INSTITUTO DE CAPACITACIÓN EN ALTA TECNOLOGÍA DEL ESTADO DE BAJA CALIFORNIA

DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES

Contenido

I. Introducción.

En el presente documento se definen las medidas de seguridad administrativas, físicas y técnicas que posee el Instituto de Capacitación en Alta Tecnología para garantizar la debida protección de los datos personales a los que se les da tratamiento.

El deber de seguridad consiste en la implementación de medidas de seguridad físicas, técnicas y administrativas necesarias para proteger los datos personales contra daño, perdida, alteración, destrucción, o su uso, acceso o tratamiento no automatizado, así como para garantizar su confidencialidad, integridad y disponibilidad.

Las medidas de seguridad son el conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permiten proteger los datos personales.

Las medidas de ***seguridad administrativas*** refieren a las políticas y procedimientos para la gestión soporte y revisión 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.

Las medidas de ***seguridad físicas*** son el conjunto de acciones y mecanismo para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.

a) Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;
b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;
c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización y
d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

Así mismo, las medidas de ***seguridad técnicas*** abarcan el conjunto de acciones y mecanismo que valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento.

De conformidad con el artículo 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, el responsable deberá elaborar un documento de seguridad, el cual debe de contener, al menos, la siguiente información:

I. Inventario de datos personales y de los sistemas de tratamiento;
II. Las funciones y obligaciones de las personas que traten datos personales;
III. El análisis de riesgos;
IV. El análisis de brecha;
V. El plan de trabajo;
VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad, y
VII. El programa general de capacitación.

II. Objeto

Garantizar que los programas, servicios, sistemas o plataformas informáticas o cualquier otra tecnología que implique el tratamiento de datos personales, cumplan con las medidas de seguridad para la protección de datos personales y las obligaciones previstas en la Ley de Datos.

III. Inventario de datos personales y de los sistemas de tratamiento.

Obligación establecida en el artículo 16 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Baja California, en relación con el artículo 33 fracción III de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, en lo que se establece que, para proteger los datos personales, el responsable en este caso el ICAT, debe establecer y mantener medidas de seguridad de carácter administrativo, físico y técnico y que, para ello, debe realizar una serie de actividades interrelacionadas, entre las que se encuentran la de elaborar un inventario de datos personales y de los sistemas de tratamiento.

I. El Instituto de Capacitación en Alta Tecnología tiene elaborado los inventarios de datos personales (anexo1) de cada una de las unidades administrativas: Dirección General, Dirección de Administración, Dirección de Planeación, Dirección Técnico Académico y Dirección de Vinculación.

Los inventarios se componen de los siguientes apartados de datos personales:

a) **Datos de Identificación y contacto**: Nombre, estado civil, registro federal de Contribuyente (RFC), Clave Única de Registro de Población (CURP), Credencial de votar (INE), lugar de nacimiento, fecha de nacimiento, nacionalidad, domicilio, teléfono particular, teléfono celular, correo electrónico, firma autógrafa, firma electrónica, edad, fotografía, referencias personales.

b) **Datos sobre características físicas:** Color de piel, color de cabello, señas particulares, estatura, peso, cicatrices, tipo de sangre.

c) **Datos biométricos:** Imagen de iris, huella dactilar, palma de la mano.

d) **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.

e) **Datos personales recabados:** Experiencia/ capacitación laboral

f) **Datos académicos:** Trayectoria educativa, títulos, cedula profesional, certificados, reconocimientos.

En el anexo 1 de cada una de las unidades administrativas viene marcada la información de los datos personales que cada uno posee y que son necesarios para el cumplimiento de los objetivos de la institución.

II. De las personas que se obtienen los datos personales:

a) Personal que labora en el ICAT.

b) Personas externas que prestan algún servicio al ICAT.

c) Personas que se capacitan en el ICAT.

Los datos personales que se recaban son por medio de documentos presentado y/o por el llenado de formularios físicos y/o electrónicos por los titulares de los datos personales.

III. Funciones y obligaciones de las personas que traten los datos personales.

Las obligaciones comunes de todos los responsables de proteger los datos personales son:

- Conocer la privacidad de todos los datos que se manejan dentro del Instituto y, por lo tanto, su obligación de mantener el secreto de dicha información.
- Hacer uso de los datos únicamente para los fines para los cuales han sido recabados.

Las direcciones encargadas de tratar datos personales son las siguientes:

- Dirección General
- Dirección de Administración
- Dirección Técnico Académico
- Dirección de Vinculación
- Dirección de Planeación

El personal que desempeña los puestos anteriores tiene como funciones y obligaciones las siguientes:

1. Garantizar la seguridad en el tratamiento de datos personales, esto con la finalidad de evitar algún riesgo, como la pérdida, robo, alteración o acceso no autorizado.
2. Garantizar la debida protección de los datos personales, conforme a la Ley y las demás disposiciones aplicables en la materia.
3. Implementar medidas de seguridad físicas, técnicas y administrativas convenientes para el tratamiento diario de los datos personales.
4. Garantizar la confidencialidad de los datos personales derivada de los procedimientos que tienen a su cargo.
5. Conocer y aplicar las acciones derivadas de este documento de seguridad.

Se cuentan con bitácoras de responsables, encargados y usuarios de los Sistemas de Datos Personales el cual cuenta con la siguiente estructura:

Dirección General:

A. Unidad administrativa:	Dirección General
A1. Nombre del sistema:	Personas Capacitadas
Responsable:	
Nombre:	[redacted]
Cargo:	Directora General
Funciones:	1. Auxiliar y orientar con relación al ejercicio del derecho a la protección de datos personales. 2. Coordinar el seguimiento a las medidas de seguridad, para garantizar la integridad, disponibilidad y confidencialidad de la información. 3. Coordinar el seguimiento al inventario de Sistema de Datos personales 4. Coordinar el seguimiento al registro de incidencias. 5. Actualizar la bitácora de responsable, encargado y usuario. 6. Establecer un mecanismo que permita la identificación de forma inequívoca y personalizada de toda persona que intente acceder al Sistema (una de ellas presentando identificación). 7. Asignara claves y contraseñas al personal autorizado
Encargados	
Nombre:	[redacted]
Cargo:	Dirección de Planeación
Funciones:	1. Informar al responsable del Sistema sobre cualquier incidencia que tenga conocimiento. 2. Coordinar con la unidad administrativa las medidas de seguridad. 3. Reportar la vulneración de los datos personales para reforzar las medidas de seguridad. 4. Coordinar la actualización del documento de seguridad 5. Elaborar los análisis de riesgo y brecha.
Usuarios:	
Nombre:	[redacted]
Cargo:	Técnico superior
Funciones:	1. Conservar el buen estado físico de los soportes documentales que tenga acceso. 2. Reportar alguna vulneración de los datos personales, mediante el llenado del anexo 5 Registro de incidencias. 3. Dar seguimiento al llenado del Inventario de sistema de datos personales (anexo 4).

Dirección de Administración:

A. Unidad administrativa:	Dirección de administración
A1. Nombre del sistema:	Personal del ICAT y Proveedores
Responsable:	
Nombre:	[redacted]
Cargo:	Director de Administración
Funciones:	1. Auxiliar y orientar con relación al ejercicio del derecho a la protección de datos personales.

	2. Coordinar el seguimiento a las medidas de seguridad, para garantizar la integridad, disponibilidad y confidencialidad de la información. 3. Coordinar el seguimiento al inventario de Sistema de Datos personales 4. Coordinar el seguimiento al registro de incidencias. 5. Actualizar la bitácora de responsable, encargado y usuario. 6. Establecer un mecanismo que permita la identificación de forma inequívoca y personalizada de toda persona que intente acceder al Sistema (una de ellas presentando identificación). 7. Asignara claves y contraseñas al personal autorizado
Encargados	
Nombre:	[redacted]
Cargo:	Dirección de Planeación
Funciones:	1. Informar al responsable del Sistema sobre cualquier incidencia que tenga conocimiento. 2. Coordinar con la unidad administrativa las medidas de seguridad. 3. Reportar la vulneración de los datos personales para reforzar las medidas de seguridad. 4. Coordinar la actualización del documento de seguridad 5. Elaborar los análisis de riesgo y brecha.
Usuarios:	
Nombre:	[redacted]
Cargo:	Especialista en teleinformática
Funciones:	1. Conservar el buen estado físico de los soportes documentales que tenga acceso. 2. Reportar alguna vulneración de los datos personales, mediante el llenado del anexo 5 Registro de incidencias. 3. Dar seguimiento al llenado del Inventario de sistema de datos personales (anexo 4).

Dirección de Vinculación:

A. Unidad administrativa:	Dirección de Vinculación
A1. Nombre del sistema:	Convenios y estadística de egresados
Responsable:	
Nombre:	[redacted]
Cargo:	Director de Vinculación
Funciones:	1. Auxiliar y orientar con relación al ejercicio del derecho a la protección de datos personales. 2. Coordinar el seguimiento a las medidas de seguridad, para garantizar la integridad, disponibilidad y confidencialidad de la información. 3. Coordinar el seguimiento al inventario de Sistema de Datos personales 4. Coordinar el seguimiento al registro de incidencias. 5. Actualizar la bitácora de responsable, encargado y usuario. 6. Establecer un mecanismo que permita la identificación de forma inequívoca y personalizada de toda persona que intente acceder al Sistema (una de ellas presentando identificación). 7. Asignara claves y contraseñas al personal autorizado

Encargados	
Nombre:	[redacted]
Cargo:	Dirección de Planeación
Funciones:	1. Informar al responsable del Sistema sobre cualquier incidencia que tenga conocimiento. 2. Coordinar con la unidad administrativa las medidas de seguridad. 3. Reportar la vulneración de los datos personales para reforzar las medidas de seguridad. 4. Coordinar la actualización del documento de seguridad 5. Elaborar los análisis de riesgo y brecha.
Usuarios:	
Nombre:	[redacted]
Cargo:	Secretaria Ejecutiva C
Funciones:	1. Conservar el buen estado físico de los soportes documentales que tenga acceso. 2. Reportar alguna vulneración de los datos personales, mediante el llenado del anexo 5 Registro de incidencias. 3. Dar seguimiento al llenado del Inventario de sistema de datos personales (anexo 4).

Dirección de Planeación:

A. Unidad administrativa:	Dirección de Planeación
A1. Nombre del sistema:	Estadística personas capacitadas
Responsable:	
Nombre:	[redacted]
Cargo:	Directora de Planeación
Funciones:	1. Auxiliar y orientar con relación al ejercicio del derecho a la protección de datos personales. 2. Coordinar el seguimiento a las medidas de seguridad, para garantizar la integridad, disponibilidad y confidencialidad de la información. 3. Coordinar el seguimiento al inventario de Sistema de Datos personales 4. Coordinar el seguimiento al registro de incidencias. 5. Actualizar la bitácora de responsable, encargado y usuario. 6. Establecer un mecanismo que permita la identificación de forma inequívoca y personalizada de toda persona que intente acceder al Sistema (una de ellas presentando identificación). 7. Asignara claves y contraseñas al personal autorizado
Encargados	
Nombre:	[redacted]
Cargo:	Dirección de Planeación
Funciones:	1. Informar al responsable del Sistema sobre cualquier incidencia que tenga conocimiento. 2. Coordinar con la unidad administrativa las medidas de seguridad. 3. Reportar la vulneración de los datos personales para reforzar las medidas de seguridad. 4. Coordinar la actualización del documento de seguridad 5. Elaborar los análisis de riesgo y brecha.

Usuarios:	
Nombre:	[redacted]
Cargo:	Secretaria Ejecutiva C
Funciones:	1. Conservar el buen estado físico de los soportes documentales que tenga acceso. 2. Reportar alguna vulneración de los datos personales, mediante el llenado del anexo 5 Registro de incidencias. 3. Dar seguimiento al llenado del Inventario de sistema de datos personales (anexo 4).

Dirección de Técnico Académico:

A. Unidad administrativa:	Dirección Técnico Académico
A1. Nombre del sistema:	Cursos y elaboración de constancias
Responsable:	
Nombre:	[redacted]
Cargo:	Directora Técnico Académica
Funciones:	1. Auxiliar y orientar con relación al ejercicio del derecho a la protección de datos personales. 2. Coordinar el seguimiento a las medidas de seguridad, para garantizar la integridad, disponibilidad y confidencialidad de la información. 3. Coordinar el seguimiento al inventario de Sistema de Datos personales 4. Coordinar el seguimiento al registro de incidencias. 5. Actualizar la bitácora de responsable, encargado y usuario. 6. Establecer un mecanismo que permita la identificación de forma inequívoca y personalizada de toda persona que intente acceder al Sistema (una de ellas presentando identificación). 7. Asignara claves y contraseñas al personal autorizado
Encargados	
Nombre:	[redacted]
Cargo:	Dirección de Planeación
Funciones:	1. Informar al responsable del Sistema sobre cualquier incidencia que tenga conocimiento. 2. Coordinar con la unidad administrativa las medidas de seguridad. 3. Reportar la vulneración de los datos personales para reforzar las medidas de seguridad. 4. Coordinar la actualización del documento de seguridad 5. Elaborar los análisis de riesgo y brecha.
Usuarios:	
Nombre:	[redacted]
Cargo:	Secretaria Ejecutiva B
Funciones:	1. Conservar el buen estado físico de los soportes documentales que tenga acceso. 2. Reportar alguna vulneración de los datos personales, mediante el llenado del anexo 5 Registro de incidencias. 3. Dar seguimiento al llenado del Inventario de sistema de datos personales (anexo 4).

IV. Análisis de riesgo

El análisis de riesgo de los datos personales se realizó considerando amenazas y vulnerabilidades existentes para los datos personales y recursos involucrados en su tratamiento, como pueden ser: hardware, software, personal responsable quienes tienen acceso a los datos personales, entre otras.

Se anexa el formato donde se detectan las situaciones de riesgo dentro de la entidad:

Anexo 2 Análisis de Riesgo				
Amenazas, vulnerabilidades y recursos involucrados				
Código	**Pregunta o Control**	**¿Existe? Si**	**¿Existe? No**	**Observaciones (acciones a realizar en caso de no contar con:**
1. Amenazas				
1.1	¿Tienes identificados los datos personales?	X		
1.2	¿Tienes clasificados los datos personales?	X		
1.3	¿Tienes establecido el ciclo de vida de los datos personales?	X		
1.4	¿Tienes definido el tratamiento que se le da a cada uno de los datos personales?	X		
1.5	¿Tienes capacitaciones sobre qué hacer en caso de que los datos personales queden expuestos?	X		
1.6	¿Tienes un catálogo sobre las consecuencias negativas para los titulares de los datos personales?		X	Se deberá elaborar catalogo con las consecuencias negativas para los titulares de los datos personales y así poder socializarlo con el personal.
1.7	¿Tienes un plan reactivo en caso de sufrir la pérdida de datos personales?		X	Se deberá de elaborar un plan reactivo en caso de sufrir la perdida de datos personales.
1.8	¿Tienes una bitácora de las causas que originaron el daño al sistema y por ende a los datos personales?	X		
1.9	¿Tienes registro de las amenazas surgidas durante la implementación, puesta en marcha y desarrollo del sistema, el cual contiene datos personales?	X		
1.10	¿Tienes contemplado el riesgo inherente al tipo de dato personal vulnerado?	X		

2. Vulneraciones				
2.1	¿Tienes una bitácora sobre vulneraciones sufridas en los datos personales?	X		
2.2	¿Tienes requerimientos regulatorios en caso de vulneración de los datos personales?		X	Se deberán establecer requerimientos regulatorios en caso de vulneraciones de los datos personales.
2.3	¿Tienes una política a seguir en caso de daño al sistema por una vulneración de los datos personales?	X		
2.4	¿Tienes códigos de conducta del personal que trata los datos personales?	X		
2.5	¿Tienes un sistema de todas y cada una de las consecuencias que surgieron a raíz de la vulneración del sistema que contiene datos personales?	X		
2.6	¿Tienes procedimientos para actuar ante la vulneración de los sistemas de datos personales?	X		
3. Recursos involucrados				
3.1	¿Tienes respaldos en el caso de que la información fue vulnerada?	X		
3.2	¿Tienes hardware y software para respaldar los datos personales?	X		
3.3	¿Tienes personal capacitado para llevar a cabo los respaldos hardware y software que contendrán los datos personales?	X		
3.4	¿Tienes calendario, con fechas para dar servicio y mantenimiento a los sistemas, computadoras, discos duros, hardware y software en los que se almacenan datos personales?	X		
3.5	¿Tienes asesoría externa para dar servicio y mantenimiento a los sistemas, computadoras, discos duros, hardware y software en los que se almacenan datos personales?	X		

V. Análisis de brecha

El análisis de brecha se realizó como un proceso de evaluación de las medidas de seguridad que ya existen en la organización contra las que seria conveniente tener, que resultan

necesaria para la protección de Datos Personales.

Con la realización del cuestionario se concluyó que, actualmente, se tiene cuenta con un nivel de seguridad óptimo en relación con los datos personales que se manejan dentro de la institución.

Con respecto con las medidas que falta atender, estas se trabajaran dentro del Plan de trabajo.

Anexo 3 Análisis de brecha Medidas de seguridad existentes y medidas de seguridad faltantes				
Código	**Pregunta o Control**	**¿Existe? Si**	**¿Existe? No**	**Observaciones (acciones a realizar en caso de no contar con:**
1. Medidas de seguridad basadas en la cultura del personal				
1.1	¿Pones atención en no dejar a la vista información personal y llevas registro de su manejo?	X		
1.1.1	Política de escritorio limpio	X		
1.1.2	Hábitos de cierre y resguardo	X		
1.1.3	Impresoras, escáneres, copiadoras y buzones limpios	X		
1.1.4	Gestión de bitácoras usuarios y accesos	X		
2.1	¿Tienes mecanismos para eliminar de manera segura la información?	X		
2.2	Destrucción segura de documentos	X		
2.3	Eliminación segura de información en equipo de cómputo y medios de almacenamiento electrónico	X		
2.4	Fijar periodos de retención y destrucción de información	X		
2.5	Tomar precauciones con los procedimientos de re-utilización	X		
2.6	¿Has establecido y documentado los compromisos respecto a la protección de datos?	X		
3.- Medidas de seguridad basadas en la cultura del personal				

3.1	Informar al personal sobre sus deberes mínimos de seguridad y protección de datos	X		
3.2	Fomentar la cultura de la seguridad de la información	X		
3.3	Difundir noticias en temas de seguridad	X		
3.4	Prevenir al personal sobre los crímenes cibernéticos	X		
3.5	Asegurar la protección de datos personales en subcontrataciones		X	El Instituto no subcontrate a terceros para el manejo de datos personales.
4	¿Tienes procedimientos para actuar ante la vulneración de los sistemas de datos personales?		X	Se deberán de elaborar procedimientos para actuar ante vulneraciones de los sistemas de datos personales
4.1	Tener un procedimiento de notificación	X		
4.2	Realizar revisiones y auditorias	X		
5	¿Realizas respaldos periódicos de los datos personales?	X		
6.- Medidas de seguridad en el entorno de trabajo físico				
6.1	¿Tienes medidas de seguridad para acceder al entorno de trabajo físico	X		
6.1.1	Alerta del entorno de trabajo	X		
6.1.2	Mantener registros del personal con acceso al entorno de trabajo	X		
6.2.1	¿Tienes medidas de seguridad para evitar el robo?	X		
6.2.2	Cerraduras y candados	X		
6.2.3	Minimizar el riesgo oportunista	X		
6.3	¿Cuidas el movimiento de información en entornos de trabajo físicos?	X		
6.3.1	Aprobación de salida de documentos, equipo de cómputo y/o medios de almacenamiento electrónico	X		
6.3.2	Mantener en movimiento sólo copias de la información, no el elemento original	X		
6.3.3	Usar mensajería certificada	X		
7.- Medidas de seguridad en el entorno de trabajo digital				

7.1	¿Realizas actualizaciones del equipo de cómputo?	X		
7.2	¿Revisas periódicamente el software instalado en el equipo de cómputo?	X		
7.3	¿Tienes medidas de seguridad para acceder al entorno de trabajo electrónico?	X		
7.3.1	Uso de contraseñas y/o cifrado	X		
7.3.2	Uso de contraseñas solidas	X		
7.3.3	Bloqueo y cierre de sesiones	X		
7.3.4	Administrar usuarios y accesos	X		
7.4	¿Revisas la configuración de seguridad del equipo de cómputo?	X		
7.5	¿Tienes medidas de seguridad para navegar en entornos digitales?	X		
7.5.1	Instalar herramientas antimalware y de filtrado de tráfico	X		
7.5.2	Reglas de navegación	X		
7.5.3	Reglas de divulgación de información	X		
7.5.4	Uso de conexiones seguras	X		
7.6	¿Cuidas el movimiento de información en entornos de trabajo digitales?	X		
7.6.1	Seguridad de la información enviada y recibida	X		

VII. Plan de trabajo

El plan de trabajo se elaboró en base a los resultados obtenidos del análisis de riesgo y análisis de brecha contenidos en los anexos 2 y 3, priorizando las medidas de seguridad más relevantes e inmediatas.

Por lo que se elabora respecto de los faltantes de análisis de riesgo y brecha:

1. Elaborar catalogo con las consecuencias negativas para los titulares de los datos

personales y así poder socializarlo con el personal.

2. Elaborar un plan reactivo en caso de sufrir la perdida de datos personales.
3. Establecer requerimientos regulatorios en caso de vulneraciones de los datos personales.
4. Revisar si es factible la realización de un contrato donde se subcontrate a terceros para el manejo de datos personales.
5. Elaborar procedimientos para actuar ante vulneraciones de los sistemas de datos personales.

Por lo anterior el plan de trabajo a parte de reforzar las medidas con las que ya cuenta el Instituto de Capacitación en Alta Tecnología, se atenderán las ya descritas durante el ejercicio fiscal.

VIII. Mecanismos de monitoreo y revisión de las medidas de seguridad

El ICAT monitorea y revisa de manera periódica las medidas de seguridad implementadas, en las cuales se consideran las amenazas y vulneraciones a las que están sujetos los datos personales, para lo cual se consideran los siguientes elementos:

1. Los nuevos activos que se incluyan en la gestión de riesgos.
2. Las modificaciones necesarias a los activos, como podrían ser el cambio o migración tecnológica.
3. Las nuevas amenazas que se pudieran activar dentro y fuera del ICAT y que no fuesen sido valoradas en la matriz de riesgo.
4. Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir.
5. Los incidentes y vulneraciones de seguridad ocurridas.

Las medidas de seguridad administrativa, físicas y técnicas son de aplicación a todas las bases de datos personales que manejan las personas a cargo de las 5 direcciones. Con la bitácora de responsables, encargados y usuarios se mantiene actualizado el Sistema de Protección de Datos, de igual manera con la identificación personalizada del personal que tenga acceso al Sistema de datos. Por otro lado, se toman medidas de seguridad en el acceso de personas a las áreas de trabajo como son las instalaciones, así como al interior medidas que se llevan a cabo para controlar el acceso a los espacios donde se almacena los soportes físicos o electrónicos del sistema.

Dentro de las acciones más relevantes para este Instituto son mantener actualizadas:

1. Política de seguridad
2. Cumplimiento de la normatividad
3. Organización de la seguridad en la información
4. Clasificación e identificación de inventarios
5. Administración de incidentes
6. Adquisición, desarrollo, uso y mantenimiento del sistema de información
7. Soportes físicos
8. Soportes electrónicos

Para el caso en específico de vulneraciones, se cuenta con el anexo 5 “Registro de Incidencia” en el cual en base al monitoreo se registran las incidencias que se pudieran presentar, a las cuales el área responsable de protección de datos le da el seguimiento pertinente para reforzar las medidas de seguridad.

IX. Programa de capacitación

La persona responsable de Protección de Datos (dirección de Planeación) diseñará y aplicará diferentes niveles de capacitación al personal del ICAT dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales, seguridad de los datos personales y el perfil de los puestos.

En los cursos se difunden los conceptos e importancia de la seguridad de la información para desarrollar la cultura en seguridad de la información, por ello la importancia de concientizar de la protección de datos personales y su importancia en el entorno laboral; así como las funciones y responsabilidades en el tratamiento y seguridad de los datos personales.

La capacitación será una vez al año, y se programa en el primer trimestre del año, esto durante el periodo que se realiza el Informe Anual de acciones en materia de protección de datos personales por parte del Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Baja California. Así mismo una vez que se presente alguna modificación a la ley, surja alguna actualización en el tema o alguna de las unidades administrativas tengan necesidad de capacitación.

Dentro de los temas primordiales a capacitar están:

1. Los requerimientos y actualización del Sistema de gestión
2. La legislación vigente en materia de protección de datos personales y las mejores practicas relacionadas con el tratamiento de estos.
3. Las consecuencias de incumplimiento de los requerimientos legales o requisitos organizacionales.
4. Las herramientas tecnológicas relacionadas o utilizadas para el tratamiento de los datos personales y para la implementación de las medidas de seguridad.

Por su parte la persona responsable de Protección de Datos se capacitará constantemente por medio de talleres ya sean presenciales o en línea por parte del Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Baja California (ITAIP).

X. Actualización del documento de seguridad.

La actualización del documento de seguridad se deberá de realizar cuando ocurran los siguientes eventos:

a) Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo.
b) Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión.
c) Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida.
d) Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

XI. Anexos

Anexo 1
Inventario de datos personales
Dirección de Administración

Datos personales recabados	Existente	Necesario	No necesario
Datos de identificación y contacto			
Nombre	X	X	
Estado Civil	X	X	
Registro Federal de Contribuyentes (RFC)	X	X	
Clave Única de Registro de Población (CURP)	X	X	
Lugar de nacimiento	X	X	
Fecha de nacimiento	X	X	
Nacionalidad	X	X	
Domicilio	X	X	
Teléfono particular	X	X	
Teléfono celular	X	X	
Correo electrónico	X	X	
Firma autógrafa	X	X	
Firma electrónica			
Edad	X	X	
Fotografía	X	X	
Referencias personales	X	X	
Datos sobre características físicas			
Color de piel			
Color de cabello			
Señas particulares			
Estatura			
Peso			
Cicatrices			
Tipo de sangre			
Datos biométricos			
Imagen de iris			
Huella dactilar			
Palma de la mano			
Datos laborales			
Puesto o cargo que desempeña	X	X	
Domicilio de trabajo	X	X	
Correo electrónico institucional	X	X	
Teléfono institucional	X	X	
Referencias laborales	X	X	
Información generada durante los procedimientos de reclutamiento, selección y contratación	X	X	
Datos personales recabados			
Experiencia/ Capacitación laboral	X	X	
Datos académicos			
Trayectoria educativa	X	X	
Títulos	X	X	
Cedula profesional	X	X	
Certificados			
Reconocimientos			

Anexo 1
Inventario de datos personales
Dirección de Planeación

Datos personales recabados	Existente	Necesario	No necesario
Datos de identificación y contacto			
Nombre	X		
Estado Civil	X		
Registro Federal de Contribuyentes (RFC)			
Clave Única de Registro de Población (CURP)	X	X	
Credencial para votar INE	X		
Lugar de nacimiento	X		
Fecha de nacimiento	X		
Nacionalidad	X		
Domicilio	X		
Teléfono particular			
Teléfono celular	X		
Correo electrónico	X		
Firma autógrafa			
Firma electrónica			
Edad	X	X	
Fotografía			
Referencias personales			
Datos sobre características físicas			
Color de piel			
Color de cabello			
Señas particulares			
Estatura			
Peso			
Cicatrices			
Tipo de sangre			
Datos biométricos			
Imagen de iris			
Huella dactilar			
Palma de la mano			
Datos laborales			
Puesto o cargo que desempeña			
Domicilio de trabajo	X		
Correo electrónico institucional	X		
Teléfono institucional			
Referencias laborales			
Información generada durante los procedimientos de reclutamiento, selección y contratación			
Datos personales recabados			
Experiencia/ Capacitación laboral			
Datos académicos			
Trayectoria educativa	X	X	
Títulos			
Cedula profesional			
Certificados			
Reconocimientos			

Anexo 1
Inventario de datos personales
Dirección General

Datos personales recabados	Existente	Necesario	No necesario
Datos de identificación y contacto			
Nombre	X		
Estado Civil	X		
Registro Federal de Contribuyentes (RFC)	X		
Clave Única de Registro de Población (CURP)	X		
Credencial para votar INE	X		
Lugar de nacimiento	X		
Fecha de nacimiento	X		
Nacionalidad	X		
Domicilio	X		
Teléfono particular	X		
Teléfono celular	X		
Correo electrónico	X		
Firma autógrafa			
Firma electrónica			
Edad	X		
Fotografía	X		
Referencias personales	X		
Datos sobre características físicas			
Color de piel			
Color de cabello			
Señas particulares			
Estatura			
Peso			
Cicatrices			
Tipo de sangre			
Datos biométricos			
Imagen de iris			
Huella dactilar			
Palma de la mano			
Datos laborales			
Puesto o cargo que desempeña			
Domicilio de trabajo	X		
Correo electrónico institucional	X		
Teléfono institucional	X		
Referencias laborales	X		
Información generada durante los procedimientos de reclutamiento, selección y contratación	X		
Datos personales recabados			
Experiencia/ Capacitación laboral	X		
Datos académicos			
Trayectoria educativa	X		
Títulos	X		
Cedula profesional	X		
Certificados			

Reconocimientos			

Anexo 1
Inventario de datos personales
Dirección Técnico Académico

Datos personales recabados	Existente	Necesario	No necesario
Datos de identificación y contacto			
Nombre	X	X	
Estado Civil	X	X	
Registro Federal de Contribuyentes (RFC)			
Clave Única de Registro de Población (CURP)	X	X	
Credencial para votar INE	X	X	
Lugar de nacimiento	X	X	
Fecha de nacimiento	X	X	
Nacionalidad	X	X	
Domicilio	X	X	
Teléfono particular			
Teléfono celular	X	X	
Correo electrónico	X	X	
Firma autógrafa			
Firma electrónica			
Edad	X	X	
Fotografía			
Referencias personales			
Datos sobre características físicas			
Color de piel			
Color de cabello			
Señas particulares			
Estatura			
Peso			
Cicatrices			
Tipo de sangre			
Datos biométricos			
Imagen de iris			
Huella dactilar			
Palma de la mano			
Datos laborales			
Puesto o cargo que desempeña			
Domicilio de trabajo	X	X	
Correo electrónico institucional	X	X	
Teléfono institucional			
Referencias laborales			
Información generada durante los procedimientos de reclutamiento, selección y contratación			
Datos personales recabados			
Experiencia/ Capacitación laboral			
Datos académicos			
Trayectoria educativa	X	X	
Títulos	X	X	
Cedula profesional	X	X	

Certificados	X	X	
Reconocimientos	X	X	

Anexo 1
Inventario de datos personales
Dirección de Vinculación

Datos personales recabados	Existente	Necesario	No necesario
Datos de identificación y contacto			
Nombre	X	X	
Estado Civil	X		
Registro Federal de Contribuyentes (RFC)	X		
Clave Única de Registro de Población (CURP)	X	X	
Credencial para votar INE	X		
Lugar de nacimiento	X		
Fecha de nacimiento	X		
Nacionalidad	X	X	
Domicilio	X	X	
Teléfono particular	X	X	
Teléfono celular	X		
Correo electrónico	X	X	
Firma autógrafa			
Firma electrónica			
Edad	X	X	
Fotografía	X		
Referencias personales	X		
Datos sobre características físicas			
Color de piel			
Color de cabello			
Señas particulares			
Estatura			
Peso			
Cicatrices			
Tipo de sangre			
Datos biométricos			
Imagen de iris			
Huella dactilar			
Palma de la mano			
Datos laborales			
Puesto o cargo que desempeña			
Domicilio de trabajo	X		
Correo electrónico institucional	X		
Teléfono institucional	X		
Referencias laborales	X		
Información generada durante los procedimientos de reclutamiento, selección y contratación	X		
Datos personales recabados			
Experiencia/ Capacitación laboral	X		
Datos académicos			
Trayectoria educativa	X	X	

Títulos	X		
Cedula profesional	X		
Certificados			
Reconocimientos			

Anexo 4

INVENTARIO DE SISTEMA DE DATOS PERSONALES

Sección I.
Identificación del Sistema de datos personales:

1. *Nombre del responsable (sujeto obligado)	
Instituto de Capacitación en Alta Tecnología del Estado de Baja California	
2. *Unidad administrativa Es posible que distintas áreas tengan injerencia en un mismo sistema de datos, por lo que es necesario identificar a la unidad administrativa que está a cargo de este proceso y que, por tanto, sea la administradora del sistema de datos personales y de los archivos que se generen.	
Dirección Técnico Académica, Dirección de Administración y Dirección de Planeación	
3. *Nombre del sistema de datos personales **Capacitados, personal del ICAT, proveedores, estadísticas y convenios**	
4. *Fecha de elaboración o última actualización →	**15 agosto 2024**

Sección II.

Fundamento legal para llevar a cabo el tratamiento:

5. *Fundamento jurídico que habilita el tratamiento de datos Anotar el nombre de la ley, tratado internacional o acuerdo, etc. que sustenta el tratamiento de datos personales, incluyendo los artículos, apartados, fracciones e incisos, y precisando su fecha de publicación o, en su caso, la fecha de la última modificación o reforma.
Ley Federal de Protección de Datos Personales, art. 6 y 7 publicación 5 de julio 2010.
6. *Atribuciones de la unidad administrativa para realizar el tratamiento de datos Registrar las atribuciones con que cuenta la unidad administrativa para realizar el tratamiento de datos personales, anotando el nombre de su Reglamento o Estatuto Orgánico Interno, incluyendo sus respectivos artículos, apartados, fracciones e incisos y, precisando su fecha de publicación o, en su caso, la fecha de la última modificación o reforma.
Reglamento Interno art 22: Tramitar la certificación y acreditamiento de la capacitación que realizan las Unidades administrativas del ICAT; Tramitar las acreditaciones y certificaciones correspondientes ante la Secretaría de Educación Pública.

Sección III.

Obtención de los datos personales:

7. *Medio de obtención de los datos personales Señalar el o los medios a través de los cuales se obtienen los datos personales en este tratamiento (directamente del titular, con su presencia física en las oficinas del sujeto obligado, por escrito, por medio de un formato, por correo

electrónico, por transferencia, a través de una aplicación tecnológica, por teléfono, de una fuente de acceso público, etc.).
Se obtienen directamente del titular por medio de un formato electrónico de inscripción en donde se adjuntan identificación oficial o CURP

8. Tercero que transfiere los datos personales, en su caso Si en el numeral anterior se indicó que se reciben datos personales por transferencia, señalar el nombre del tercero o terceros que realizan la transferencia.	9. Finalidades de la transferencia recibida, en su caso Señalar para qué finalidades se realiza dicha transferencia, por cada tercero que remite los datos.
n/a	**n/a**

10. Fuente de acceso público de la que se obtienen los datos personales, en su caso Si en el numeral 7 se indicó que se obtienen datos personales de una fuente de acceso público, señalar el nombre de la fuente, cuando ello sea posible, o bien, el tipo de fuente, por ejemplo: medios de comunicación en línea.
n/a
11. *Listado de datos personales, señalando los que sean sensibles, en su caso. Enlistar los datos personales que se recaban en este sistema; de recabar datos sensibles, anotar tal situación. ejemplo: 1. nombre; 2. origen racial – sensible.
Nombre, CURP, correo electrónico, edad, escolaridad, domicilio, teléfono, RFC, estado civil, nombre de la empresa.

Sección IV.
Nivel de riesgo de los datos personales

12. *Nivel de riesgo de los datos personales
Señalar el o los niveles de riesgo inherente, dependiendo de los tipos o categorías de datos tratados en este sistema.

☒**Nivel estándar**	☐**Nivel sensible**	☐**Nivel especial**
Categorías de datos personales: identificativos, de contacto, laborales y académicos. Tipos de datos: nombre, teléfono, edad, sexo, RFC, CURP, estado civil, correo electrónico, lugar y fecha de nacimiento, nacionalidad, puesto y lugar de trabajo, experiencia laboral, datos de contacto laborales, idioma o lengua, escolaridad, trayectoria educativa, títulos, certificados, cédula profesional, entre otros.	Categorías de datos personales: datos de tránsito y movimientos migratorios, patrimoniales, de autenticación, biométricos y jurídicos. Tipos de datos: ubicación física, información relativa al tránsito dentro y fuera del país, saldos bancarios, estados y/o números de cuenta, cuentas de inversión, bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos, egresos, buró de crédito, seguros, afores, fianzas, número de tarjeta bancaria (crédito y débito), usuarios, contraseñas, huellas dactilares, iris, voz, firma autógrafa, firma electrónica, antecedentes penales, amparos, demandas, contratos, litigios, información de una persona relativa a un proceso administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal o administrativa, origen racial o étnico, estado de salud pasado, presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opinión política, preferencias o hábitos sexuales,	Categorías de datos personales: datos adicionales de autenticación, y datos de titulares de alto riesgo Tipos de datos: número de tarjeta bancaria en combinación con cualquier otro, contenido en la misma, como la fecha de vencimiento, el código de seguridad, el número de identificación personal (PIN) o los datos de banda ancha, profesión, oficio de personas que por su condición están mayormente expuestos a un ataque (ej. líderes políticos, religiosos, empresarios, etc.), entre otros.

	entre otros que pudieran causar discriminación o un riesgo grave al titular.	

Sección V.

Formato y ubicación de la base de datos y plazo de conservación de los datos personales:

13. *Formato de la base de datos Señalar el o los formatos en los que se encuentra la base de datos del tratamiento.				**14. *Ubicación de la base de datos** Señalar la ubicación de la base de datos (ej. equipo de cómputo, archivero físico de la unidad administrativa, archivo de trámite, archivo de concentración, etc.).
☒ **Físico**	☒**Electrónico**	☒**Nube**	**Otro:**	
15. *Fondo	**16. *Sección de archivos**		**17. *Serie de archivos**	**18. Subserie de archivos**
Indicar según su cuadro general de clasificación archivística.				
19. *Plazo de conservación Señalar el plazo de conservación de los datos personales, según los instrumentos de clasificación archivística. →				5 años o cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados.

Sección VI.

Finalidades del tratamiento y obtención del consentimiento:

20. *Finalidades del tratamiento Anotar cada una de las finalidades para las cuales se tratan los datos personales; las finalidades deben ser explícitas y concretas, relacionadas con las atribuciones de la unidad administrativa.	**21. *Consentimiento** Por cada finalidad, señalar si se requiere o no el consentimiento del titular (si / no).	**22. Excepciones del consentimiento** En caso de que la finalidad no requiera el consentimiento del titular, señalar el o los supuestos del artículo 11 de la LPDPPSOBC que se actualizan.	**23. Tipo de consentimiento** En caso de que la finalidad requiera el consentimiento, señalar si este es de tipo tácito, expreso o expreso por escrito.
Inscripción a curso de capacitación, generación de constancia con validez oficial, estadística	No	Se entenderá que el titular consiente tácitamente el tratamiento de sus datos cuando habiéndose puesto a su disposición el aviso de privacidad, no manifieste su oposición.	Tácito

Sección VII.

Personas que intervienen en el tratamiento de datos personales:

24. *Servidores públicos que tienen acceso a la base de datos	**25. *Privilegios del servidor público respecto de la base de datos**

Señalar los nombres o cargos de los servidores públicos que tienen acceso a la base de datos del tratamiento correspondiente.	Señale con qué fin o fines tiene acceso cada servidor público: O - Obtención, U - Uso, D - Divulgación, A - Almacenamiento, B - Bloqueo, C - Cancelación.
[redacted]	Obtención, uso, almacenamiento, bloqueo y cancelación
26. Nombre del encargado, en su caso Señalar el nombre de la o las personas físicas o morales que actúan como encargados en el tratamiento, en su caso.	**27. Número de contrato o convenio con el encargado** Señalar el número de identificación del instrumento jurídico que regula la relación con el encargado.
[redacted]	n/a

Sección VIII.

Información sobre transferencias:

28. *Señalar si se realizan o no transferencias en el marco del tratamiento		**☐ Si ☒ No**	
29. Tercero al que se transfieren los datos personales, en su caso En su caso y, cuando ello sea posible, señalar el nombre, razón o denominación social de los terceros a los que se transfieren los datos personales, o bien, su categoría, por ejemplo: Ministerio Público.	**30. Finalidades de la transferencia** Señalar las finalidades para las cuales se transfieren los datos personales por cada uno de los terceros.	**31. Consentimiento** Señalar si la transferencia requiere o no el consentimiento (si / no).	**32. Excepción del consentimiento** En caso de que la transferencia no requiera consentimiento, señalar los supuestos de los artículos 11 o 37 de la LPDPPSOBC que se actualizan.
N/a	N/a	N/a	N/a
33. Tipo de consentimiento En caso de que la finalidad de la transferencia requiera el consentimiento, señalar si este es de tipo tácito, expreso o expreso por escrito.	**34. Cláusulas contractuales para realizar la transferencia** Indicar si la transferencia requiere o no la suscripción de cláusulas contractuales, convenios de colaboración u otro instrumento jurídico, según el artículo 66 de la LGPDPPSO (si / no).	**35. Excepción de las cláusulas contractuales** Señalar el supuesto del artículo 66 LGPDPPSO que en su caso se actualiza, si no se requiere de la suscripción de cláusulas contractuales, convenios de colaboración u otro instrumento jurídico para realizar la transferencia.	
N/a	N/a	N/a	

Sección IX.

Difusión de los datos personales:

36. *Difusión de los datos personales Indicar si en el tratamiento se realiza la difusión de los datos personales.	**37. Fundamento jurídico para la difusión** Indicar el fundamento jurídico que justifica la difusión de los datos personales.
☐ Si ☒ No	

Sección X.

Aviso de privacidad del sistema de datos personales:

38. *Aviso de privacidad integral Señalar si el sistema de datos personales cuenta con el aviso de privacidad en modalidad integral.	**39. *Aviso de privacidad simplificado** Señalar si el sistema de datos personales cuenta con el aviso de privacidad en modalidad simplificada.

☐ Si ☐ No	☒ Si ☐ No
40. *Hipervínculo al aviso de privacidad integral Colocar el hipervínculo del aviso de privacidad integral, publicado permanentemente en el portal de internet del Sujeto Obligado. →	https://drive.google.com/file/d/1N7n6whwh48iNBmZJJlP4T7v50SITG37W/edit http://www.icatbc.gob.mx/

Anexo 5
Registro de incidencias

Fecha de la incidencia:	Número de incidencia:
Tipo de incidencia	
Descripción detallada de la incidencia:	
Nombre y cargo de la persona que registra la incidencia:	
Nombre y cargo de la persona a quien se le comunica la incidencia:	
Consecuencias de la incidencia:	

_____ _____

Nombre y firma de quien registra la incidencia

Nombre y firma de a quien se le comunico la incidencia