemas de datos personales.

El Coordinador Administrativo y Financiero.

1.1.8.- Terceros encargados de datos personales.

Proveedor/Tercero	N/A
Actividad	N/A
Relación	N/A
Instrumento jurídico que formalizala prestación del servicio	N/A

1.1.9.- Ciclo de Vida y riesgo inherente de los datos personales.

Su ciclo de vida es conforme a la baja documental que la Unidad Administrativa podrá realizar de acuerdo con las disposiciones que regulan la gestión documental al interior del I2T2.

1.2.- Contratación de Servicios

1.2.1.- Servidor público responsable del sistema o base de tratamiento

Nombre	Puesto	Correo electrónico	Teléfono Institucional
Adrián Godínez González	Coordinador de Recursos Materiales, Servicios Generales y Archivo	adrian.godines@i2t2.gob.mx	81120331109

1.2.2.-Objeto de la base de datos o sistema de tratamiento:

Brindar una certeza jurídica, financiera y de buena práctica gubernamental en la administración de los recursos financieros otorgados al I2T2.

1.2.3.-Datos personales que se recaban y su finalidad.

DATO PERSONAL	FINALIDAD
Nombre	**Principal**: Requisito indispensable para el brindar el trámite correspondiente
RFC Registro Federal de contribuyentes (RFC)	
CURP	
Correo electrónico	
Teléfono celular	
Domicilio	
Firma autógrafa	
Núm. Cedula profesional	
Cuentas bancarias	

Los datos que se recaban no son considerados como sensibles.

1.2.4.-Fundamento legal que lo faculta para el tratamiento.

Ley de Adquisiciones, Arrendamientos y Contratación de Servicios del Estado de Nuevo León y Reglamento de la Ley de Adquisiciones, Arrendamientos y Contratación de Servicios del Estado de Nuevo León

1.1.5.- Forma de obtención, directa o indirectamente del titular, y medios de almacenamiento físico o electrónico.

FORMA DE OBTENCIÓN	MEDIOS DE ALMACENAMIENTO
Directamente: Por el servidor público responsable del sistema.	**FÍSICO:** Los expedientes se encuentran almacenados en un archivero. **ELECTRÓNICO:** Mediante discos duros (tantopropios del equipo de cómputo como los portátiles), memorias extraíbles como USB.

1.1.6.-Sitios de resguardo

En la Coordinación de Recursos Materiales, Servicios Generales y Archivo

1.1.7.- Servidores públicos que tienen acceso a los sistemas de datos personales. Coordinador de Recursos Materiales, Servicios Generales y Archivo.

1.1.8.- Terceros encargados de datos personales.

Proveedor/Tercero	N/A
Actividad	N/A
Relación	N/A
Instrumento jurídico que formaliza la prestación del servicio	N/A

1.1.9.- Ciclo de Vida y riesgo inherente de los datos personales.
Su ciclo de vida es conforme a la baja documental que la Unidad Administrativa podrá realizar de acuerdo con las disposiciones que regulan la gestión documental al interior del I2T2.

1.3- Adquisición de Bienes

1.3.1.- Servidor público responsable del sistema o base de tratamiento

Nombre	Puesto	Correo electrónico	Teléfono Institucional
Adrián Godines González	Coordinador de Recursos Materiales, Servicios Generales y Archivo	adrian.godines@i2t2.gob.mx	81120331109

1.3.2.-Objeto de la base de datos o sistema de tratamiento:
Brindar una certeza jurídica, financiera y de buena práctica gubernamental en la administración de los recursos financieros otorgados al I2T2.

1.3.3.-Datos personales que se recaban y su finalidad.

DATO PERSONAL	FINALIDAD
Nombre	**Principal**: Requisito indispensable para el brindarel trámite correspondiente
RFC Registro Federal de contribuyentes (RFC)	
CURP	
Correo electrónico	
Teléfono celular	
Domicilio	
Firma autógrafa	
Núm. Cedula profesional	
Cuentas bancarias	

Los datos que se recaban no son considerados como sensibles.

1.3.4.-Fundamento legal que lo faculta para el tratamiento.
Ley de Adquisiciones, Arrendamientos y Contratación de Servicios del Estado de Nuevo León y Reglamento de la Ley de Adquisiciones, Arrendamientos y Contratación de Servicios del Estado de Nuevo León

1.3.5.- Forma de obtención, directa o indirectamente del titular, y medios de almacenamiento físico o electrónico.

FORMA DE OBTENCIÓN	MEDIOS DE ALMACENAMIENTO
Directamente: Por el servidor público responsable del sistema.	**FÍSICO:** Los expedientes se encuentran almacenados en un archivero. **ELECTRÓNICO:** Mediante discos duros (tanto propios del equipo de cómputo como los portátiles), memorias extraíbles como USB.

1.3.6.-Sitios de resguardo
En la Coordinación de Recursos Materiales, Servicios Generales y Archivo

1.3.7.- Servidores públicos que tienen acceso a los sistemas de datos personales. Coordinador de Recursos Materiales, Servicios Generales y Archivo

1.3.8.- Terceros encargados de datos personales.

Proveedor/Tercero	N/A
Actividad	N/A
Relación	N/A
Instrumento jurídico que formaliza la prestación del servicio	N/A

1.3.9.- Ciclo de Vida y riesgo inherente de los datos personales.
Su ciclo de vida es conforme a la baja documental que la Unidad Administrativa podrá realizar de acuerdo a las disposiciones que regulan la gestión documental al interior de la Institución.

2.- Dirección de Innovación, Emprendimiento e Infraestructura tecnológica

2.1- Ingreso de Emprendedores a las Incubadoras

2.1.1.- Servidor público responsable del sistema o base de tratamiento

Nombre	Puesto	Correo electrónico	Teléfono Institucional
Jorge Enrique Fernández Salazar	Coordinador de Emprendimiento	jorge.fernandez@i2t2.gob.mx	8130602117

2.1.2.-Objeto de la base de datos o sistema de tratamiento:

Para establecer un convenio de colaboración entre el incubando y el I2T2 con la finalidad de ofrecer el servicio; y para envió de cotización y facturación

2.1.3.-Datos personales que se recaban y su finalidad.

DATO PERSONAL	FINALIDAD
Nombre	**Principal**: Requisito indispensable para el brindarel trámite correspondiente
RFC Registro Federal de contribuyentes (RFC)	
CURP	
Correo electrónico	
Teléfono celular	
Domicilio	
Firma	
Huella	
Foto	
Edad	

El dato que se recaba como huella si es considerado como sensible.

2.1.4.-Fundamento legal que lo faculta para el tratamiento.

Reglamento Interior del I2T2. Artículo 24 Fracción I, II, III, IV, V, VI, XV

2.1.5.- Forma de obtención, directa o indirectamente del titular, y medios de almacenamiento físico o electrónico.

FORMA DE OBTENCIÓN	MEDIOS DE ALMACENAMIENTO
Directamente: Por el servidor público responsable del sistema.	**FÍSICO:** Los expedientes se encuentran almacenados en un archivero. **ELECTRÓNICO:** Mediante discos duros (tantopropios del equipo de cómputo como los portátiles), memorias extraíbles como USB.

2.1.6.-Sitios de resguardo
En la Coordinación de Emprendimiento

2.1.7.- Servidores públicos que tienen acceso a los sistemas de datos personales. Coordinador de Emprendimiento

2.1.8.- Terceros encargados de datos personales.

Proveedor/Tercero	N/A
Actividad	N/A
Relación	N/A
Instrumento jurídico que formaliza la prestación del servicio	N/A

2.1.9.- Ciclo de Vida y riesgo inherente de los datos personales.
Su ciclo de vida es conforme a la baja documental que la Unidad Administrativa podrá realizar de acuerdo con las disposiciones que regulan la gestión documental al interior de la Institución.

2.2.- Prestaciones de Servicio a las Incubadoras

2.2.1.- Servidor público responsable del sistema o base de tratamiento

Nombre	Puesto	Correo electrónico	Teléfono Institucional
Jorge Enrique Fernández Salazar	Coordinador de Emprendimiento	jorge.fernandez@i2t2.gob.mx	8130602117

2.2.2.-Objeto de la base de datos o sistema de tratamiento:
Para envió de cotización y facturación

2.2.3.-Datos personales que se recaban y su finalidad.

DATO PERSONAL	FINALIDAD
Nombre	**Principal**: Requisito indispensable para el brindarel trámite correspondiente
Correo electrónico	
Teléfono celular	
Domicilio	

Los datos que se recaban no son considerados como sensibles.

2.2.4.-Fundamento legal que lo faculta para el tratamiento.
Reglamento Interior del I2T2. Artículo 24 Fracción I, II, III, IV, V, VI, XV

2.2.5.- Forma de obtención, directa o indirectamente del titular, y medios de almacenamiento físico o electrónico.

FORMA DE OBTENCIÓN	MEDIOS DE ALMACENAMIENTO
Directamente: Por el servidor público responsable del sistema.	**FÍSICO:** Los expedientes se encuentran almacenados en un archivero. **ELECTRÓNICO:** Mediante discos duros (tantopropios del equipo de cómputo como los portátiles), memorias extraíbles como USB.

2.2.6.-Sitios de resguardo
En la Coordinación de Emprendimiento

2.2.7.- Servidores públicos que tienen acceso a los sistemas de datos personales. Coordinador de Emprendimiento

2.2.8.- Terceros encargados de datos personales.

Proveedor/Tercero	N/A
Actividad	N/A
Relación	N/A
Instrumento jurídico que formaliza la prestación del servicio	N/A

2.2.9.- Ciclo de Vida y riesgo inherente de los datos personales.
Su ciclo de vida es conforme a la baja documental que la Unidad Administrativa podrá realizar de acuerdo a las disposiciones que regulan la gestión documental aal interior del I2T2.

3.- Dirección de Planeación y Gestión del Conocimiento

3.1- Ferias de Ciencias Nuevo León.

3.1.1.- Servidor público responsable del sistema o base de tratamiento

Nombre	Puesto	Correo electrónico	Teléfono Institucional
Vanessa Zula-amath Chávez Rodríguez	Coordinador de Formación de Vocaciones y Capital Humano	vanessa.chavez@i2t2.gob.mx	81201110

3.1.2.-Objeto de la base de datos o sistema de tratamiento:

Las finalidades de recabar sus datos personales son elaborar constancias y verificar el cumplimiento de los requisitos de la convocatoria Expo Ciencias y FEMECI Nuevo León.

3.1.3.-Datos personales que se recaban y su finalidad.

DATO PERSONAL	FINALIDAD
Nombre	**Principal**: Requisito indispensable para el brindarel trámite correspondiente
Nombre de la Institución Educativa	
Fecha de nacimiento	
Domicilio	
Correo Electrónico	

Los datos que se recaban no son considerados como sensibles.

3.1.4.-Fundamento legal que lo faculta para el tratamiento.

Ley de Ciencia, Tecnología e Innovación del Estado de Nuevo León, artículo 26, fracciones IV, XIV, XX y XXI. El Artículo 6 del Reglamento Interior del Instituto de Innovación y Transferencia de Tecnología de Nuevo León y el Manual Integral de Organización del I2T2, numeral 7, apartado 9

3.1.5.- Forma de obtención, directa o indirectamente del titular, y medios de almacenamiento físico o electrónico.

FORMA DE OBTENCIÓN	MEDIOS DE ALMACENAMIENTO
Directamente: Por el servidor público responsable del sistema.	**FÍSICO:** Los expedientes se encuentran almacenados en un archivero. **ELECTRÓNICO:** Mediante discos duros (tantopropios del equipo de cómputo como los portátiles), memorias extraíbles como USB.

3.1.6.-Sitios de resguardo
En la Coordinación de Formación de Vocaciones y Capital Humano

3.1.7.- Servidores públicos que tienen acceso a los sistemas de datos personales. Coordinador de Formación de Vocaciones y Capital Humano

3.1.8.- Terceros encargados de datos personales.

Proveedor/Tercero	N/A
Actividad	N/A
Relación	N/A
Instrumento jurídico que formaliza la prestación del servicio	N/A

3.1.9.- Ciclo de Vida y riesgo inherente de los datos personales.
Su ciclo de vida es conforme a la baja documental que la Unidad Administrativa podrá realizar de acuerdo con las disposiciones que regulan la gestión documental al interior del I2T2.

3.2- Estancias Doctorales

3.2.1.- Servidor público responsable del sistema o base de tratamiento

Nombre	Puesto	Correo electrónico	Teléfono Institucional
Vanessa Zula-amath Chávez Rodríguez	Coordinador de Formación de Vocaciones y Capital Humano	vanessa.chavez@i2t2.gob.mx	8120331110

3.2.2.-Objeto de la base de datos o sistema de tratamiento:
Aquellos datos personales, a los cuales tiene acceso la Coordinación de Formación de Capital Humano del I2T2, tienen como única finalidad; la elaboración del padrón de beneficiarios, acreedores al apoyo para realizar su estadía doctoral, a través del Programa de Becas al Extranjero CONACYTI2T2 (DOCTORADO).

3.2.3.-Datos personales que se recaban y su finalidad.

DATO PERSONAL	FINALIDAD
Nombre	**Principal**: Requisito indispensable para el brindarel trámite correspondiente
RFC	
CURP	
Domicilio	

Los datos que se recaban no son considerados como sensibles.

3.2.4.-Fundamento legal que lo faculta para el tratamiento.

Ley de Ciencia, Tecnología e Innovación del Estado de Nuevo León, artículo 26, fracciones IV, XIV, XX y XXI. El Artículo 6 del Reglamento Interior del Instituto de Innovación y Transferencia de Tecnología de Nuevo León y el Manual Integral de Organización del I2T2, numeral 7, apartado 9

3.2.5.- Forma de obtención, directa o indirectamente del titular, y medios de almacenamiento físico o electrónico.

FORMA DE OBTENCIÓN	MEDIOS DE ALMACENAMIENTO
Directamente: Por el servidor público responsable del sistema.	**FÍSICO:** Los expedientes se encuentran almacenados en un archivero. **ELECTRÓNICO:** Mediante discos duros (tantopropios del equipo de cómputo como los portátiles), memorias extraíbles como USB.

3.2.6.-Sitios de resguardo

En la Coordinación de Formación de Vocaciones y Capital Humano.

3.2.7.- Servidores públicos que tienen acceso a los sistemas de datos personales.

Coordinador de Formación de Vocaciones y Capital Humano.

3.2.8.- Terceros encargados de datos personales.

Proveedor/Tercero	N/A
Actividad	N/A
Relación	N/A
Instrumento jurídico que formaliza la prestación del servicio	N/A

3.2.9.- Ciclo de Vida y riesgo inherente de los datos personales.

Su ciclo de vida es conforme a la baja documental que la Unidad Administrativa podrá realizar de acuerdo a las disposiciones que regulan la gestión documental al interior de I2T2.

3.3- Becas Conacyt- Regional Noreste

3.3.1.- Servidor público responsable del sistema o base de tratamiento

Nombre	Puesto	Correo electrónico	Teléfono Institucional
Vanessa Zula-amath Chávez Rodríguez	Coordinador de Formación de Vocaciones y Capital Humano	vanessa.chavez@i2t2.gob.mx	8120331110

3.3.2.-Objeto de la base de datos o sistema de tratamiento:
Con la finalidad de revisar los expedientes de los aspirantes, que ingresan su solicitud a la CONVOCATORIA “BECAS CONACYT-REGIONAL NORESTE”,

3.3.3.-Datos personales que se recaban y su finalidad.

DATO PERSONAL	FINALIDAD
Nombre	**Principal**: Requisito indispensable para el brindarel trámite correspondiente
RFC	
CURP	
Domicilio	
Firma autógrafa	
Sexo	
Lugar de nacimiento	
Estado civil	
Nacionalidad	
Edad	

Los datos que se recaban no son considerados como sensibles.

3.3.4.-Fundamento legal que lo faculta para el tratamiento.
Ley de Ciencia, Tecnología e Innovación del Estado de Nuevo León, artículo 26, fracciones IV, XIV, XX y XXI. El Artículo 6 del Reglamento Interior del Instituto de Innovación y Transferencia de Tecnología de Nuevo León y el Manual Integral de Organización del I2T2, numeral 7, apartado 9

3.3.5.- Forma de obtención, directa o indirectamente del titular, y medios de almacenamiento físico o electrónico.

FORMA DE OBTENCIÓN	MEDIOS DE ALMACENAMIENTO
Directamente: Por el Servidor público responsable del sistema.	**FÍSICO:** Los expedientes se encuentran almacenados en un archivero. **ELECTRÓNICO:** Mediante discos duros (tantopropios del equipo de cómputo como los portátiles), memorias extraíbles como USB.

3.3.6.-Sitios de resguardo
En la Coordinación de Formación de Vocaciones y Capital Humano.

3.3.7.- Servidores públicos que tienen acceso a los sistemas de datos personales. Coordinador de Formación de Vocaciones y Capital Humano.

3.3.8.- Terceros encargados de datos personales.

Proveedor/Tercero	N/A
Actividad	N/A
Relación	N/A
Instrumento jurídico que formaliza la prestación del servicio	N/A

3.3.9.- Ciclo de Vida y riesgo inherente de los datos personales.

Su ciclo de vida es conforme a la baja documental que la Unidad Administrativa podrá realizar de acuerdo con las disposiciones que regulan la gestión documental al interior del I2T2.

3.4- Verano de Investigación en el PIIT

3.4.1.- Servidor público responsable del sistema o base de tratamiento

Nombre	Puesto	Correo electrónico	Teléfono Institucional
Vanessa Zula-amath Chávez Rodríguez	Coordinador de Formación de Vocaciones y Capital Humano	vanessa.chavez@i2t2.gob.mx	8120331110

3.4.2.-Objeto de la base de datos o sistema de tratamiento:

Revisar y validar la información del solicitante en relación con los requisitos de la convocatoria

3.4.3.-Datos personales que se recaban y su finalidad.

DATO PERSONAL	FINALIDAD
Nombre	**Principal**: Requisito indispensable para el brindarel trámite correspondiente
Edad	
Constancia de Estudios	
Correo electrónico	
Número de celular	
INE	

Los datos que se recaban no son considerados como sensibles.

3.4.4.-Fundamento legal que lo faculta para el tratamiento.

Ley de Ciencia, Tecnología e Innovación del Estado de Nuevo León, artículo 26, fracciones IV, XIV, XX y XXI. El Artículo 6 del Reglamento Interior del Instituto de Innovación y Transferencia de Tecnología de Nuevo León y el Manual Integral de Organización del I2T2, numeral 7, apartado 9

3.4.5.- Forma de obtención, directa o indirectamente del titular, y medios de almacenamiento físico o electrónico.

FORMA DE OBTENCIÓN	MEDIOS DE ALMACENAMIENTO
Directamente: Por el Servidor público responsable del sistema, o **Indirectamente** por el titular	**FÍSICO:** Los expedientes se encuentran almacenados en un archivero. **ELECTRÓNICO:** Mediante discos duros (tantopropios del equipo de cómputo como los portátiles), memorias extraíbles como USB.

3.4.6.-Sitios de resguardo
En la Coordinación de Formación de Vocaciones y Capital Humano.

3.4.7.- Servidores públicos que tienen acceso a los sistemas de datos personales. Coordinador de Formación de Vocaciones y Capital Humano.

3.4.8.- Terceros encargados de datos personales.

Proveedor/Tercero	N/A
Actividad	N/A
Relación	N/A
Instrumento jurídico que formaliza la prestación del servicio	N/A

3.4.9.- Ciclo de Vida y riesgo inherente de los datos personales.
Su ciclo de vida es conforme a la baja documental que la Unidad Administrativa podrá realizar de acuerdo a las disposiciones que regulan la gestión documental al interior del I2T2.

3.5- Premio Estatal de Ciencia, Tecnología e Innovación

3.5.1.- Servidor público responsable del sistema o base de tratamiento

Nombre	Puesto	Correo electrónico	Teléfono Institucional
María de Jesús Rodríguez Herrera	Coordinación de Planeación y Vinculación	mariadejesus.rodriguez@i2t2.gob.mx	8120331122

3.5.2.-Objeto de la base de datos o sistema de tratamiento:
Contar con información de los participantes de la Convocatoria del Premio Estatal de Ciencia Tecnología e Innovación

3.5.3.-Datos personales que se recaban y su finalidad.

DATO PERSONAL	FINALIDAD
Nombre	**Principal**: Requisito indispensable para el brindarel trámite correspondiente
Fotografía	
CURP	
Domicilio	
Firma	
Fecha de nacimiento	

Los datos que se recaban no son considerados como sensibles.

3.5.4.-Fundamento legal que lo faculta para el tratamiento.
Artículo 39, fracción VI de la Ley de Ciencia, Tecnología e Innovación del Estado de Nuevo León

3.5.5.- Forma de obtención, directa o indirectamente del titular, y medios de almacenamiento físico o electrónico.

FORMA DE OBTENCIÓN	MEDIOS DE ALMACENAMIENTO
Directamente: Por el Servidor público responsable del sistema.	**ELECTRÓNICO:** Mediante discos duros (tantopropios del equipo de cómputo como los portátiles), memorias extraíbles como USB.

3.5.6.-Sitios de resguardo
En Plataforma para el Sistema Estatal de Información Científica y Tecnológica (SEICYT)

3.5.7.- Servidores públicos que tienen acceso a los sistemas de datos personales.

Jefe de Sistemas y Tecnologías de la Información y Comunicación, Analista Operativo de TIC´s

3.5.8.- Terceros encargados de datos personales.

Proveedor/Tercero	N/A
Actividad	N/A

Relación	N/A
Instrumento jurídico que formaliza la prestación del servicio	N/A

3.5.9.- Ciclo de Vida y riesgo inherente de los datos personales.

Su ciclo de vida es conforme a la baja documental que la Unidad Administrativa podrá realizar de acuerdo con las disposiciones que regulan la gestión documental al interior del I2T2.

Documento de Seguridad para la Protección de los Datos Personales

Firma de los servidores públicos que elaboraron y validaron la información contenida en el Documento de Seguridad para la Protección de los Datos Personales 2024

ELABORÓ

Lic. Jorge Eduardo Rangel Medrano
Jefe de Unidad de Transparencia

VALIDAN

C.P. Roberto Sequera Vargas
Coordinador Administrativo y Financiero y Servidor público responsable del sistema o base de tratamiento

C.P. Adrián Godines González
Coordinador de Recursos Materiales, Servicios Generales y Archivo y Servidor público responsable del sistema o base de tratamiento

Lic. Vanessa Zula-amath Chávez Rodríguez
Coordinador de Formación de Vocaciones y Capital Humano y Servidor público responsable del sistema o base de tratamiento.

Lic. Jorge Enrique Fernández Salazar
Coordinador de Emprendimiento y Servidor público responsable del sistema o base de tratamiento.

Ing. María de Jesús Rodríguez Herrera
Coordinación de Planeación y Vinculación
Servidor público responsable del sistema o base de tratamiento