UNIVERSIDAD TECNOLÓGICA
UT CADEREYTA
NUEVO LEÓN

2024

DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE LOS DATOS PERSONALES

CONTENIDO

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 de la UNIVERSIDAD TECNOLÓGICA CADEREYTA, como sujeto obligado. Teniendo como base dicha normatividad, y en cumplimiento de 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, la UNIVERSIDAD TECNOLÓGICA CADEREYTA, en conjunto con los encargados que tiene en cada área generadora de información, ha realizado acciones y actividades que tuvieron como finalidad establecer los principios para la creación de este documento.

Para recabar información precisa, se realizó un cuestionario a través de los Titulares de las Unidades Administrativas de la UNIVERSIDAD TECNOLÓGICA CADEREYTA, con la finalidad de detectar medidas de seguridad con las que ya contaba cada Dirección y definir posibles riesgos.

Una vez contestado el cuestionario, se analizó la información recabada, lo que permitió la creación de las medidas de seguridad. A partir del inventario inicial de las bases de datos personales y diversas acciones, se generaron cada una de las partes que integran el presente documento de seguridad, siguiendo como objetivo el propiciar la protección de los datos personales de la forma más completa, ello encaminado a lograr el adecuado tratamiento delos 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.

Bios: El Sistema Básico de Entrada/Salida o BIOS por sus siglas en inglés (Basic Input- Output System), que es un software básico instalado en la placa base, que localiza y carga el sistema operativo en la memoria conocida como RAM por sus siglas en inglés (Random Access Memory), que es la que usa el procesador para recibir instrucciones y guardar resultados.

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.

UTC: UNIVERSIDAD TECNOLÓGICA CADEREYTA.

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

CTUTC: Comité de Transparencia de la Universidad Tecnológica Cadereyta.

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 alo 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 la UNIVERSIDAD TECNOLÓGICA CADEREYTA, 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 del Reglamento de la Ley que crea la UNIVERSIDAD TECNOLÓGICA CADEREYTA, 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 de la UNIVERSIDAD TECNOLÓGICA CADEREYTA 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 el CTUTC, solicitó de manera oportuna a las unidades administrativas de esta UNIVERSIDAD TECNOLÓGICA CADEREYTA que informaran sobre los sistemas de tratamiento con los que cuenta cada área, por lo tanto, el presente documento está integrado por 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 datospersonales 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 la normatividad aplicable les confiera. **Finalidad principal**: Dan origen y son necesarias para la Inscripción, Continuidad, Becas, Bolsa de Trabajo, Estadías, Seguimiento de Egresados. **Finalidad secundaria:** No son necesarias.
FUNDAMENTO LEGAL QUE FACULTAPARA EL TRATAMIENTO	El tratamiento de datos personales por parte del responsabledeberá sujetarse a las facultades o atribuciones que la normatividad aplicable les confiera.

FORMA DE OBTENCIÓN DIRECTA/INDIRECTAMENTE DEL TITULAR MEDIOS FÍSICOS/ELECTRÓNICOS	Directamente del titular: • De manera personal, con la presencia física del titular delos datos personales o su representante, en su caso. • Vía telefónica • Por correo electrónico • Por WhatsApp o Inbox

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 dispositivo electrónico 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 (tantopropios 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 de almacenamiento, tanto físicos como electrónicos pertenecientes a la UNIVERSIDAD TECNOLÓGICA CADEREYTA.
SERVIDORES PÚBLICOS QUE TIENE ACCESO A LOS SISTEMAS DE DATOS PERSONALES	Personal adscrito a la UNIVERSIDAD TECNOLÓGICA CADEREYTA autorizado para llevar acabo el tratamiento de datos personales

ENCARGADO	Servidor público designado para que solo o conjuntamentecon 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 a 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 yexperiencia/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 a las atribuciones de cada unidad administrativa:

- Personas que laboran en la UNIVERSIDAD TECNOLÓGICA CADEREYTA
- Personas externas que prestan algún servicio para la UNIVERSIDAD TECNOLÓGICA CADEREYTA.
- Personas externas que participan en actividades que llevan a cabo las áreas o direcciones de la UNIVERSIDAD TECNOLÓGICA CADEREYTA (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.

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 de la UNIVERSIDAD TECNOLÓGICA CADEREYTA que participan en el tratamiento de los datos personales derivado de sus atribuciones. **Al momento de recibir los datos personales, el servidor público que se encargue de su recepción deberá:**

a. Tener a la vista el Aviso de Privacidad.

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

c. 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 el COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD TECNOLÓGICA CADEREYTA, (CTUTC).

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

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

f. 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.

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

h. 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.

i. Conocer, aplicar y sujetarse al Aviso de Privacidad y al Documento de Seguridad de la UNIVERSIDAD TECNOLÓGICA CADEREYTA, en el tratamiento de datos personales.

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

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

l. 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:

a. Conocer, aplicar y sujetarse al Aviso de Privacidad y al Documento de Seguridad de la

UNIVERSIDAD TECNOLÓGICA CADEREYTA, en el tratamiento de datos personales.

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

c. 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.

d. 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 el COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD TECNOLÓGICA CADEREYTA, (CTUTC).

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

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

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

h. 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 deberá:

a. Conocer, aplicar y sujetarse al Aviso de Privacidad y al Documento de Seguridad de la UNIVERSIDAD TECNOLÓGICA CADEREYTA, en el tratamiento de datos personales.

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

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

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

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

f. 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.

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

h. Tomar por lo menos, una vez al año, un curso, taller o capacitación sobre el tratamiento de

datos personales.

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

j. 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 el Comité de Transparencia de la Universidad Tecnológica Cadereyta, (**CTUTC)**

k. Informar a el Comité de Transparencia de la Universidad Tecnológica Cadereyta, (**CTUTC)** 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.

l. Acudir a el Comité de Transparencia de la Universidad Tecnológica Cadereyta**, (CTUTC)** en caso de requerir asesoría sobre el tratamiento de datos personales.

m. 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.

n. Dar aviso al Comité de Transparencia, a través del Comité de Transparencia de la Universidad Tecnológica Cadereyta**, (CTUTC)**, sobre las actas circunstanciadas de hechos levantadas por el incumplimiento del documento de seguridad y sobre el seguimiento de las mismas.

o. 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 responsable de cada sistema, o en su caso, el titular de la Unidad Administrativa responsable de cada sistema deberá:

a. Conocer, aplicar y sujetarse al Aviso de Privacidad y al Documento de Seguridad del Comité de Transparencia de la Universidad Tecnológica Cadereyta**, (CTUTC)**, en el tratamiento de datos personales.

b. Implementar las medidas de seguridad que establece el documento de seguridad.

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

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

e. 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 el Comité de Transparencia de la Universidad Tecnológica Cadereyta**, (CTUTC).**

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

g. Informar a el Comité de Transparencia de la Universidad Tecnológica Cadereyta**, (CTUTC)**

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.

h. Monitorear la implementación de las medidas de seguridad.

i. 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.

j. Dar aviso al Comité de Transparencia, a el Comité de Transparencia de la Universidad Tecnológica Cadereyta, **(CTUTC)**, sobre las actas circunstanciadas de hechos levantadas por el incumplimiento del documento de seguridad y sobre el seguimiento de las mismas.

k. Presentar propuestas de mejora o modificación del documento de seguridad a través de Comité de Transparencia de la Universidad Tecnológica Cadereyta, **(CTUTC)**

l. Emitir reportes en relación al tratamiento de los datos personales y la aplicación de medidas de seguridad, según sea requerido por el Comité de Transparencia a través de Comité de Transparencia de la Universidad Tecnológica Cadereyta, **(CTUTC)**.

m. 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.

n. 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:

a. Difundir al interior los avisos de privacidad y el documento de seguridad.
b. 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.
c. Proponer al Comité de Transparencia actualizaciones o modificaciones al documento de seguridad.
d. 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 de la Contraloría.

Son obligaciones del Comité de Transparencia en relación al 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:

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

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

c. Requerir anualmente a las áreas responsables que tratan datos personales, a través de Comité de Transparencia de la Universidad Tecnológica Cadereyta, **(CTUTC)** 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 adatos personales	Adquirir información odatos personales.	Divulgación de datos personales. Robo de información. Modificaciones no autorizadas.
Alteración o pérdida de datos personales no intencionada	Tratamiento inadecuado de lainformación.	Falta de disponibilidad íntegra dedatos personales
Daño físico	Agua, fuego, accidentes ocorrosión.	Daño o pérdida de los datos personales.
Eventos naturales	Fenómenos meteorológicos. Sismos. Cualquier eventualidad porcausa natural.	Daño o pérdida de los datos 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 datospersonales. Modificaciones no autorizadas.

ANÁLISIS DE BRECHA

Para realizar el análisis de brecha, el Comité de Transparencia de la Universidad Tecnológica Cadereyta, **(CTUTC)** de la UNIVERSIDAD TECNOLÓGICA CADEREYTA, 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 de esta Universidad.

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 de la UNIVERSIDAD TECNOLÓGICA

CADEREYTA
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 el responsable asignado del trámite que se está realizando.
- El área donde se recaban los datos personales, se encuentra dentro de las instalaciones de la Universidad.
- Cuando los datos personales son recabados de forma digital, se realiza por medio de un correo electrónico oficial del departamento.
- El área donde se recibe a los aspirantes y se recaban los datos personales se tiene adecuado, para que una vez que los datos fueron recibidos y capturados, los alumnos no puedan pasar al área donde se resguardan los expedientes.
- Las llaves de las oficinas y de los archiveros del departamento se encuentran resguardadas y solo pueden ser utilizadas por los miembros del mismo.
- Una vez recabados los datos personales, se genera un expediente, en el cual se resguarda la documentación entregada, este puede ser físico o electrónico, según sea el trámite.
- Los expedientes generados con los datos personales, ya sean físicos y/o electrónicos, son guardados en su área correspondiente, y solamente tendrán acceso los miembros del Departamento.
- Una vez recabados los datos personales de manera electrónica, son almacenados en el equipo del responsable del proceso, así como en carpetas compartidas, a las que solamente tienen acceso los miembros del departamento.
- Una vez concluido el trámite, los datos personales recabados se archivan en el expediente del trámite al que pertenecen.

MEDIDAS DE SEGURIDAD EN LA UNIVERSIDAD TECNOLÓGICA CADEREYTA

Medidas de seguridad físicas.

La UNIVERSIDAD TECNOLÓGICA CADEREYTA deberá implementar como mínimo las siguientes **medidas generales de seguridad 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 condatos 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.

La UNIVERSIDAD TECNOLÓGICA CADEREYTA 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;
II. Portar el gafete de visitante dentro de las instalaciones, por personas ajenas a la UNIVERSIDAD TECNOLÓGICA CADEREYTA Asegurar el retiro de pases de visita;
III. Identificar a los servidores públicos adscritos al sujeto obligado, los cuales deberán portar el gafete de identificación dentro de las instalaciones. La identificación deberá ser expedida y firmada por autoridad competente, e incluir cuando menos, nombre, cargo y número de empleado, fotografía, nombre de la Dependencia de su adscripcióny unidad administrativa a la que pertenece.

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 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 informaciónde datos personales, sin afectación de derechos laborales;
IV. Establecer en el contrato laboral, para el personal de nuevo ingreso, la existencia de medidas relacionadas con la seguridad en el manejo de la información y el tratamientode datos personales que deberá cumplir en el desempeño de su puesto, de conformidad con la Ley y normatividad aplicable, según resulte aplicable, asentando que una vez que

concluya la relación laboral o contractual, subsistirán las obligaciones de respeto a los principios de confidencialidad y secrecía en relación con la información de datos personales a la que tuvieron conocimiento o acceso;

V. Procurar permear la información señalada en la fracción inmediata anterior al personal que ya labora en la institución;

VI. Requerir, como parte de su obligación contractual con servidores públicos o terceros, que se acepten y firmen los términos, condiciones y obligaciones relacionados con el debido tratamiento de datos personales y la seguridad de información en términos dela Ley y demás normatividad aplicable;

VII. Procurar capacitar, conforme resulte procedente, a terceros con que se tenga una relación contractual sobre el debido tratamiento de datos personales, la existencia de amenazas de seguridad, de cómo pueden ser prevenidas mediante el debido cumplimiento de sus responsabilidades, obligaciones y de la pertinencia de la seguridad de la información;

VIII. 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;

IX. Suscribir acuerdos de confidencialidad con servidores públicos o terceros que actualmente estén relacionados con la seguridad de los servicios de procesamiento dela 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 dela 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 información de 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.

La UNIVERSIDAD TECNOLÓGICA CADEREYTA 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. Registrar habitualmente la información que corresponda en el Sistema de Datos Personales y mantenerlo actualizado;
II. Requerir el apoyo del área de tecnologías de la información para la implementación de medidas tecnológicas idóneas para proteger la información;

III. En caso de que UNIVERSIDAD TECNOLÓGICA CADEREYTA no cuente con un área de tecnologías de la información,convenir, según resulte procedente, con la Subsecretaría de Tecnologías de la Secretaría de Administración, para efectos del soporte informático necesario;
IV. Inventariar el equipo tecnológico que tiene La UNIVERSIDAD TECNOLÓGICA CADEREYTA, 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 sólo quede bajo la custodia de La UNIVERSIDAD TECNOLÓGICA CADEREYTA.
V. 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 UNIVERSIDAD TECNOLÓGICA CADEREYTA, en coordinación con el Departamento de Sistemas, 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 la UNIVERSIDAD TECNOLÓGICA CADEREYTA, el personal que labora en caseta principal deberá registrar al ciudadano y previa identificación, darle el acceso correspondiente con una tarjeta de visitante.
b. Una de las medidas de seguridad tomadas para prevenir errores por injerencias humanas, ya sea deliberadas o accidentales, es colocar cámaras de seguridad, las instalaciones de La UNIVERSIDAD TECNOLÓGICA CADEREYTA, se concentran en el edificio denominado Rectoría ubicada en las Instalaciones de la Universidad, siendo el titular de la oficina, la encargada del cuidado, resguardo y almacenamiento de la grabación de las cámaras quese encuentran en el edificio.

Medidas de seguridad en caso de desastres naturales.

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

b. **Incendios y humos:** Se cuenta con detectores y sensores contra incendios, humos y gases, los cuales se encuentran ubicados en puntos estratégicos dentro de esta La UNIVERSIDAD TECNOLÓGICA CADEREYTA, a detectar un incendio emiten una señal avisando que el siniestro está ocurriendo en un lugar determinado, cabe mencionar que La UNIVERSIDAD TECNOLÓGICA CADEREYTA, 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 la UNIVERSIDAD TECNOLÓGICA CADEREYTA, 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 los artículos 19, 20 y 21 del Reglamento Interior de la Secretaría de Administración del Estado de Nuevo León (última reforma integrada publicada en Periódico Oficial número 149, de fecha 14 de octubre de 2022), la Subsecretaría de Tecnologías es la unidad administrativa encargada de las medidas de seguridad con respecto a:

- Amenazas externas en la red
- Antivirus
- Firewall
- Instalación de software no autorizado
- Servidores y sus copias de seguridad
- Copias de seguridad o respaldos de la Información de los servidores

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 intranet de La UNIVERSIDAD TECNOLÓGICA CADEREYTA, previa solicitud del servicio a la Dirección Administrativa.

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 dealmacenamiento utilizables en un medio de almacenamiento, es decir, se trata deescribir 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 de La UNIVERSIDAD TECNOLÓGICA CADEREYTA, 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 La UNIVERSIDAD TECNOLÓGICA CADEREYTA, 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.

   El Comité de Transparencia revisará de manera anual, a partir de la emisión delpresente documento de seguridad:

2. La actualización de las medidas de Seguridad para la protección de datos personales.
3. 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.
4. La actualización del plan de trabajo de acuerdo a las medidas y situaciones que se presenten.

PROGRAMA GENERAL DE CAPACITACIÓN

Se manejarán las capacitaciones de conformidad con las necesidades de las unidades administrativas 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 elINFO NL.

Las fechas exactas se les notificarán a los encargados que sean designados con al menos una semana de anticipación a las fechas estimadas con la intención de que éstos las difundancon los interesados en asistir a las capacitaciones.

ACTUALIZACIONES AL DOCUMENTO DE SEGURIDAD

El presente documento de seguridad se actualizará cuando sucedan los siguientesacontecimientos:

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 delComité de Transparencia;
III. Como resultado de un proceso de mejora continua para mitigar el impacto deuna vulneración,
IV. Implementación de acciones correctivas y preventivas ante una vulneración deseguridad.

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 estructuraorgánica y atribuciones de las áreas que lo componen.

El presente documento fue aprobado por unanimidad de los integrantes del comité de Transparencia de la Universidad Tecnológica Cadereyta en la Primera sesión Ordinaria efectuada el día 14 de Abril 2024.

Firman los integrantes del Comité de Transparencia

Lic. Jorge Américo Castillo Medina
Abogado General
Presidente

Lic. Dania González Méndez
Jefatura de Recursos Humanos

Ing. Candido Abraham Galindo Seseña
Vocal del Comité
Secretario de Transparencia

ANEXO I. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES DE LA UNIVERSIDAD TECNOLÓGICA CADEREYTA

Departamento de Servicios Escolares y Estudiantiles.

1. Inscripción TSU y Continuidad
2. Becas
3. Ficha General de Salud Alumnos / Personal

1.- DEPARTAMENTO DE SERVICIOS ESCOLARES Y ESTUDIANTILES

1.1.-Inscripción TSU y Continuidad

1.1.1- Servidor público responsable del sistema o base de tratamiento

Nombre	Puesto	Correo electrónico	Teléfono Institucional
Oziel Ernesto Ramírez Ruiz	Subdirector de Servicios Escolares y Estudiantiles		
Samantha Puga Franco	Jefatura de Servicios Escolares y Estudiantiles		
Luis Carlos Gamboa Jalomo	Ingeniero en Sistema de Servicios Escolares y Estudiantiles		
Yajahira Elizabeth Cardenas Muñoz	Analista Administrativo de Servicios Escolares y Estudiantiles		

1.2.-Becas

1.2.1- Servidor público responsable del sistema o base de tratamiento

Nombre	Puesto	Correo electrónico	Teléfono Institucional
Oziel Ernesto Ramírez Ruiz	Subdirector de Servicios Escolares y Estudiantiles		
Roberto Jesús Barrón Alba	Jefe de Servicios Escolares y Estudiantiles		
Yajahira Elizabeth Cardenas Muñoz	Analista Administrativo de Servicios Escolares y Estudiantiles		

1.3.-Ficha General de Salud Alumnos / Personal

1.3.1- Servidor público responsable del sistema o base de tratamiento

Nombre	Puesto	Correo electrónico	Teléfono Institucional
Oziel Ernesto Ramírez Ruiz	Subdirector de Servicios Escolares y Estudiantiles		
Roberto Jesús Barrón Alba	Jefe de Servicios Escolares y Estudiantiles		
María Elena Cruz Torres	Analista Administrativo de Servicios Escolares y Estudiantiles		
Yadira Isabel Zamora Barrón	Analista Administrativo de Servicios Escolares y Estudiantiles		

2.-Objeto de la base de datos o sistema de tratamiento.

La finalidad para la cual se hace esta base de datos o sistema de tratamiento es debido a que los datos personales que se recaban integran la información mínima necesaria para la correcta operación de cada proceso:

2.1 Inscripción TSU y Continuidad. - Reunir la información de los aspirantes con el fin de concluir el proceso de inscripción a la Universidad para la integración de la matrícula de cada ciclo escolar, los cuales se registran en la R-02-8.2.2-CE Ficha de Inscripción, misma información que es capturada en el SIIDUT para la generación de matricula y otros conceptos.

2.2 Becas.- Recabar información de vivienda y gastos del hogar, la cual es analizada y considerada por un Comité para recibir un apoyo de beca, datos que son registrados en R-01-8.2.3.-CE Solicitud de Beca Interna y-o Renovación y en R-04-8.2.2-CE Estudio

Socioeconómico

2.3 Ficha General de Salud Alumnos / Personal.- Reunir información de salud del alumnado y el personal para en caso de Emergencia dar la atención adecuada, o bien, llamar a los servicios de atención médica y dar a aviso a los familiares de contacto.

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

DATO PERSONAL	FINALIDAD
Nombre	**Principal**: Todos estosdatos personales se utilizan para el desarrollo de los siguientes procesos: 1.Inscripción TSU y Continuidad 2.Becas 3.Ficha General de Salud Alumnos / Personal Mismos que se detallan en el punto 2.- *Objeto de la base de datos o sistema de tratamiento.*
Estado Civil	
Clave única de Registro de Población (CURP)	
Lugar de nacimiento	
Fecha de Nacimiento	
Nacionalidad	
Domicilio	
Teléfono particular y celular	
Correo electrónico	
Teléfonos de contacto	
Información de salud	
Ingresos/Gastos del hogar	

Los datos que se recaban no son considerados como sensibles.

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

La Dirección Jurídica a través de la Coordinación de Situación y Evolución Patrimonial cuenta con atribuciones para realizar el tratamiento de datos personales contenidos en esta base o sistema de tratamiento, de conformidad con los artículos 32, 33 y 34 del La Ley General de Responsabilidades Administrativas y artículo 12 fracción XVII del Reglamento Interior de la Contraloría y Transparencia Gubernamental.

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

FORMA DE OBTENCIÓN	MEDIOS DE ALMACENAMIENTO
Directamente: de forma directa con el interesado, formularios físicos **Indirectamente:** correo electrónico, WhatsApp	**Electrónico:** carpetas electrónicas en los equipos de cómputo del Departamento, en la nube (Google Drive). **Físico:** archiveros que almacena los expedientes de las y los estudiantes.

6.-Sitios de resguardo

El Departamento de Servicios Escolares y Estudiantiles resguarda los datos personales recabados de la siguiente forma:

a. Física, en los archiveros donde se encuentran los expedientes de las y los estudiantes.
b. Electrónica, en los equipos de cómputo del área y en la nube.

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

- ☐ Titulares de Servicios Escolares y Estudiantiles
- ☐ Ingeniero en Sistemas de Servicios Escolares y Estudiantiles
- ☐ Analistas Administrativos de Servicios Escolares y Estudiantiles

8.- Terceros encargados de datos personales.

Proveedor/Tercero	Coordinación Nacional De Becas Para el Bienestar Benito Juárez
Actividad	Administrador de la plataforma
Relación	Institucional
Instrumento jurídico que formalizala prestación del servicio	No aplica

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

1. Inscripción TSU y Continuidad. - La información obtenida es vitalicia, ya que se conserva aún después de causar egreso y titularse, los expedientes con copias y escaneados de los documentos originales se resguardan en el archivo muerto de la institución.
2. Becas. - Durante la estancia del alumno/a en la Institución y durante 5 años posteriores a su egreso.
3. Ficha General de Salud Alumnos / Personal. - El tiempo necesario desde su inscripción a la Universidad, o en su defecto, cuando el alumno/a solicite su baja de la Institución.

Al tratarse de datos personales contenidos en un equipo de cómputo o bien en la nube, los riesgos que por la propia naturaleza se tendrían son: la falla, robo o vandalización de los equipos, la falla en el acceso a la nube (sistema caído); por ello, la Universidad cuenta con el apoyo del Departamento de Sistemas quien se encarga de ejecutar acciones para garantizar la seguridad de la información.

Al tratarse de datos personales resguardados físicamente, los riesgos existentes sonla pérdida de la información, deterioro, así como su destrucción por error humano o siniestro.

ANEXO II. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES DE LA UNIVERSIDAD TECNOLÓGICA CADEREYTA

Vinculación

1. Promoción
2. Estadía Profesional
3. Bolsa de Trabajo
4. Modelo de Formación Dual
5. Seguimiento de Egresados

1.- VINCULACIÓN

1.1. Promoción

1.1.1- Servidor público responsable del sistema o base de tratamiento

Nombre	Puesto	Correo Electrónico	Teléfono Institucional
Yojebet Meléndez Zermeño	Jefatura de Promoción		
José Alfredo Bazana Pérez	Coordinador de Promoción		
Oziel Ernesto Ramírez Ruiz	Subdirector de Servicios Escolares y Estudiantiles		

1.2. Estadía Profesional

1.2.1- Servidor público responsable del sistema o base de tratamiento

Nombre	Puesto	Correo electrónico	Teléfono Institucional
Gloria Leticia Aguilar Pachecano	Coordinadora de Vinculación		
Angélica Liliana Garza Ibarra	Auxiliar de Vinculación		
Claudia Margarita Segovia Páez	Directora de Vinculación		

1.3. Bolsa de Trabajo

1.3.1- Servidor público responsable del sistema o base de tratamiento

Nombre	Puesto	Correo electrónico	Teléfono Institucional
Gloria Leticia Aguilar Pachecano	Coordinadora de Vinculación		
Angélica Liliana Garza Ibarra	Auxiliar de Vinculación		
Claudia Margarita Segovia Páez	Directora de Vinculación		

1.4. Modelo de Formación Dual

1.4.1- Servidor público responsable del sistema o base de tratamiento

Nombre	Puesto	Correo electrónico	Teléfono Institucional
Gloria Leticia Aguilar Pachecano	Coordinadora de Vinculación	.....	
Angélica Liliana Garza Ibarra	Auxiliar de Vinculación		
Claudia Margarita Segovia Páez	Directora de Vinculación		

1.5. Seguimiento de Egresados

1.5.1- Servidor público responsable del sistema o base de tratamiento

Nombre	Puesto	Correo electrónico	Teléfono Institucional
Gloria Leticia Aguilar Pachecano	Coordinadora de Vinculación		
Angélica Liliana Garza Ibarra	Auxiliar de Vinculación		
Claudia Margarita Segovia Páez	Directora de Vinculación		

2. Objeto de la base de datos o sistema de tratamiento.

La finalidad para la cual se hace esta base de datos o sistema de tratamiento es debido a que los datos personales que se recaban integran la información mínima necesaria para la correcta operación de cada proceso:

2.1 Promoción. - contar con los datos mínimos necesarios para dar seguimiento al (los)

Cond. de Jalisco

prospecto(s) a fin de concretar su inscripción como estudiantes de la Universidad, que en conjunto integran la matrícula de nuevo ingreso cada ciclo escolar, estos datos se registran en el R-02-8.5.3-VI Solicitud de Información de Prospectos, R-03-8.5.3-VI Lista de Prospectos. Los datos de los enlaces de Educación Media Superior se registran en el R-01-8.1-VI Calendario de Promoción.

2.2 Estadía Profesional. - contar con los datos mínimos necesarios de alumnos y empresarios, para documentar el proceso de Estadía Profesional de las y los estudiantes que cursan el último cuatrimestre de los programas educativos de Técnico Superior Universitario y de su continuidad a Ingeniería y Licenciatura, la cual se lleva a cabo en las instalaciones de una empresa de la zona de influencia, de acuerdo a los lineamientos y políticas del Modelo Educativo. Los registros donde obran uno o varios datos son: R- 01-8.5.3-VI Datos para la Estadía, R-02-8.6-VI Control de Estadía, R-03-8.5.1-VI Convenio de Estadías, R-04-8.6-VI Ejemplo de Carta de Terminación, R-05-8.5.1-VI Carta de Presentación, R-06-8.5.1-VI Autorización de Horario, R-01-8.5.1-VI Directorio de Empresas.

2.3 Bolsa de Trabajo. - contar con los datos de contacto mínimos necesarios para promover a las y los estudiantes registrados en la bolsa de trabajo en las empresas cuyas vacantes sean comunicadas a la Universidad, mediante el R-07-8.5.1-VI Vacante Empresa, y con ello contribuir a la colocación de egresados, en atención a los Lineamientos de Vinculación del Subsistema de Universidades Tecnológicas.

2.4 Modelo de Formación Dual. - contar con los datos mínimos necesarios para promover el perfil de las y los estudiantes en las empresas que pertenecen o desean pertenecer al Modelo de Formación Dual de la Universidad; así como documentar la Plataforma Dual de la Secretaría de Educación del Estado de Nuevo León. Los datos se almacenan en la plataforma de Registro y Control de Estudiantes de Educación Dual, diseñada para ese propósito y que es administrada por la propia Secretaría.

2.5 Seguimiento de Egresados. - contar con los datos requeridos por la Dirección General de Universidades Tecnológicas y Politécnicas para alimentar la base de datos del Seguimiento Nacional de Egresados y los diferentes instrumentos nacionales de Planeación y Evaluación. Los registros utilizados son: R-01-9.1.2-VI Encuesta de Satisfacción de Egresados y R-01-8.6-VI Encuesta de Satisfacción de Empleadores.

3. Datos personales que se recaban y su finalidad.

DATO PERSONAL	FINALIDAD
Nombre(s) y Apellidos	**Principal**: Todos estosdatos personales se utilizan para el desarrollo de los siguientes procesos: Promoción
Clave Única de Registro de Población (CURP)	
Fecha de Nacimiento / Edad al Egresar	
Nacionalidad	

Estado Civil	Estadía Profesional Bolsa de Trabajo Modelo de Formación Dual Seguimiento de Egresados Mismos que se detallan en el punto 2.- *Objeto de la base de datos o sistema de tratamiento.*
Nivel de escolaridad	
Domicilio	
No. de teléfono celular / No. de teléfono particular / No. de teléfono de familiar.	
Correo electrónico	
Puesto / Cargo que desempeña / Área / Tipo de Contrato	
Sueldo	
Antigüedad	

Los datos que se recaban no son considerados como sensibles.

4. Fundamento legal que lo faculta para el tratamiento.

La Dirección Jurídica a través de la Coordinación de Situación y Evolución Patrimonial cuenta con atribuciones para realizar el tratamiento de datos personales contenidos en esta base o sistema de tratamiento, de conformidad con los artículos 32, 33 y 34 del La Ley General de Responsabilidades Administrativas y artículo 12 fracción XVII del Reglamento Interior de la Contraloría y Transparencia Gubernamental.

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

FORMA DE OBTENCIÓN	MEDIOS DE ALMACENAMIENTO
Directamente: de forma directa con el interesado, formularios físicos (registros del Sistema de Gestión de la Calidad, bitácora) **Indirectamente:** correo electrónico, WhatsApp, Inbox de Facebook, Facebook Seguimiento de Egresados, formularios electrónicos (Google Forms).	**Electrónico:** carpetas electrónicas en los equipos de cómputo del Departamento, en la nube (Google Drive). **Físico:** archivero que almacena los expedientes de las y los estudiantes.

6. Sitios de resguardo

La Dirección de Vinculación resguarda los datos personales recabados de la siguiente forma:

c. Electrónica, en los equipos de cómputo del área y en la nube.
d. Física, en los archiveros donde obran los expedientes de las y los estudiantes.

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

- ☐ Titular de Vinculación
- ☐ Titular de Servicios Escolares y Estudiantiles
- ☐ Jefa de Promoción
- ☐ Coordinadora de Vinculación
- ☐ Coordinador de Promoción

☐ Auxiliar de Vinculación

8. Terceros encargados de datos personales.

Para la plataforma de Registro y Control de Estudiantes de Educación Dual

Proveedor/Tercero	Secretaría de Educación Pública del Estado de Nuevo León
Actividad	Administrador de la plataforma
Relación	Institucional
Instrumento jurídico que formalizala prestación del servicio	No aplica

9. Ciclo de Vida y Riesgo

9.1 Promoción. - 1-2 cuatrimestres, mientras el prospecto se inscribe como alumno(a), una vez inscrito(a) el resguardo y manejo de los datos personales queda bajo la responsabilidad de Servicios Escolares y Estudiantiles.

9.2 Estadía Profesional. - Durante el proceso de estadía y durante 5 años posteriores al egreso de las y los estudiantes.

9.3 Bolsa de Trabajo. - el tiempo necesario hasta que el alumno sea colocado en el mercado laboral.

9.4 Modelo de Formación Dual. - el tiempo necesario, desde su inicio en el Modelo de Formación Dual y hasta su egreso; o en su defecto, cuando el(la) estudiante solicite baja del modelo, de la Universidad o de la empresa.

9.5 Seguimiento de Egresados. - 5 años posteriores al egreso de las y los estudiantes.

Al tratarse de datos personales contenidos en un equipo de cómputo o bien en la nube, los riesgos que por la propia naturaleza se tendrían son: la falla, robo o vandalización de los equipos, la falla en el acceso a la nube (sistema caído); por ello, la Universidad cuenta con el apoyo del Departamento de Sistemas quien se encarga de ejecutar acciones para garantizar la seguridad de la información.

Al tratarse de datos personales resguardados físicamente, los riesgos existentes sonla pérdida de la información, deterioro, así como su destrucción por error humano o siniestro.