Documento de Seguridad

Instituto de Capacitación y Vinculación Tecnológica del Estado de Chiapas

ÍNDICE

PRESENTACIÓN.

La Constitución Política de los Estados Unidos Mexicanos en los artículos 6 y 16 incorpora el derecho de toda persona a la protección de sus datos personales, así como al acceso, rectificación, cancelación y oposición en los términos que determina la ley.

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO o Ley General) y la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas (LPDPPSOECH o Ley Estatal) establece por su parte un conjunto de bases, principios y procedimientos para garantizar el derecho a la protección de datos con carácter personal y que se encuentren en posesión de los sujetos obligados.

De ahí que el presente Documento de Seguridad tiene como propósito establecer el marco de referencia del tratamiento de los datos personales que se llevan a cabo al interior del Instituto de Capacitación y Vinculación Tecnológica del Estado de Chiapas por los diversos órganos administrativos que conforman su estructura orgánica, para mantener vigente y promover la mejora continua en la protección de los mismos, en términos de lo previsto por las leyes en materia mencionadas en el párrafo anterior, además de desarrollar buenas prácticas en la materia.

En ese sentido, del Instituto de Capacitación y Vinculación Tecnológica del Estado de Chiapas ha identificado los procesos que en el ámbito de su competencia involucran el tratamiento de datos personales, a efecto de mantener la seguridad de los mismos durante el ciclo de vida de la información, indicando la forma en la que se trata, las medidas de seguridad adoptadas y las áreas responsables de su protección, así como las finalidades del tratamiento de acuerdo a sus respectivos ámbitos de funciones.

Considerando que los datos personales constituyen el principal activo de información objeto del presente documento, es necesario señalar que todos y cada uno de los elementos que lo integran, constituyen un sistema interno para la gestión y tratamiento de los datos personales en posesión del Instituto de Capacitación y Vinculación Tecnológica del Estado de Chiapas, pues se entiende por sistema de gestión al conjunto

de elementos y actividades interrelacionadas para establecer, operar, monitorear, mantener y mejorar el tratamiento y seguridad de los datos personales.

Así, el Instituto de Capacitación y Vinculación Tecnológica del Estado de Chiapas, comprometido con la tutela de los datos personales que trata impulsa a su interior las acciones conducentes para evitar la alteración, pérdida, transmisión y acceso no autorizados a los datos, mediante la implementación de medidas físicas, administrativas y técnicas, tendentes a garantizar la seguridad e integralidad de los mismos, así como su seguimiento y supervisión continuos.

De ahí, que dicho Sistema permita disponer de información relacionada con las medidas de seguridad, el análisis general de las amenazas y posibles vulnerabilidades, así como los mecanismos o acciones a implementar para mitigarlas, integrándose a partir la gestión de actividades coordinadas para controlar y verificar que el tratamiento de los datos personales sea acorde con los principios que rigen su protección.

GLOSARIO DE TÉRMINOS.

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

II. Aviso de privacidad: Documento físico, electrónico o en cualquier otro formato generado por el responsable, que es puesto a disposición del titular con el objeto de informarle los propósitos principales del tratamiento al que serán sometidos sus datos personales.

III. Base de datos: Conjunto ordenado de datos personales que estén en posesión del responsable, ya sea en formato escrito, impreso, digital, sonoro, visual, electrónico, informático u holográfico, referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

IV. Catálogo de base de datos personales: Lista detallada del conjunto ordenado de base de datos personales que estén en posesión del responsable, ya sea en formato escrito, impreso, digital, sonoro, visual, electrónico, informático u holográfico, referente a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

V. Consentimiento: Manifestación de la voluntad libre, específica e informada del titular, mediante la cual autoriza el tratamiento de sus datos personales.

VI. Datos Personales: Cualquier información numérica alfabética, grafica, fotográfica, acústica o de cualquier otro tipo concerniente a una persona física o identificable, se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

VII. Datos personales sensibles: Aquellos que se refieren a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo

grave para éste. Se consideran sensibles, de manera enunciativa más no limitativa, los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud pasado, presente o futuro, creencias religiosas, filosóficas y morales, opiniones políticas, datos genéticos, datos biométricos y preferencia sexual.

VIII. Derechos ARCO: Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales.

IX. 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.

X. Encargado: Prestador de servicios, que con el carácter de persona física o jurídica pública o privada, ajena a la organización del responsable, trata datos personales a nombre y por cuenta de éste.

XI. ICATECH: Al Instituto de Capacitación y Vinculación Tecnológica del Estado de Chiapas.

XII. Inventario de datos personales: Lista ordenada y detallada que posea el responsable o encargado, de cualquier información numérica, alfabética, grafica, fotográfica, acústica o de cualquier otro tipo, concerniente a una persona física identificada o identificable.

XIII. Ley Estatal: Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Chiapas.

XIV. Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismo administrativos, técnicos y físicos que permitan proteger los datos personales.

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

XVI. Medidas de seguridad físicas: Conjunto de acciones y mecanismo para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento como prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información.

XVII. Medidas de seguridad técnicas: Conjunto de acciones, mecanismos y sistemas de los datos personales y los recursos involucrados en su tratamiento como revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware.

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

XIX. Remisión: Toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado, con independencia de que se realice dentro o fuera del territorio mexicano.

XX. Responsable: Cualquier autoridad, dependencia, entidad, órgano y organismos de los poderes Legislativo, Ejecutivo y Judicial, ayuntamientos, órganos constitucionales autónomos, fideicomisos y fondos públicos y partidos políticos locales, que decide y determina los fines, medios y demás cuestiones relacionadas con determinado tratamiento de datos personales.

XXI. Titular: Persona física a quien corresponde los datos personales.

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

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

OBJETIVOS DEL DOCUMENTO DE SEGURIDAD.

I. Proveer el marco de trabajo necesario para la protección de los datos personales en posesión del Instituto de Capacitación y Vinculación Tecnológica del Estado de Chiapas;
II. Cumplir con las obligaciones que establece, la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del estado de Chiapas y los Lineamientos Generales, así como la normatividad que derive de los mismos;
III. Establecer los elementos y actividades de dirección, operación y control de los procesos que impliquen el tratamiento de datos personales, a efecto de protegerlos de manera sistemática y continua, y
IV. Promover la adopción de mejores prácticas en la protección de datos personales, de manera preferente una vez que el programa se haya implementado de manera integral en la organización, o bien, cuando se estime pertinente la implementación de buenas prácticas en tratamientos específicos.
V. Determinar las posibles vulnerabilidades, amenazas y riesgos de los que pueden ser objeto los diversos sistemas de información y procesos en los se tratan datos personales por las diversas unidades administrativas.

ALCANCES DEL DOCUMENTO DE SEGURIDAD.

El alcance de este documento se relaciona con la identificación de sistemas de información o procesos administrados por parte de cada uno de los órganos administrativos del Instituto de Capacitación y Vinculación Tecnológica del Estado de Chiapas, en los que de acuerdo con su ámbito de funciones llevan a cabo el uso y tratamiento de datos personales, mismos que se encuentran bajo su estricta responsabilidad tanto en los medios electrónicos como en los espacios físicos en que se administran, operan y resguardan dichos datos personales.

Los órganos administrativos que forman parte del Instituto de Capacitación y Vinculación Tecnológica del Estado de Chiapas a la fecha de emisión del presente instrumento, así como las que posteriormente sean incorporadas a su estructura, y que deberán observar el Programa son las siguientes:

- Dirección General
- Comisaría
- Unidad Jurídica
- Unidad Ejecutiva
    - Área de Desarrollo Administrativo
    - Área de Informática
    - Área de Mercadotecnia
- Unidad de Transparencia
- Dirección Administrativa
    - Departamento de Recursos Financieros
    - Departamento de Recursos Humanos
    - Departamento de Recursos Materiales
- Dirección de Planeación
    - Departamento de Programación y Presupuesto
    - Departamento de Proyectos y Análisis

    - Departamento de Organización y Evaluación
- Dirección Técnica Académica
    - Departamento de Gestión Académica
    - Departamento de Certificación y Control
    - Departamento de Información e Innovación Académica
- Dirección de Vinculación
    - Departamento de Vinculación Gubernamental
    - Departamento de Vinculación Social y Empresarial
    - Departamento de Vinculación para la Competitividad
- Dirección de Unidad de Capacitación Tuxtla Gutiérrez
    - Departamento de Vinculación
    - Delegación Administrativa
    - Departamento Académico
- Dirección de Unidad de Capacitación Comitán
    - Departamento de Vinculación
    - Delegación Administrativa
    - Departamento Académico
- Dirección de Unidad de Capacitación Tapachula
    - Departamento de Vinculación
    - Delegación Administrativa
    - Departamento Académico
- Dirección de Unidad de Capacitación Reforma
    - Departamento de Vinculación
    - Delegación Administrativa
    - Departamento Académico
- Dirección de Unidad de Capacitación Tonalá
    - Departamento de Vinculación
    - Delegación Administrativa
    - Departamento Académico
- Dirección de Unidad de Capacitación Villaflores
    - Departamento de Vinculación

  - Delegación Administrativa
  - Departamento Académico
- Dirección de Unidad de Capacitación Jiquipilas
  - Departamento de Vinculación
  - Delegación Administrativa
  - Departamento Académico
- Dirección de Unidad de Capacitación Catazajá
  - Departamento de Vinculación
  - Delegación Administrativa
  - Departamento Académico
- Dirección de Unidad de Capacitación Yajalón
  - Departamento de Vinculación
  - Delegación Administrativa
  - Departamento Académico
- Dirección de Unidad de Capacitación San Cristóbal de Las Casas
  - Departamento de Vinculación
  - Delegación Administrativa
  - Departamento Académico
- Dirección de Unidad de Capacitación Ocosingo
  - Departamento de Vinculación
  - Delegación Administrativa
  - Departamento Académico

INVENTARIO DE DATOS PERSONALES DEL ICATECH.

Por inventario de tratamiento de datos, se entiende el control documentado del conjunto de operaciones que realizan los órganos administrativos del ICATECH con motivo de los datos que se recaban de las personas, a través de procedimientos automatizados o físicos, que van desde su obtención, registro, organización, conservación, utilización, difusión, hasta la rectificación, cancelación y oposición, con motivo de la atención del ejercicio de estos derechos en el ámbito de sus atribuciones.

Es así que a través del desarrollo de un instrumento homogéneo y estandarizado, se llevó a cabo el levantamiento del inventario de datos, con el propósito de identificar, entre otros aspectos, la categoría y tipo datos que son sometidos a tratamiento, incluyendo los de carácter sensible; los medios a través de los cuales se obtienen dichos datos; el sistema físico y/o electrónico que se utiliza para su acceso, manejo, aprovechamiento, monitoreo y procesamiento; las características del lugar donde se ubican las bases físicas o electrónicas de datos; las finalidades del tratamiento, y el nombre, cargo y adscripción de los servidores públicos que tienen acceso al tratamiento, además de si son objeto de la transferencia y la identificación de los destinatarios o receptores de los mismos, así como las causas que la justifican.

En ese mismo sentido, el inventario ha contribuido desde el punto operativo a considerar el ciclo de vida de los datos personales, de forma tal que los servidores públicos que intervienen en el tratamiento conocen que, una vez concluida la finalidad los datos, éstos deben ser sometidos a un proceso de bloqueo y, en su caso, de cancelación, supresión o destrucción, lo que cobra especial relevancia en el marco del proceso de baja documental que las áreas realizan conforme a las disposiciones que regulan la gestión documental al interior de la Institución.

En tal virtud, en coordinación con los órganos administrativos y derivado del proceso de actualización de información, se advirtió que, 21 órganos administrativos (mismas que se encuentran integrados por direcciones, unidades, áreas y departamentos) llevan a cabo el tratamiento de datos personales a través de diversos procedimientos internos propios de sus respectivas atribuciones y facultades.

A continuación, se enlista y resume el inventario de datos personales arrojado del sondeo a cada uno de los órganos administrativos del ICATECH:

Órgano Administrativo	Procedimiento Administrativo	Categoría de Datos Personales	No. de Procedimientos:
Dirección General	▪ Registro de Visitantes (Audiencias)	Identificativos	01
Unidad Jurídica	▪ Procedimientos Administrativos del ICATECH. ▪ Procedimientos judiciales del ICATECH. ▪ Reporte trimestral de Procedimientos judiciales del ICATECH.	Legales	03
Unidad de Transparencia	▪ Atención a Solicitudes de Información. ▪ Elaboración de Actas. ▪ Directorio de Responsables de Transparencia, Archivo y Datos Personales. ▪ Controles archivísticos.	▪ Identificativos. ▪ Identificativos y laborales. ▪ Identificativos y laborales ▪ Identificativos y laborales.	04

Unidad Ejecutiva.			04
-Área de Desarrollo Administrativo.	▪ Supervisión Funcional a los Órganos Administrativos a través de encuestas electrónicas.	▪ Identificativos y laborales.	
-Área de Informática.	▪ Creación de Firma Electrónica Avanzada ▪ Carga de información en materia de Transparencia.	▪ Electrónicos. ▪ Patrimoniales.	
-Área de Mercadotecnia.	▪ Difusión institucional	▪ Identificativos.	
Dirección Administrativa			11
-Depto. de Recursos Financieros.	▪ Pago de Honorarios. ▪ Pago de Bienes y Servicios.	▪ Financieros e Identificativos.	
-Depto. de Recursos Humanos.	▪ Movimientos nominales de personal. ▪ Registro de alta para registro de asistencia de personal.	▪ Identificativos, y laborales. ▪ Identificativos y Biométricos.	

-Depto. de Recursos Materiales.	▪ Reporte de altas, bajas y cambios de servidores públicos ante la Secretaria de la Honestidad y la Función Pública. ▪ Integración de Expediente de Personal. ▪ Tramite de Pago de Compras Directas Menores y Servicios Básicos. ▪ Excepción al Proceso Licitatorio (Adjudicación Directa). ▪ Procesos licitatorios ▪ Registro de acceso de visitantes a las Instalaciones del ICATECH. ▪ Monitoreo y Vigilancia con cámaras.	▪ Identificativos. ▪ Identificativos y Académicos. Identificativos.	
<u>Dirección de Planeación</u> -Depto. de Programación y Presupuesto.	▪ Validación de suficiencia presupuestal para pago de instructores.	Identificativos	03

-Depto. de Proyectos y Análisis. -Depto. de Organización y Evaluación.	▪ Actualización del Formato de Validación de Recursos de Servicios Personales (Layout) ▪ Reunión de Juntas Directivas		
<u>Dirección Técnica Académica.</u> -Depto. de Gestión Académica. -Depto. de Certificación y Control. -Depto. de Información e Innovación Académica.	▪ Validación de Instructores. ▪ Certificación y Control de Formato T. ▪ Validación de Exoneración y Reducción de Pago	Identificativos y Académicos	03
<u>Dirección de Vinculación.</u> -Depto. de Vinculación Gubernamental.	▪ Validación de documentación para suscribir de Convenios.	Identificativos y Legales	03

-Depto. de Vinculación Social y Empresarial. -Depto. de Vinculación para la Competitividad.	▪ Validación de documentación para suscribir de Convenios. ▪ Validación de documentación para suscribir de Convenios.		
<u>Unidades de Capacitación.</u> *-Departamento Académico.* *-Departamento de Vinculación.* *-Delegación Administrativa.*	▪ Integración del Expediente Único del Curso: - *Validación del Instructor, Integración de RIACS, Solicitud de Apertura del Curso, Evidencias del Curso.* - *Exoneración y Reducción de Pago, Expediente del Alumno; Integración del SID, Integración de Convenios y Actas de Acuerdo* - *Contrato y pago de Instructores.*	Identificativos	01

Total de Órganos Administrativos que tratan datos personales:	Total de Procedimientos Administrativos que involucran datos personales:	Categorías involucradas:	
21	33	- Identificativos - Laborales - Académicos - Patrimoniales - Financieros - Legales - Biométricos - Electrónicos - Salud	

A partir de lo anterior, el Inventario de Datos Personales del ICATECH posibilitó la identificación de hallazgos en relación con el tratamiento de datos personales, aportando los elementos que permiten focalizar las áreas con mayor incidencia en el tratamiento de éstos, y con ello, enfocar los trabajos de atención para el cumplimiento de las disposiciones aplicables en materia de protección de datos.

A continuación, se describen las categorías de datos personales con los que cuenta el ICATECH, esto; según el Inventario de Datos Personales que fue integrado de manera conjunta con los Órganos Administrativos involucrados.

Datos de identificación: Nombre, domicilio, teléfono particular y/o celular, correo electrónico personal, estado civil, firma, firma electrónica, lugar y fecha de nacimiento, nacionalidad, edad, fotografía, clave del Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP), nombres de familiares, dependientes y/o beneficiarios.

Datos Laborales: Datos contenidos en las solicitudes de empleo (correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales, referencias personales, capacitaciones, nombramiento,

incidencias, hojas de servicio y otras generadas derivadas de nuestra una relación laboral).

Datos Académicos: Permiten identificar la trayectoria académica y formación profesional (calificaciones, boletas, constancias, certificados, reconocimientos, títulos, cédulas profesionales, etc.).

Datos Patrimoniales y/o Financieros: Bienes muebles e inmuebles, ingresos y egresos, cuentas bancarias, seguros, afores, información fiscal, etc.

Datos Legales: Situación jurídica de la persona (juicios, amparos, procesos administrativos, entre otros.)

Datos biométricos (DATO PERSONAL SENSIBLE): Datos relacionados con propiedades biológicas, características fisiológicas o rasgos de nuestra persona que mediante métodos automáticos identifican rasgos físicos únicos e intransferibles (huella dactilar).

Datos electrónicos (DATO PERSONAL SENSIBLE): Datos relativos a correos electrónicos, nombres de usuarios, contraseñas, firma electrónica, dirección de IP (Protocolo de Internet) privada, o cualquier dirección de control o información que implique la identificación o acceso en internet, conexión o red de comunicación electrónica.

Datos de salud (DATO PERSONAL SENSIBLE): Datos relacionados con el estado físico o discapacidades.

Tipos de personas de quienes se obtienen los datos personales:

- Personas externas que solicitan información y/o participan en los cursos que promueve el ICATECH.
- Personal que labora en el ICATECH.
- Personas externas que acuden a las oficinas del ICATECH a realizar diversas diligencias.

- Personas externas que ofrecen servicios derivados de las adquisiciones, licitaciones y servicios en las que el ICATECH es parte.
- Personas que participan en la suscripción de Convenios en los que el ICATECH es parte.

Los datos personales se recaban por medio de:

- Documentos presentados ante el ICATECH.
- Por el llenado de formularios físicos y/o electrónicos.
- Por la información proporcionada de manera verbal y directa por los titulares de los datos personales.

FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATAN DATOS PERSONALES.

Los órganos administrativos son responsables del manejo de los datos personales en virtud de sus facultades administrativas y operativas que están enfocadas a impartir e impulsar la capacitación acelerada para el trabajo en la entidad procurando la mejor calidad y vinculación de este servicio con el aparato productivo y las necesidades de desarrollo regional, estatal y nacional; así como de las actividades administrativas que se deriven de lo anterior.

Por lo anterior; los responsables e involucrados en el tratamiento de los datos personales también están obligados a:

- Dar cumplimiento a los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad contemplados en la Ley Estatal, garantizando la debida protección de los datos personales, conforme a las disposiciones aplicables.
- Integrar el formato de inventario de datos personales.
- Realizar y vigilar el cumplimiento de los Avisos de Privacidad de acuerdo a las atribuciones que les compete.
- Garantizar la confidencialidad respecto de los datos personales tratados, dicha obligación, subsistirá aún después de finalizar las relaciones laborales con el ICATECH y sin menoscabo de los establecidos en las disposiciones de acceso a la información pública.
- Conocer y aplicar las acciones derivadas de este Documento de Seguridad.
- Garantizar el cumplimiento de los derechos ARCO a los titulares de los datos personales.

Registro de incidencias.

Se entiende que el origen de las incidencias con respecto al manejo y la protección de los datos personales, representan una vulnerabilidad por lo que es necesario que los Órganos Administrativos registren y reporten las incidencias que se susciten. Dicho registro de incidencias deberá contener, por lo menos:

- Fecha de la incidencia
- Tipo de incidencia.
- Descripción de la incidencia.
- Personas involucradas.
- Persona a quien se le comunica.
- Consecuencias que tendrá la incidencia.

El personal del ICATECH que trate datos personales debe de contar con el registro de incidencias, ya que quien identifique la incidencia será el encargado de registrarla y notificar a su superior inmediato, quien a su vez se encargará de notificar a las o los personas afectadas para que este tome las precauciones debidas en caso de uso inadecuado de la información.

Identificación y autentificación

El personal del Área de Informática, es quien administra los datos sobre los equipos de cómputo y respectivos usuarios y quienes son responsables directos del uso de los mismos; asimismo, asignan usuarios y contraseñas para uso de los equipos de cómputo, por lo que la reserva y confidencialidad de estas contraseñas queda bajo la responsabilidad del personal a la que se le designó la cuenta de usuario; de tal forma que por ningún motivo las cuentas y las contraseñas de los usuarios de los correos electrónicos y de los equipos de cómputo serán transferibles, excepto los casos que sean

de común acuerdo por todos los responsables sin menoscabar ningún derecho o privilegio a persona o institución alguna.

ANÁLISIS DE RIESGOS.

La realización del análisis de riesgo está a cargo de la Unidad de Transparencia y/o del Oficial de Datos Personales del ICATECH, este; es aplicable a los órganos administrativos que tratan datos personales y debe contener por lo menos lo siguiente:

I. Identificar las vulnerabilidades y amenazas a las que el correcto tratamiento de los datos personales se encuentra expuesto en cada proceso; tomando en consideración:
   a) La sensibilidad de los datos personales tratados.
   b) La transferencia de datos personales que se realicen.
   c) El valor de los datos personales de acuerdo con su clasificación previamente definida.
   d) El valor y exposición de los activos involucrados en el tratamiento de los datos personales.
   e) El valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión
II. Posibles consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad a los datos personales.

Considerando que la identificación de vulnerabilidades tiene por objeto prevenir posibles dificultades en la seguridad de los datos bajo un enfoque proactivo; resulta imprescindible identificar áreas de oportunidad en materia de seguridad de datos personales sin que éstas constituyan un daño efectivo.

> *Vulnerabilidad.- Es la debilidad propia de un sistema o procedimiento que permite ser atacado o recibir un daño. Estas se producen por una baja protección y también se les conoce como agujeros de seguridad; sin embargo, tienen la ventaja de poder ser solventados una vez que son identificados.*

Amenaza.- Es la acción provocada por la vulnerabilidad de un sistema o procedimiento y provocándole modificaciones o daños provenientes de fuentes externas (sucesos naturales o por acción humana).

Vulnerabilidades	Amenazas	Valor de Riesgo Inherente.
1.- Ausencia de controles de registro (bitácoras) para la consulta de expedientes representa.	• Robo, extravío o copia no autorizada de bases de datos o archivos que contienen datos personales. • Uso o tratamiento no autorizado a de bases de datos o archivos que contienen datos personales. • Daño, alteración o modificación no autorizada de bases de datos o archivos que contienen datos personales. • Pérdida o destrucción no autorizada de bases de datos o archivos que contienen datos personales.	- Riesgo inherente medio

2.- Hábito de resguardar expedientes en espacios a los que se puede tener acceso sin restricciones.	• Robo, extravío o copia no autorizada de bases de datos o archivos que contienen datos personales. • Uso o tratamiento no autorizado a de bases de datos o archivos que contienen datos personales. • Daño, alteración o modificación no autorizada de bases de datos o archivos que contienen datos personales. • Pérdida o destrucción no autorizada de bases de datos o archivos que contienen datos personales.	- Riesgo inherente medio.
3.- Los equipos de cómputo y el acceso a las redes o servidores generalmente no cuentan con accesos restringidos (usuarios y contraseñas), por lo	• Robo, extravío o copia no autorizada de bases de datos o archivos que contienen datos personales. • Uso o tratamiento no autorizado a de bases de datos o archivos que contienen datos personales.	- Riesgo inherente medio.

que el ingreso a los equipos electrónicos para la consulta de archivos electrónicos es de fácil acceso.	• **Daño, alteración o modificación no autorizada** de bases de datos o archivos que contienen datos personales. • **Pérdida o destrucción no autorizada** de bases de datos o archivos que contienen datos personales.	
4.- Compartir tareas o actividades que incluyan acceso a bases de datos almacenados de forma digital representa un riesgo en virtud de que no se delimita claramente el rol específico de cada uno de los involucrados; por lo que las responsabilidades no son claras y no existe el compromiso específico del resguardo y manejo	• **Robo, extravío o copia no autorizada** de bases de datos o archivos que contienen datos personales. • **Uso o tratamiento no autorizado** a de bases de datos o archivos que contienen datos personales. • **Daño, alteración o modificación no autorizada** de bases de datos o archivos que contienen datos personales. • **Pérdida o destrucción no autorizada** de bases de datos o archivos que contienen datos personales.	- Riesgo inherente medio.

adecuado de la información.		
5.- La falta de instrumentos, como lo es la CARTA DE CONFIDENCIALIDAD; representa un riesgo en virtud de que no existe el compromiso ni la responsabilidad asumida por cada uno de los colaboradores del ICATECH de desempeñarse con integridad respecto del tratamiento adecuado de los datos personales bajo resguardo del Instituto.	• Robo, extravío o copia no autorizada de bases de datos o archivos que contienen datos personales. • Uso o tratamiento no autorizado a de bases de datos o archivos que contienen datos personales. • Daño, alteración o modificación no autorizada de bases de datos o archivos que contienen datos personales. • Pérdida o destrucción no autorizada de bases de datos o archivos que contienen datos personales.	- Riesgo inherente medio.

Con base en el análisis de riesgo, además de promover el reconocimiento de las medidas de seguridad administrativas, entendidas como el conjunto de políticas y procedimientos de gestión, soporte y revisión de la seguridad de la información; físicas, que corresponden a las acciones o mecanismos para proteger el entorno físico de los datos, así como de los

recursos involucrados en su tratamiento y, técnicas que se valen de la tecnología para proteger el entorno digital de la información, también se torna indispensable implementar medidas de seguridad para fortalecer algunos de los controles que actualmente son implementados; es decir, ejecutar el análisis de brecha.

ANÁLISIS DE BRECHA.

Con el análisis de brecha se busca mitigar las amenazas a los que están expuestos los datos tratados que de manera general puede presentarse en caso de que las amenazas señaladas exploten las vulnerabilidades. Con esto, se busca mitigar el riesgo del acceso a los datos personales de manera no autorizada con el fin de comprometer su confidencialidad, disponibilidad e integridad, por lo que las medidas de seguridad por parte de las áreas comisionadas están orientadas a proteger los datos personales.

Identificar los tipos de datos personales que se tratan, la sensibilidad de los mismos y el número de titulares involucrados es útil para determinar el valor de riesgo inherente de que los datos sean accesibles a un tercero no autorizado.

- Datos con riesgo inherente bajo

Esta categoría considera vulneración a la información general concerniente a una persona física identificada o identificable, como por ejemplo datos de identificación y contacto o información académica o laboral, tal como nombre, teléfono, edad, sexo, RFC, CURP, estado civil, dirección de correo electrónico, lugar y fecha de nacimiento, nacionalidad, puesto de trabajo y lugar de trabajo, idioma o lengua, escolaridad, cedula profesional, información migratoria, entre otra información que no refiera a los siguientes tres categorías.

- Datos riesgo inherente medio

Esta categoría contempla los datos que permiten conocer la ubicación física de la persona, tales como la dirección física, información relativa al tránsito de las personas dentro y fuera del país, y/o cualquier otro que permita volver identificable a una persona a través de los datos que proporcione alguien más, por ejemplo: dependencia, beneficiarios, familiares, referencias laborales, referencias personales, etc.

También son datos de riesgo inherente medio aquellos que permitan inferir el patrimonio de una persona, que incluye entre otros, los saldos bancarios, estados y/o número de cuenta, cuentas de inversión, bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos, egresos, buró de crédito, seguros, afores, fianzas, sueldos y salarios, servicios contratados. Incluye el número de tarjeta bancaria de crédito y/o débito.

Son considerados también, los datos de autenticación con información referente a los usuarios, contraseñas, información biométrica (huellas dactilares, iris, voz, entre otros) firma autógrafa y electrónica, fotografías, identificaciones oficiales, inclusive escaneadas o fotocopiadas y cualquier otro que permita autenticar a una persona.

Dentro de esta categoría se toman en cuenta los datos jurídicos tales como antecedentes penales, amparos, demandas, contratos litigios y cualquier otro tipo de información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil penal o administrativa.

- Datos con riesgo inherente alto

Esta categoría de datos contempla a los datos personales sensibles, que de acuerdo a la Ley incluyen datos de salud los cuales se refieren a la información médica donde se documente el estado de salud física y mental, pasado, presente o futuro; información genética; origen racial o étnico, ideología, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual, hábitos sexuales y cualquier otro cuya utilización indebida pueda dar origen a discriminación o con lleve un riesgo grave para la/el titular.

Los datos de mayor riesgo son los que de acuerdo a su naturaleza derivan en mayor beneficio para un atacante, por ejemplo:

Información adicional de tarjeta bancaria que considera el número de la tarjeta de crédito y/o débito mencionado anteriormente en combinación con cualquier otro dato relacionado o contenido de la misma, por ejemplo, fecha de vencimiento, códigos de seguridad, datos de banda magnética o número de identificación personal (PIN).

Las personas de alto riesgo son aquellas cuya profesión, oficio o condición están expuestas a una mayor probabilidad de ser atacadas debido al beneficio económico o reputacional que sus datos personales pueden representar para un atacante, por ejemplo, líderes políticos, religiosos, empresariales, de opinión y cualquier otra persona que sea considerada como personaje público.

Asimismo, se considera a cualquier persona cuya profesión esté relacionada con la impartición de justicia y seguridad nacional. Tratar datos de personas de alto riesgo involucra que la base de datos contiene nombres de figuras públicas que pueden ser reconocidas a primera vista, así como información personal donde se infiera o se relacione explícitamente con su profesión, puesto o cargo en combinación con datos de identificación como nombre, domicilio, entre otros.

Considerando lo anterior y analizando de manera cuantitativa y cualitativa sobre la posibilidad de que un activo de información pueda sufrir una pérdida o daño, así como las causas y consecuencias de la amenaza y vulnerabilidades en los sistemas de tratamiento de datos personales, se establece que los efectos de posibles vulneraciones de seguridad al interior del ICATECH se encuentran dentro del rango de:

Datos con riesgo inherente medio.

PLAN DE TRABAJO.

A. Canalizar a cada dirección, unidad o áreas, que trate datos personales, la encuesta sobre el estado actual del cumplimiento de las obligaciones en materia de datos personales para que sea contestada y así poder conocer el nivel del tratamiento de los datos personales con los cuales se trabajara.
B. Capacitar al personal del ICATECH en materia de datos personales.
C. Proponer a las áreas respectivas la implementación de seguridad físicas, administrativas y técnicas para la debida protección de los datos personales.
D. Integrar de manera conjunta con los órganos administrativos del ICATECH los respectivos Avisos de Privacidad.
E. Realizar revisiones de monitoreo, verificación y seguimiento con el objetivo de corroborar el cumplimiento de las obligaciones que marca la ley.
F. Actualizar anualmente el Documento de Seguridad.
G. Actualizar anualmente el Inventario de Datos Personales; o bien, de acuerdo al apartado final del presente instrumento.
H. Fomentar las Reglas Generales del Tratamiento de los Datos Personales en el ICATECH.

REGLAS GENERALES DEL TRATAMIENTO DE LOS DATOS PERSONALES EN EL ICATECH.

Como parte del sistema de gestión y política de seguridad institucional, se enmarcan las reglas generales siguientes; mismas que deberán ser observadas por los órganos administrativos del ICATECH:

I. Informar a los titulares del tratamiento de los datos y sus finalidades;
II. Procurar que los datos personales tratados sean correctos y estén actualizados;
III. Respetar los derechos de los titulares en relación con sus datos personales;
IV. No obtener datos personales a través de medios fraudulentos;
V. Tratar estrictamente los datos personales necesarios, adecuados y relevantes en relación con las finalidades;
VI. Sujetar el tratamiento de los datos personales al principio de consentimiento, salvo las excepciones previstas por la Ley;
VII. Tratar los datos personales estrictamente para propósitos legales o legítimos;
VIII. Limitar el tratamiento de los datos personales al cumplimiento de las finalidades;
IX. Identificar el flujo y ciclo de vida de los datos personales;
X. Suprimir los datos personales cuando hayan dejado de ser necesarios para las finalidades para las cuales se obtuvieron;
XI. Identificar a los servidores públicos responsables del tratamiento de los datos personales.
XII. Respetar la expectativa razonable de privacidad del titular;
XIII. Establecer y mantener medidas de seguridad acordes a la capacidad y objetivos de cada área;
XIV. Guardar la confidencialidad de los datos personales;
XV. Mantener actualizado el inventario de datos, y;
XVI. Aplicar las excepciones contempladas en la normativa en materia de protección de datos personales.

Con base en lo anterior, se determinan las pautas de acción del personal encargado de tratamiento de datos personales con miras a generar su correcto resguardo, buscando en todo momento actuar en apego a los lineamientos de la materia, siempre en consideración de la salvaguarda del derecho a la privacidad y protección de datos de las personas, por lo que los órganos administrativos del ICATECH que dan tratamiento a datos personales son los responsables de controlar el acceso a sus bases de datos personales físicas o electrónicas, y de implementar las medidas de seguridad que salvaguarden la confidencialidad y la integridad de los mismos.

APARTADO FINAL

El presente documento de seguridad se actualizará cuando ocurran los siguientes eventos:

1. Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo.
2. Como resultado de un cambio de funciones al interior de los órganos administrativos involucrados.
3. Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión.
4. Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a l seguridad, e
5. Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.
6. Se realicen reformas o modificaciones a las leyes aplicables.