



Educación
Secretaría de Educación Pública



GOBIERNO DEL
ESTADO DE
CHIAPAS
2024 - 2030



TECNOLÓGICO
NACIONAL DE MÉXICO®



**INSTITUTO
TECNOLÓGICO
SUPERIOR
DE CINTALAPA**
GOBIERNO DE CHIAPAS
2024 - 2030

DOCUMENTO DE SEGURIDAD DEL INSTITUTO TECNOLÓGICO SUPERIOR DE CINTALAPA. (VERSIÓN PÚBLICA)

ÍNDICE

❖ INTRODUCCIÓN	2
❖ OBJETIVO DEL DOCUMENTO DE SEGURIDAD.....	3
❖ I. CONCEPTOS BÁSICOS EN LA MATERIA.....	5
❖ DEPARTAMENTO DE CONTROL ESCOLAR.....	8
❖ DEPARTAMENTO DE POSGRADO E INVESTIGACIÓN	29
❖ DEPARTAMENTO DE CIENCIAS BÁSICAS	40
❖ DIVISIÓN DE INGENIERÍA EN DESARROLLO COMUNITARIO	47
❖ DIVISIÓN DE INGENIERÍA CIVIL.....	55
❖ DIVISIÓN DE INGENIERÍA EN ENERGÍAS RENOVABLES	63
❖ DIVISIÓN DE INGENIERÍA INDUSTRIAL	71
❖ DIVISIÓN DE INGENIERÍA EN INDUSTRIAS ALIMENTARIAS	80
❖ DIVISIÓN DE INGENIERÍA INFORMÁTICA.....	90
❖ DEPARTAMENTO DE PERSONAL	98
❖ DEPARTAMENTO DE DIFUSIÓN Y CONCERTACIÓN	111
❖ DEPARTAMENTO DE RECURSOS FINANCIEROS	120
❖ DEPARTAMENTO DE RECURSOS MATERIALES Y SERVICIOS.....	134
❖ DEPARTAMENTO DE RESIDENCIAS PROFESIONALES Y SERVICIO SOCIAL	147
❖ SUBDIRECCION DE VINCULACION	160
❖ SUBDIRECCIÓN ACADÉMICA.....	174
❖ DEPARTAMENTO DE DESARROLLO ACADEMICO.....	189
❖ DIRECCIÓN ACADÉMICA	206

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

INTRODUCCIÓN

El derecho a la protección de los datos personales es un derecho humano reconocido en la Constitución Política de los Estados Unidos Mexicanos, en sus artículos 6, apartado A, fracción II, y 16, párrafo segundo, los cuales establecen las bases para garantizar la protección de la información personal y el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

El Instituto Tecnológico Superior de Cintalapa, como institución pública de educación superior, realiza diversas actividades académicas, administrativas, de investigación, vinculación y extensión educativa que implican la obtención, uso, registro, almacenamiento, conservación y, en su caso, transferencia de datos personales de estudiantes, aspirantes, egresados, docentes, personal administrativo, proveedores y demás personas que mantienen una relación con esta institución.

En el ejercicio de sus atribuciones, el Instituto reconoce la importancia de garantizar la protección de los datos personales que se encuentran bajo su resguardo, mediante la implementación de medidas de seguridad administrativas, físicas y técnicas que permitan prevenir su pérdida, alteración, destrucción, acceso, uso o divulgación no autorizados.

La Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas define los datos personales como cualquier información concerniente a una persona física identificada o identificable, considerando que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

Asimismo, distingue los datos personales sensibles como aquellos que se refieren a la esfera más íntima de su titular, cuya utilización indebida pueda dar origen a discriminación o conllevar un riesgo grave para este. Entre ellos se encuentran, de manera enunciativa y no limitativa, los datos relativos al origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas, datos biométricos y preferencia sexual.

En el ámbito institucional, el tratamiento de datos personales puede comprender información de identificación, contacto, trayectoria académica, situación escolar, información laboral, administrativa, patrimonial y, cuando resulte necesario para el cumplimiento de las atribuciones institucionales, información de carácter sensible.

Por lo anterior, el Instituto Tecnológico Superior de Cintalapa reconoce la necesidad de establecer mecanismos de protección que garanticen el tratamiento adecuado de dicha información, considerando las particularidades de los procesos desarrollados por sus diferentes direcciones, subdirecciones, departamentos, divisiones de carrera y demás áreas administrativas y académicas.

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

El presente Documento de Seguridad constituye un instrumento institucional que describe y da cuenta, de manera general, de las medidas de seguridad administrativas, físicas y técnicas adoptadas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales en posesión del Instituto.

Su elaboración se fundamenta en las disposiciones aplicables en materia de protección de datos personales en posesión de sujetos obligados, así como en las atribuciones y responsabilidades que corresponden al Instituto Tecnológico Superior de Cintalapa, de conformidad con su instrumento de creación y demás disposiciones que regulan su organización y funcionamiento.

En este sentido, el Instituto, a través de sus órganos administrativos y académicos, tiene la responsabilidad de implementar acciones que permitan proteger los datos personales tratados durante el desarrollo de sus actividades, procurando que su utilización se limite a las finalidades institucionales que justificaron su obtención.

Por lo anterior, el Instituto Tecnológico Superior de Cintalapa, con la finalidad de establecer, implementar y mantener las medidas de seguridad necesarias para la protección de los datos personales en su posesión, emite el presente Documento de Seguridad, en observancia de los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad, aplicables al tratamiento de datos personales en el ejercicio de sus atribuciones.

Asimismo, este documento constituye una herramienta de coordinación interna para que las diferentes áreas del Instituto identifiquen los datos personales que tratan, los riesgos asociados a su manejo, las medidas de seguridad existentes y las acciones necesarias para fortalecer su protección.

OBJETIVO DEL DOCUMENTO DE SEGURIDAD

El presente Documento de Seguridad tiene como objetivo general establecer, implementar, mantener y controlar las medidas de seguridad administrativas, físicas y técnicas necesarias para garantizar la protección de los datos personales en posesión del Instituto Tecnológico Superior de Cintalapa, mediante la identificación de los tratamientos de información, la asignación de responsabilidades, el análisis de riesgos y la aplicación de mecanismos de supervisión y mejora continua.

Asimismo, tiene como finalidad establecer y controlar internamente:

- El tratamiento de los datos personales en posesión del Instituto Tecnológico Superior de Cintalapa, derivado de sus actividades académicas, administrativas, de investigación, vinculación y extensión educativa.
- La identificación de los datos personales que integran los expedientes, archivos físicos, bases de datos, sistemas informáticos y demás medios de almacenamiento utilizados por las diferentes áreas del Instituto.
- Las obligaciones y responsabilidades de las personas servidoras públicas que intervienen en la obtención, registro, uso, almacenamiento, conservación, transferencia y disposición de los datos personales.
- La identificación y el análisis de los posibles riesgos que pudieran enfrentar los órganos administrativos y académicos del Instituto durante el tratamiento de los datos personales, considerando las amenazas, vulnerabilidades y consecuencias que pudieran comprometer su confidencialidad, integridad y disponibilidad.
- El establecimiento de medidas de seguridad administrativas, físicas y técnicas que permitan prevenir el acceso, uso, alteración, pérdida, destrucción o divulgación no autorizados de los datos personales.
- La identificación de las funciones y obligaciones del personal que, en el ejercicio de sus atribuciones, tenga acceso a información que contenga datos personales.
- La implementación de mecanismos de monitoreo, supervisión y revisión periódica de las medidas de seguridad adoptadas por las diferentes áreas del Instituto.
- El establecimiento de procedimientos para identificar, atender, documentar y, cuando corresponda, notificar las vulneraciones de seguridad que pudieran comprometer los datos personales bajo resguardo institucional.
- La promoción de una cultura institucional de protección de datos personales mediante acciones de capacitación, sensibilización y actualización dirigidas al personal académico y administrativo.
- La integración de la información proporcionada por las diferentes áreas académicas y administrativas, a fin de conformar un Documento de Seguridad institucional que refleje los tratamientos de datos personales y las medidas de protección implementadas en el Instituto.

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

En cumplimiento de las disposiciones aplicables en materia de protección de datos personales en posesión de sujetos obligados, el Instituto Tecnológico Superior de Cintalapa, a través de sus áreas académicas y administrativas, deberá identificar y documentar los tratamientos de datos personales que realiza en el ejercicio de sus atribuciones.

Para tal efecto, cada área deberá proporcionar la información correspondiente a los datos personales que trata, las finalidades de su utilización, los medios en que se encuentran almacenados, las personas que tienen acceso a ellos, los riesgos identificados y las medidas de seguridad implementadas.

La información proporcionada por las diferentes áreas será integrada y coordinada por la Unidad de Transparencia del Instituto, con la participación de las instancias institucionales competentes, a fin de conformar un documento que permita establecer las condiciones generales de seguridad para la protección de los datos personales en posesión de este sujeto obligado.

I. CONCEPTOS BÁSICOS EN LA MATERIA

Para efectos de la aplicación e interpretación del presente Documento de Seguridad para la Protección de los Datos Personales en Posesión del Instituto Tecnológico Superior de Cintalapa, se entenderá por:

- **Titular:** A la persona física a quien corresponden o pertenecen los datos personales que son objeto de tratamiento por parte del Instituto Tecnológico Superior de Cintalapa.
- **Responsable:** Al Instituto Tecnológico Superior de Cintalapa, en su carácter de sujeto obligado que decide sobre el tratamiento de los datos personales, de conformidad con sus atribuciones y las disposiciones legales aplicables.
- **Datos personales:** A cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.
- **Datos personales sensibles:** A los datos personales que se refieran a la esfera más íntima de su titular o cuya utilización indebida pueda dar origen a discriminación o conllevar un riesgo grave para este. De manera enunciativa, mas no limitativa, se consideran sensibles aquellos que puedan revelar aspectos como el origen racial o étnico, estado de

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas, datos biométricos y preferencia sexual.

- **Tratamiento:** A cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con su obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición.
- **Medidas de seguridad:** Al conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permiten proteger los datos personales contra su pérdida, alteración, destrucción, acceso, uso o divulgación no autorizados.
- **Medidas de seguridad administrativas:** A las políticas, procedimientos y acciones para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, así como para la identificación, clasificación y protección de los datos personales.
- **Medidas de seguridad físicas:** Al conjunto de acciones y mecanismos destinados a proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento, incluyendo instalaciones, archivos, mobiliario, equipos y dispositivos de almacenamiento.
- **Medidas de seguridad técnicas:** Al conjunto de acciones y mecanismos que se implementan mediante el uso de tecnologías para proteger los datos personales almacenados o tratados en equipos de cómputo, sistemas informáticos, redes institucionales y medios electrónicos.
- **Área u órgano administrativo:** A las direcciones, subdirecciones, departamentos, divisiones de carrera, unidades y demás áreas que integran la estructura orgánica del Instituto Tecnológico Superior de Cintalapa y que, en el ejercicio de sus funciones o atribuciones, realizan operaciones de tratamiento de datos personales.
- **Persona servidora pública responsable del tratamiento:** A la persona que, conforme a sus funciones, atribuciones y responsabilidades institucionales, interviene en el tratamiento, administración, manejo o resguardo de datos personales dentro de un área del Instituto.

- **Enlace de datos personales:** A la persona servidora pública designada por cada área académica o administrativa del Instituto para colaborar en la identificación de los tratamientos de datos personales, la recopilación de información, la documentación de medidas de seguridad y la coordinación de las actividades relacionadas con la elaboración y actualización del Documento de Seguridad institucional.
- **Unidad de Transparencia:** A la instancia del Instituto Tecnológico Superior de Cintalapa encargada de ejercer las funciones que le correspondan en materia de transparencia, acceso a la información pública y protección de datos personales, de conformidad con las disposiciones legales aplicables.
- **Autoridad garante:** A la autoridad competente en materia de protección de datos personales en posesión de sujetos obligados del Estado de Chiapas, conforme a la legislación vigente.
- **Instituto o ITSC:** Al Instituto Tecnológico Superior de Cintalapa.
- **Ley General:** A la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- **Ley Estatal:** A la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas.
- **Documento de Seguridad:** Al instrumento que describe y da cuenta, de manera general, de las medidas de seguridad administrativas, físicas y técnicas adoptadas por el Instituto Tecnológico Superior de Cintalapa para garantizar la confidencialidad, integridad y disponibilidad de los datos personales en su posesión.
- **Sistema de tratamiento:** Al conjunto organizado de archivos, registros, bases de datos, sistemas informáticos y demás medios físicos o electrónicos mediante los cuales el Instituto realiza operaciones de tratamiento de datos personales.
- **Inventario de datos personales:** Al registro que permite identificar los datos personales tratados por las diferentes áreas del Instituto, las categorías de sus titulares, las finalidades del tratamiento, los medios de almacenamiento y las demás características necesarias para su adecuada protección.

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

- **Análisis de riesgos:** Al proceso mediante el cual se identifican y evalúan las amenazas y vulnerabilidades que pudieran afectar los datos personales en posesión del Instituto, considerando la probabilidad de que ocurran y las posibles consecuencias para sus titulares.
- **Vulneración de seguridad:** A la afectación de la seguridad de los datos personales que puede comprender, entre otros supuestos, su pérdida, destrucción, robo, extravío, copia, uso, acceso, tratamiento, daño, alteración o modificación no autorizados.
- **Confidencialidad:** A la propiedad de la información que garantiza que los datos personales únicamente sean conocidos o utilizados por las personas autorizadas para ello.
- **Integridad:** A la propiedad de la información que permite preservar la exactitud y completitud de los datos personales, evitando su alteración o modificación no autorizada.
- **Disponibilidad:** A la propiedad de la información que permite que los datos personales sean accesibles y utilizables por las personas autorizadas cuando sean necesarios para el cumplimiento de sus funciones.
- **Derechos ARCOP:** A los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales que corresponden a sus titulares, en los términos establecidos por la legislación aplicable.
- **Aviso de privacidad:** Al documento que se pone a disposición del titular de los datos personales para informarle sobre las características y finalidades del tratamiento de su información, así como sobre los demás aspectos exigidos por la legislación aplicable.
- **Transferencia:** A toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a una persona distinta del titular, del responsable o del encargado, en los términos establecidos por la legislación aplicable.
- **Encargado:** A la persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta de este.

DEPARTAMENTO DE CONTROL ESCOLAR

II. NOMBRES DE LOS SISTEMAS DE TRATAMIENTO

Los datos personales en posesión del Departamento de Control Escolar del Instituto Tecnológico Superior de Cintalapa son sometidos a los siguientes tratamientos, derivados de los procesos de inscripción, reinscripción, seguimiento académico, egreso, titulación y demás actividades administrativas relacionadas con la trayectoria escolar de los estudiantes:

1. Integración, actualización y resguardo de los expedientes físicos y electrónicos de los estudiantes inscritos en los diferentes programas educativos de la institución.
2. Registro, captura y actualización de los datos personales de los estudiantes mediante el Sistema de Gestión de Matrícula Escolar MindBox.
3. Registro y control de los procesos de inscripción y reinscripción de los estudiantes, incluyendo la recepción, revisión y validación de la documentación personal y académica.
4. Integración, actualización y resguardo del historial académico de los estudiantes, incluyendo calificaciones, cargas académicas, movimientos escolares y demás información relacionada con su trayectoria educativa.
5. Registro, seguimiento y control de las solicitudes de bajas temporales y definitivas, así como de los movimientos académicos de los estudiantes.
6. Integración, uso y resguardo de los datos personales de los estudiantes para la expedición de constancias, credenciales, kárdex, certificados de estudios y demás documentos escolares oficiales.
7. Registro, integración y actualización de la información de los estudiantes para la elaboración de estadísticas institucionales, reportes de matrícula, ingreso, egreso, titulación, deserción, reprobación y eficiencia terminal.

8. Integración, uso y transferencia de los datos personales de los estudiantes al Tecnológico Nacional de México, para la elaboración de estadísticas oficiales, validación de información académica y cumplimiento de los requerimientos institucionales.
9. Integración, uso y transferencia de los datos personales de los estudiantes a la Coordinación Nacional de Becas para el Bienestar, para la validación de matrícula, inscripción, permanencia escolar y seguimiento de los programas de apoyos económicos federales.
10. Integración, actualización y resguardo de los expedientes físicos y electrónicos de los estudiantes egresados de los diferentes programas educativos de la institución.
11. Registro, integración y tratamiento de los datos personales de los egresados que solicitan el trámite de titulación electrónica.
12. Elaboración, integración y resguardo de los reportes de titulación denominados «Sábanas de Titulación», que contienen información personal y académica de los egresados.
13. Captura, validación y transferencia de los datos personales de los egresados mediante la Plataforma de Títulos Electrónicos de la Secretaría de Educación Pública del Estado de Chiapas, para la gestión y expedición de títulos profesionales electrónicos.
14. Integración, uso y resguardo de los archivos electrónicos y representaciones gráficas de los títulos profesionales, así como su entrega a los egresados mediante correo electrónico.
15. Integración, uso y transferencia de información personal y académica a la Dirección Académica, Dirección de Planeación y Vinculación y Dirección General del Instituto, para el cumplimiento de sus respectivas funciones institucionales.
16. Registro y control de las solicitudes de consulta y acceso a los expedientes escolares, mediante los formatos de autorización correspondientes.
17. Integración y resguardo de la documentación relacionada con los adeudos documentales de los estudiantes, mediante las cartas compromiso correspondientes.
18. Registro y control de acceso a los expedientes físicos y electrónicos que contienen datos personales de estudiantes y egresados, mediante las bitácoras institucionales correspondientes.

19. Registro, seguimiento y documentación de las vulneraciones a la seguridad de los datos personales bajo resguardo del Departamento de Control Escolar, mediante las bitácoras y mecanismos de control establecidos.

III. EL NOMBRE, CARGO Y ADSCRIPCIÓN DEL ADMINISTRADOR DEL SISTEMA DE TRATAMIENTO.

Los responsables del tratamiento de los datos personales del Departamento de Control Escolar, son los que describen a continuación:

Responsable	Cargo	Órgano Administrativo	Tratamiento
[REDACTED]	Jefa del Departamento de Control Escolar. Responsable de la Supervisión y revisión de la información estudiantil, física y electrónica.	Departamento de Control Escolar.	[REDACTED]
[REDACTED]	Psicóloga Responsable de la gestión de archivo físico del estudiantado vigente y no vigente.	Departamento de Control Escolar – Área de Archivo.	[REDACTED]
[REDACTED]	Analista Especializado Responsable de la gestión de archivo físico y electrónico de los egresados, para trámites de egreso (Títulos Electrónicos).	Departamento de Control Escolar – Área de Títulos Electrónicos.	[REDACTED]

“Se están las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTIIP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTIAPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

IV. LAS FUNCIONES Y OBLIGACIONES DEL RESPONSABLE Y TODAS LAS PERSONAS SERVIDORAS PÚBLICAS QUE TRATEN DATOS PERSONALES.

Las funciones y obligaciones del responsable y de todas las personas servidoras públicas que traten datos personales en el Departamento de Control Escolar son las siguientes:

Funciones:

- Dar a los datos personales un tratamiento responsable, conforme a las medidas de seguridad establecidas para tal efecto;
- Salvaguardar los datos personales a los que se tenga acceso con motivo del ejercicio de sus funciones;
- Comprobar que el inventario de datos personales y de los sistemas de tratamiento a los que tengan acceso estén ordenados, y su resguardo corresponda a su periodo de atención y gestión;
- Conservar actualizado el listado de personas usuarias que den tratamiento a datos personales;
- Ante un incidente de vulneración de seguridad de los datos personales o de sus sistemas de tratamiento, notificar de inmediato a la persona titular y documentar los hechos, mediante el Anexo 2.

Obligaciones:

- Guardar confidencialidad respecto de los datos personales a los que se tenga acceso, incluso después de concluida la relación laboral;
- Limitar el tratamiento de los datos personales a las finalidades previstas en el aviso de privacidad correspondiente;
- Abstenerse de transferir, difundir o divulgar datos personales sin el consentimiento de la persona titular o sin fundamento legal que lo autorice o bien sea una función a fin a sus actividades laborales;
- Utilizar únicamente los equipos, sistemas y medios institucionales autorizados para el tratamiento de los datos personales;

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

- Custodiar los expedientes físicos y electrónicos en espacios con acceso restringido, controlado y autorizado.

V. LOS DATOS PERSONALES TRATADOS EN LOS SISTEMAS DE TRATAMIENTOS Y/O BASE DE DATOS PERSONALES SON LOS SIGUIENTES:

Datos:

- ❖ Número de Control
- ❖ Nombres y Apellidos
- ❖ Firma
- ❖ Nivel Educativo
- ❖ Dirección
- ❖ Código postal
- ❖ Localidad
- ❖ Municipio y entidad federativa.
- ❖ Estado INGENIERIA
- ❖ Nacionalidad
- ❖ Edad
- ❖ Género
- ❖ Lugar y Fecha de Nacimiento
- ❖ Tipo de Sangre
- ❖ Número de Seguridad Social
- ❖ Número de Teléfono Fijo o Celular
- ❖ Correo electrónico
- ❖ Lengua indígena o pertenencia a un pueblo originario
- ❖ Condición de discapacidad o necesidad de apoyo
- ❖ Situación laboral
- ❖ Situación económica

Documentos:

- Solicitud de Inscripción
- Formato de Autorización de Consulta de Expediente.
- Carta Compromiso de Adeudo de Documentos.

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

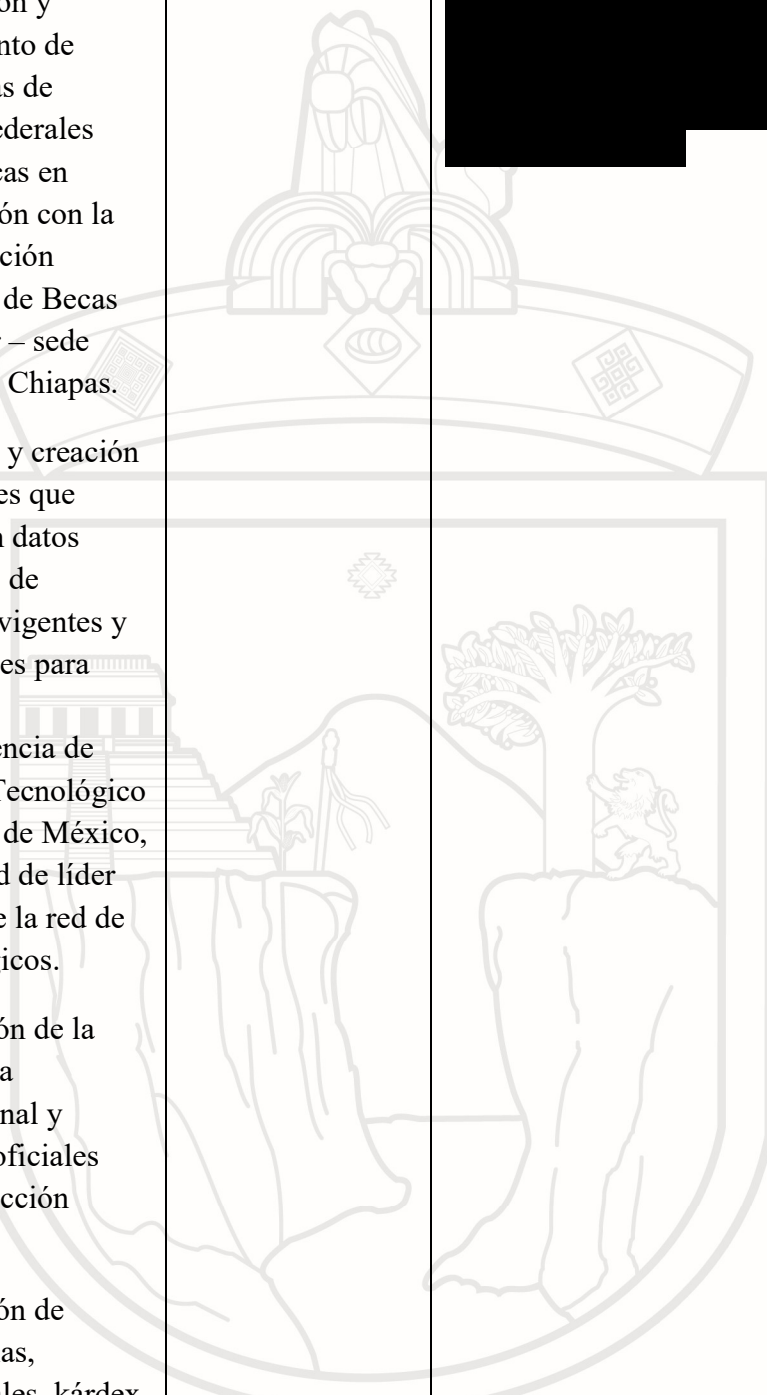
- Carga Académica del periodo escolar en curso.
- Acta de Nacimiento
- Credencial para Votar (INE)
- Cartilla Militar
- Pasaporte
- Clave Única de Registro de Población (CURP)
- Comprobante de Domicilio
- Número de Teléfono Fijo o Celular
- Certificado Médico
- Carta de Buena Conducta
- Certificado de Bachillerato
- Constancias de Terminación de Estudios de Bachillerato.

VI. LA DESCRIPCIÓN DEL SISTEMA DE TRATAMIENTO, SEÑALANDO EL TIPO DE SOPORTE Y LAS CARACTERÍSTICAS DEL LUGAR DONDE SE RESGUARDAN.

Descripción del Sistema de Tratamiento	Tipo de Soporte	Características del lugar de resguardo
1. Integración de datos electrónicos mediante el Sistema de Gestión de Matrícula Escolar; MindBox. Sistema que resguarda y gestiona el historial académico de la matrícula de los 6 programas educativos vigentes de la institución. • Descarga y creación de reportes que contienen datos generales de alumnos vigentes para la gestión,	Electronico. Sistema de Gestión de Matrícula Escolar; MindBox.	[REDACTED]

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LEIAPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

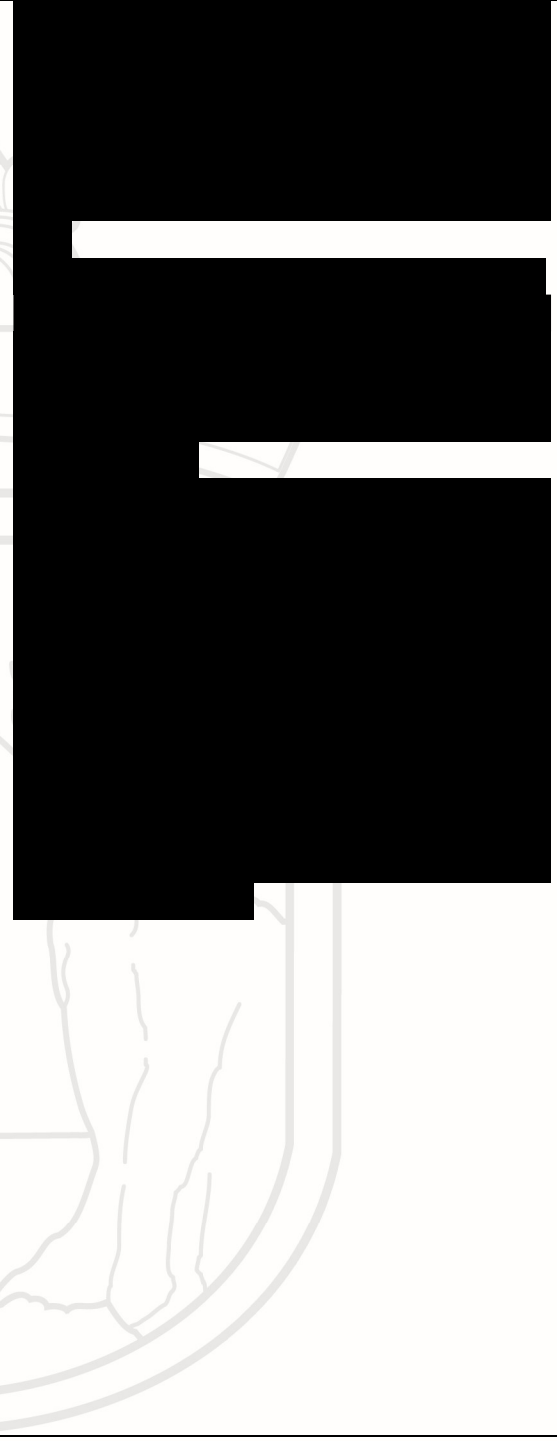


adquisición y seguimiento de programas de apoyos federales como becas en vinculación con la Coordinación Nacional de Becas Bienestar – sede estatal en Chiapas. • Descarga y creación de reportes que contienen datos generales de alumnos vigentes y no vigentes para realizar Transferencia de datos al Tecnológico Nacional de México, en calidad de líder federal de la red de Tecnológicos. • Integración de la estadística institucional y reportes oficiales para Dirección General. • Expedición de constancias, credenciales, kárdex		
--	---	--

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

y certificados de estudios mismos que son entregados a los estudiantes titulares del trámite y de la información que integra dichos documentos escolares.		
2. Se integran y actualizan los expedientes de cada persona con estatus de Alumno Vigente, para el control y seguimiento de los datos personales y sensibles tratados para: - Inscripción, reinscripción y control de la trayectoria académica (calificaciones, movimientos, bajas temporales y definitivas). - Guarda y custodia en los expedientes de los alumnos vigentes e inscritos en el periodo en curso, así como de alumnos que solicitan su baja académica.	Físico.	

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

3. Creación de reportes impresos (Sabanas de Titulación) que contienen datos generales de alumnos no vigentes con estatus de Egresados, quienes realizan la solicitud de trámite de Titulación Electrónica, por lo cual se procede a realizar el trámite a petición de los interesados, el proceso requiere realizar entrega a la Secretaría de Educación Pública Estatal, en calidad de enlace entre institución educativa y la Dirección General de Profesiones para la emisión de Títulos Electrónicos Profesionales. Paso 1: El Analista Especializado responsable del área de Títulos Electrónicos, procede a trabajar la información de los egresados en un formato Tabla en archivo CSV editable, mismo que es impreso para realizar entrega física a la SEP estatal, mediante las “Sabanas de Titulación”, y resguardar el archivo CSV editable en el equipo de cómputo del departamento de Títulos Electrónicos, mismo que se utilizará en el paso 3. Paso 2: Una vez entregado a la SEP estatal las sábanas de Titulación Físicas, esta	Físico y electrónico.		“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIIP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPEC), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”
--	------------------------------	---	--

procede a realizar una validación de los datos del egresado que contiene dicho reporte, y queda en resguardo de la SEP estatal este documento en original, acusando de recibido mediante una copia fiel del documento original.

Paso 3: Una vez entregado el documento físico ante la SEP estatal, la institución educativa carga el reporte en archivo digital editable CSV en la Plataforma de Títulos Electrónicos, una vez cargado notifica a la SEP estatal para seguimiento y aplicación de firmas electrónicas de las autoridades educativas correspondientes.

Paso 4: La Dirección General de la Institución Educativa, también firma de forma electrónica en coordinación con la SEP estatal, confirma a la instancia cuando la firma ha sido aplicada.

Paso 5: Una vez finalizado el proceso de firmas, se procede a la emisión de las representaciones gráficas de los “Títulos Electrónicos” de cada egresado.

Paso 6: Una vez que se cuenta con las representaciones gráficas de

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

cada egresado, estos son enviados por correo electrónico individual a cada egresado, mismos que confirman de recibido el correo electrónico y se da por concluido el trámite por parte de la Institución Educativa y de la SEP estatal.

VII. LOS CONTROLES Y MECANISMOS DE SEGURIDAD PARA LAS TRANSFERENCIAS QUE, EN SU CASO, SE EFECTÚEN.

A continuación, se detalla las áreas tanto internas como externas que reciben información del Departamento de Control Escolar:

Áreas Internas:

- Dirección de Planeación y Vinculación

Uso de información:

- Integrar la estadística institucional (matrícula, ingreso, egreso, titulación, deserción, reprobación y eficiencia terminal) para dar seguimiento a los reportes oficiales, como la estadística 911 de la SEP y reportes presentados ante los miembros de la Junta Directiva Institucional;
- Elaborar y dar seguimiento a los programas institucionales, indicadores y metas, así como a los procesos de evaluación y acreditación;
- Atender solicitudes de información del TecNM, SEP y las autoridades, así como auditorías y requerimientos de transparencia.

Uso de información:

- Dar seguimiento a la trayectoria académica de los alumnos (aprobación, reprobación, rezago y deserción y posible reincorporación con apego a los lineamientos vigentes de TecNM Federal);

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIIP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

- Operar los programas de tutoría, asesoría académica y atención a alumnos en riesgo de abandono escolar.
- Analizar y dictaminar casos de alumnos con estatus de equivalencia, revalidación, baja, reingreso o situaciones académicas especiales;
- Coordinar los procesos de acreditación de programas educativos y las opciones de titulación en vinculación con el Departamento de Control Escolar.

➤ Dirección General

Uso de información:

- Tomar decisiones institucionales;
- Elaborar los informes de rendición de cuentas ante las autoridades y órganos de gobierno;
- Atender los requerimientos del TecNM, la SEP Federal, estatal y otras instancias fiscalizadoras o de control;
- Firmar y validar documentos oficiales, como certificados de estudios, actas y documentación de titulación;
- Resolver casos especiales que requieran su intervención.

Áreas externas:

➤ Tecnológico Nacional de México

Uso de información:

- Integrar la estadística institucional y los reportes oficiales de matrícula, ingreso, egreso y titulación.
 - Alimentar y validar los sistemas de información del TecNM Federal.
 - Supervisar los procesos de titulación y el cumplimiento de la normatividad académica y administrativa.
 - Atender auditorías, evaluaciones, acreditaciones y requerimientos de rendición de cuentas federales.
 - Dar seguimiento a los programas y apoyos federales que operan a través del TecNM.
- Secretaría de Educación Pública del Estado

Uso de información:

- Fungir como enlace de trámite ante la Institución Educativa y la Dirección General de Profesiones, así como realizar la expedición de Títulos Electrónicos.
 - Integrar la estadística educativa estatal con los datos otorgados por parte de la Institución Educativa;
 - Registrar y validar la información de estudiantes, egresados y titulados para efectos oficiales.
- Coordinación Nacional de Becas Bienestar

Uso de información:

- Verificar la inscripción y la vigencia escolar de los alumnos postulantes o beneficiarios;
- Conciliar los padrones de beneficiarios;
- Dispersar los apoyos económicos;
- Validar la identidad y los datos de los becarios (CURP, matrícula, programa educativo y semestre);
- Confirmar la permanencia, la baja o el egreso para continuar o suspender el apoyo económico;
- Atender revisiones, auditorías y requerimientos de control del programa a nivel federal.

Mecanismos de seguridad:

Para implementar las medidas de seguridad aplicables a la transferencia de datos personales el receptor de los datos personales asumirá el carácter de responsable conforme a la legislación en la materia al recibir dicha información mediante el traslado de soportes físicos, electrónicos o a través del correo electrónico institucional, por lo que deberá tratar los datos personales atendiendo y apegándose al aviso de privacidad del Departamento de Control Escolar, mismo que se encuentra publicado en:

<https://cintalapa.tecnm.mx/aviso-privacidad>

En cada una de estas modalidades se deberá sujetarse a lo siguiente:

A. Traslado de soportes físicos: Los datos personales se trasladan en documentos impresos que pueden leerse directamente, sin necesidad de un dispositivo que procese su contenido para consultarlo, modificarlo o almacenarlo.

Por ejemplo: cuando el Departamento de Control Escolar remite por correo electrónico

institucional oficial oficios, formatos, constancias o copias de documentos del expediente del alumno o del egresado a la Dirección Académica.

B. Traslado físico de soportes electrónicos: Los datos personales se entregan al destinatario mediante archivos electrónicos almacenados en medios que requieren un dispositivo con circuitos electrónicos para consultar, modificar o almacenar su contenido.

Por ejemplo: cuando el Departamento de Control Escolar entrega mediante una memoria USB con los archivos digitalizados de expedientes.

C. Traslado sobre redes electrónicas: Los datos personales se transmiten en archivos electrónicos a través de una red electrónica.

Por ejemplo: cuando el Departamento de Control Escolar realiza carga de las bases de datos de la matrícula institucional en las plataformas oficiales del Tecnológico Nacional de México, para las estadísticas oficiales.

VIII. EL RESGUARDO DE LOS SOPORTES FÍSICOS DE LOS DATOS PERSONALES.

Los expedientes físicos se encuentran resguardados y en custodia de los responsables del sistema de tratamiento de los datos personales en el área asignada para tal efecto.

IX. LAS BITÁCORAS DE ACCESO Y VULNERACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES.

Los datos que se registran en la Bitácora de acceso (anexo 1) son los siguientes:

- Número consecutivo;
- Quien accede a los datos personales (Nombre completo);
- Cargo;
- Área de adscripción;
- Propósito del acceso;
- Número de control del alumno y/o egresado;
- Tipo de soporte utilizado (Expediente o registro electrónico);
- Fecha en formato mes y año (Al que corresponde la bitácora).

Los datos que se registran en la Bitácora de vulneraciones (anexo 2) son los siguientes:

- Número consecutivo;
- Fecha y hora de la vulneración;
- Documento o información vulnerada;

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIIP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPECHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

- Motivo de la vulneración;
- Acciones correctivas y definitivas implementadas;
- Persona que resolvió la vulneración;
- Fecha y hora de notificación de la vulneración a los titulares de los datos personales comprometidos;
- Fecha en formato mes y año (Al que corresponde la bitácora).

X. EL ANÁLISIS DE RIESGOS.

Amenaza	Vulnerabilidades	Posibles consecuencias

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIIP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTALPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

- [REDACTED]
- 3. [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
- 4. [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
- 5. [REDACTED]
 - [REDACTED]
 - [REDACTED]

XII. LA GESTIÓN DE VULNERACIONES.

En caso de ocurrir alguna vulneración deberá registrarse en la bitácora de contingencias (Anexo 2), y se llevará a cabo conforme al siguiente procedimiento:

1. **Detección y aviso interno:** El personal del departamento que detecte o sospeche de una vulneración lo comunicará de inmediato a la Jefatura del Departamento de Control Escolar, preservando el estado de los documentos, equipos o sistemas involucrados.
2. **Contención:** Se ejecutarán acciones inmediatas para evitar mayor afectación, tales como resguardar el archivo, suspender accesos, cambiar contraseñas o desconectar el equipo comprometido.
3. **Registro inicial:** Se asentará en la bitácora la fecha y hora de la vulneración, el documento o información vulnerada y el motivo de la vulneración.

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx



“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

4. **Evaluación:** La Jefatura determinará el alcance del incidente, las personas titulares afectadas y si se comprometen sus derechos patrimoniales o morales.
5. **Acciones correctivas y definitivas:** Se implementarán las medidas para restablecer la información y eliminar la causa, y se registrarán en la bitácora junto con el nombre de la persona que resolvió la vulneración.
6. **Notificación:** Se informará a las personas titulares, sin dilación alguna y dentro del plazo no mayor a 3 días (72 horas), la notificación incluirá la naturaleza del incidente, los datos personales comprometidos, las recomendaciones para la persona titular, las acciones correctivas realizadas y los medios para obtener mayor información. Se registrará en la bitácora la fecha y hora de cada notificación.
7. **Cierre y prevención.** La Jefatura revisará las medidas de seguridad vigentes y ajustará las que resulten necesarias para evitar que el incidente se repita.

XIII. LAS MEDIDAS DE SEGURIDAD FÍSICAS APLICADAS A LAS INSTALACIONES.

[Redacted content]

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTIAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPECIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

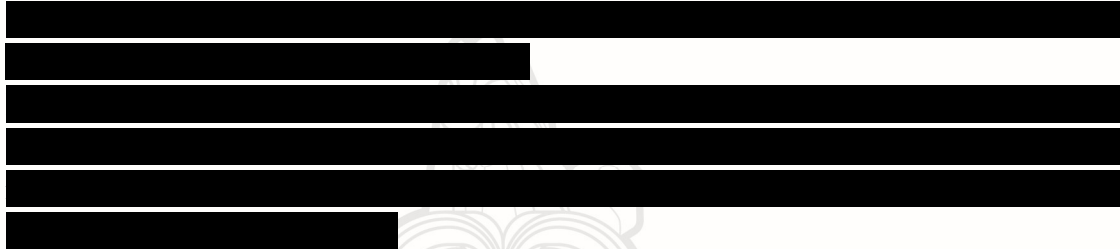
XIV. LOS CONTROLES DE IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS.

XV. LOS PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS PERSONALES.

XVI. EL PLAN DE CONTINGENCIA.

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIIP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales de la información de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx



XVII. LAS TÉCNICAS UTILIZADAS PARA LA SUPRESIÓN Y BORRADO SEGURO DE LOS DATOS PERSONALES.

La supresión de expedientes y archivos que contengan datos personales sólo podrá efectuarse una vez cumplidos los periodos de conservación y las disposiciones archivísticas y académicas aplicables. Los documentos físicos cuya eliminación proceda deberán destruirse de manera que la información no pueda reconstruirse **ni reutilizarse**; los archivos electrónicos deberán eliminarse mediante mecanismos que impidan su recuperación no autorizada.

No deberán utilizarse como papel de reúso documentos que contengan datos personales de estudiantes o egresados.

XVIII. EL PLAN DE TRABAJO.



XIX. LOS MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD.

La Jefatura del Departamento realizará el monitoreo de los controles de acceso físico y electrónico, las bitácoras de acceso y vulneraciones, los permisos de los sistemas y el estado de los expedientes y respaldos bajo resguardo.

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIPI) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPI-CHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

Los incidentes, cambios de plataforma o nuevas condiciones de riesgo deberán revisarse para determinar si es necesario actualizar las medidas de seguridad y el presente Documento de Seguridad.

XX. EL PROGRAMA GENERAL DE CAPACITACIÓN.

El personal del Departamento de Control Escolar que trate datos personales deberá participar en acciones de capacitación sobre confidencialidad, avisos de privacidad, derechos ARCOP, manejo seguro de expedientes, uso autorizado de MindBox y de la Plataforma de Títulos Electrónicos, registro de accesos y atención de vulneraciones.

La capacitación deberá reforzarse cuando se incorporen nuevas personas al área, cambien los sistemas o procedimientos de tratamiento o se detecten incidentes y riesgos que requieran nuevas medidas de protección.

ANEXO 1: BITÁCORA DE ACCESO A LOS DATOS PERSONALES

Órgano Administrativo (o área generadora/resguardante):

Instituto Tecnológico Superior de Cintalapa
Departamento de Control Escolar.

Responsable del Archivo:

María Antonieta Medina Mata
Jefa del Departamento de Control Escolar

Número consecutivo	Quien accede a los datos personales (Nombre completo)	Cargo	Área de adscripción	Propósito del acceso	Número de control del alumno y/o egresado	Tipo de soporte utilizado (Expediente o registro electrónico)	Fecha en formato mes y año (Al que corresponde la bitácora)

ANEXO 2: BITÁCORA DE VULNERACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES

Órgano Administrativo (o área generadora/resguardante):

Instituto Tecnológico Superior de Cintalapa
Departamento de Control Escolar.

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

Responsable del Archivo:

María Antonieta Medina Mata

Jefa del Departamento de Control Escolar

Número consecutivo	Fecha y Hora Vulneración	Documento o información vulnerada	Motivo de la vulneración	Acciones correctivas y definitivas implementadas	Persona que resolvió la vulneración	Fecha y hora de notificación de la vulneración a los titulares de los datos personales comprometidos	Fecha en formato mes y año (Al que corresponde la bitácora)

DEPARTAMENTO DE POSGRADO E INVESTIGACIÓN:

II. NOMBRES DE LOS SISTEMAS DE TRATAMIENTO

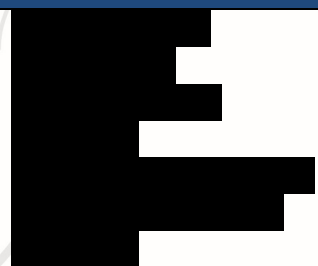
Los datos personales en posesión del Departamento de Posgrado e Investigación del Instituto Tecnológico Superior de Cintalapa son sometidos a los siguientes tratamientos, derivados de las actividades de seguimiento de proyectos de investigación, integración de expedientes docentes y gestión de la información institucional:

1. Registro y seguimiento de los proyectos de investigación desarrollados por el personal docente de la institución.
2. Integración, actualización y resguardo de los expedientes físicos y electrónicos de los docentes que participan en proyectos de investigación.
3. Recopilación, registro y actualización de los datos personales de los docentes, incluyendo nombre completo, correo electrónico, adscripción institucional, cargo o función y firma, para el seguimiento de sus proyectos de investigación.
4. Integración, organización y resguardo de la documentación proporcionada por los docentes para el seguimiento de los proyectos de investigación.
5. Registro y control de la información personal y académica contenida en los documentos que integran los expedientes docentes relacionados con las actividades de investigación.

6. Integración y resguardo de las carpetas electrónicas que contienen información de los proyectos de investigación y expedientes docentes, mediante los servicios institucionales de almacenamiento en la nube autorizados por el Instituto.
7. Registro y control de acceso a los expedientes físicos y electrónicos que contienen datos personales de los docentes, mediante las bitácoras correspondientes.
8. Integración y resguardo de los documentos físicos que contienen datos personales de los docentes, mediante los archiveros y espacios asignados al Departamento de Posgrado e Investigación.
9. Registro, seguimiento y documentación de las vulneraciones a la seguridad de los datos personales bajo resguardo del Departamento de Posgrado e Investigación, mediante las bitácoras institucionales correspondientes.
10. Respaldo y recuperación de los documentos electrónicos que contienen datos personales de los docentes, mediante los servicios institucionales de almacenamiento autorizados.
11. Conservación y, cuando corresponda, supresión o eliminación segura de los documentos físicos y electrónicos que contienen datos personales, conforme a los periodos de conservación y las disposiciones archivísticas aplicables.

III. EL NOMBRE, CARGO Y ADSCRIPCIÓN DEL ADMINISTRADOR DEL SISTEMA DE TRATAMIENTO.

Los responsables del tratamiento de los datos personales es el Departamento de Posgrado e Investigación, son los que se describen a continuación:

Responsable	Cargo	Órgano Administrativo	Tratamiento
	Jefe de Departamento de Posgrado e Investigación	Instituto Superior Tecnológico de Cintalapa	

IV. LAS FUNCIONES Y OBLIGACIONES DEL RESPONSABLE Y TODAS LAS PERSONAS SERVIDORAS PÚBLICAS QUE TRATEN DATOS PERSONALES.

Funciones:

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

- Tratar los datos personales con responsabilidad y las medidas de seguridad que se hayan establecido para tal fin.
- Resguardar los datos personales a los que tengan acceso en el ejercicio de sus atribuciones.
- Verificar que el inventario de datos personales y de los sistemas de tratamiento de los mismos, a los que tienen acceso, se encuentren actualizados.
- En caso de que se presente algún incidente de vulneración de seguridad de los datos personales y/o de los sistemas de tratamiento de los mismos, informar sin dilación alguna a la persona titular, a la Unidad de Transparencia y llevar el registro de los hechos.

Obligaciones:

- Llevar a cabo permanentemente las medidas de seguridad necesarias para la protección de los datos personales, evitando daño, pérdida, alteración, destrucción o uso, acceso o tratamiento no autorizado, así como también garantizar la confidencialidad, integridad y disponibilidad de los mismos.
- Acatar los mecanismos para asegurar que los datos personales a los que tengan acceso en el ejercicio de sus atribuciones no se difundan, distribuyan o comercialicen.
- Guardar confidencialidad sobre la información que se conozca en el desarrollo de sus actividades.

V. Los datos personales tratados en los sistemas de tratamientos y/o base de datos personales son los siguientes:

- Nombre completo;
- Correo electrónico;
- Adscripción institucional;
- Cargo o función;
- Firma;
- Los demás datos personales que se encuentren contenidos en los documentos proporcionados para el seguimiento de proyectos de investigación y la integración de expedientes docentes.

VI. LA DESCRIPCIÓN DEL SISTEMA DE TRATAMIENTO, SEÑALANDO EL TIPO DE SOPORTE Y LAS CARACTERÍSTICAS DEL LUGAR DONDE SE RESGUARDAN.

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIIP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

Descripción del Sistema de Tratamiento	Tipo de Soporte	Características del lugar de resguardo
Seguimiento de Proyectos de Investigación de Docentes.	Carpetas electrónicas almacenadas en el servicio institucional de almacenamiento en nube autorizado por el Instituto, con acceso restringido mediante cuentas institucionales	[REDACTED]
Integración y resguardo de los expedientes de Docentes.	Carpetas electrónicas almacenadas en el servicio institucional de almacenamiento en nube autorizado por el Instituto, con acceso restringido mediante cuentas institucionales	[REDACTED]

VII. LOS CONTROLES Y MECANISMOS DE SEGURIDAD PARA LAS TRANSFERENCIAS QUE, EN SU CASO, SE EFECTÚEN.

Con base en la información proporcionada por el Departamento de Posgrado e Investigación para los tratamientos descritos en los apartados II a VI, no se documentan transferencias específicas de datos personales a terceros. El tratamiento identificado se concentra en el seguimiento de proyectos de investigación, la integración y resguardo de expedientes docentes y el almacenamiento institucional autorizado. Si en el ejercicio de sus atribuciones resultara necesario comunicar información a otra área institucional o a una instancia competente, deberá limitarse a los datos estrictamente necesarios, utilizar medios institucionales autorizados y observar el aviso de privacidad y los controles de acceso aplicables.

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIPI) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

VIII. EL RESGUARDO DE LOS SOPORTES FÍSICOS DE LOS DATOS PERSONALES.

Los expedientes físicos se encuentran resguardos y en custodia de los responsables del sistema de tratamiento de los datos personales en el área asignada para tal efecto.

IX. LAS BITÁCORAS DE ACCESO Y VULNERACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES.

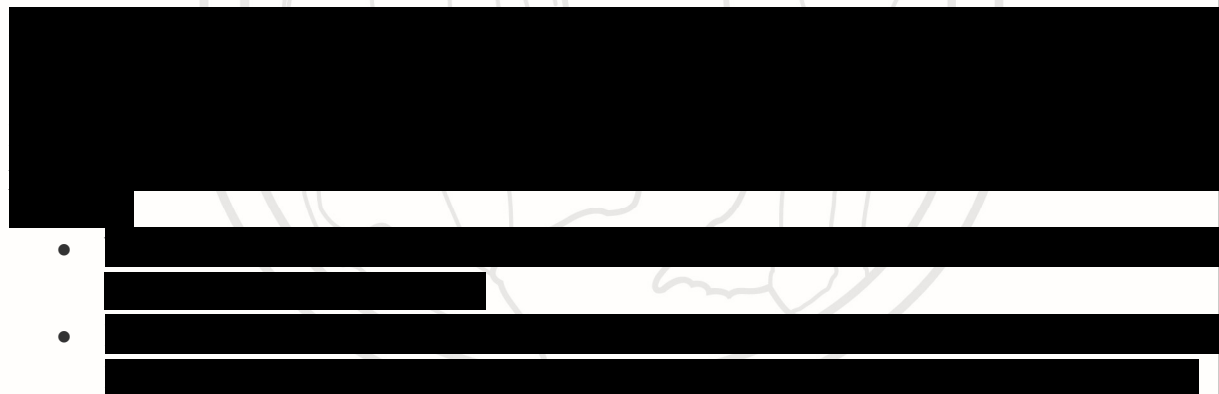
Los datos que se registran en la Bitácora de acceso (Anexo 1) son los siguientes:

- Quien accede a los datos personales, cargo y adscripción;
- Fecha y hora en la que se realiza el acceso o se intenta el mismo, así como fecha y hora de salida;
- Propósito del acceso;
- Firma de quien autoriza el acceso.

Los datos que se registran en la Bitácora de vulneraciones (Anexo 2) son los siguientes:

- Fecha y hora de la vulneración;
- Motivo de la vulneración;
- Acciones correctivas y definitivas implementadas;
- Persona que resolvió la vulneración;
- Fecha y hora de notificación de la vulneración a los titulares de los datos personales comprometidos o afectados y a la Autoridad Garante en materia de protección de datos personales; y
- Los oficios, documentos, expedientes, estantes o archiveros dañados y los recuperados.

X. EL ANÁLISIS DE RIESGOS.





- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

[Redacted]

[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIIP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de información, así como para la elaboración de versiones públicas.”



XIII. LAS MEDIDAS DE SEGURIDAD FÍSICAS APLICADAS A LAS INSTALACIONES.

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

XIV. LOS CONTROLES DE IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS.

[REDACTED]

XV. LOS PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS PERSONALES.

[REDACTED]

XVI. EL PLAN DE CONTINGENCIA.

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 1 y 2 de la Ley de Transparencia y Acceso a la Información Pública (LTAIP), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación de la información, así como para la elaboración de versiones públicas.”



XVII. LAS TÉCNICAS UTILIZADAS PARA LA SUPRESIÓN Y BORRADO SEGURO DE LOS DATOS PERSONALES.

- Destrucción segura de documentos: Los documentos y otros medios físicos no deben simplemente desecharse una vez que ya no se utilizan, sino destruirse por ejemplo con trituración mecánica o método autorizado de destrucción segura, conforme a las disposiciones archivísticas aplicables.
- Destrucción segura de información en equipo de cómputo y medios de almacenamiento electrónico: Herramientas de software que borran archivos electrónicos específicos o dispositivos completos.
- Fijar periodos de retención y destrucción de información: Identificar de manera regular toda la información que ya no es de utilidad.
- Tomar precauciones con los procedimientos de reutilización: Bajo ninguna circunstancia deberían utilizarse documentos con datos personales como papel de reúso.

XVIII. EL PLAN DE TRABAJO.

Actividad	Responsable	Periodicidad	Evidencia
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

XIX. LOS MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD.

Las medidas de seguridad serán revisadas al menos una vez al año y adicionalmente cuando exista una modificación sustancial en los sistemas de tratamiento, se presente una vulneración o se identifique un nuevo riesgo.

XX. EL PROGRAMA GENERAL DE CAPACITACIÓN.

- Sensibilización en materia de Protección de Datos Personales en el Departamento de Posgrado e Investigación y su importancia en el entorno laboral por parte de la Unidad de Transparencia.
- Capacitación a las personas servidoras públicas asignadas como enlaces en materia de datos personales respecto a los mecanismos, medios y procedimientos disponibles para ejercer los Derechos ARCO y Portabilidad de los datos personales por parte de la Unidad de Transparencia.
- Concientizar a las personas servidoras públicas que dentro de sus funciones y obligaciones se encuentren la de recabar los datos personales, respecto a la importancia de informar a la persona titular de los datos personales a través del Aviso de Privacidad, el tratamiento de los mismos.
- Informar a las personas servidoras públicas que cuentan con la facultad de autorizar, acordar y/o decidir en el Órgano Administrativo, respecto a la implementación de las medidas de seguridad administrativa, técnicas y físicas, para la protección de los datos personales.
- Capacitar a las personas servidoras públicas autorizadas en el manejo, resguardo, conservación y eliminación segura de documentos físicos y electrónicos que contengan datos personales.

ANEXO 1: Bitácora de acceso a los Datos Personales

Órgano Administrativo: Departamento de Posgrado e Investigación

Responsable del Archivo: Jefe del Departamento de Posgrado e Investigación.

No.	Nombres y Apellidos	Cargo y Adscripción	Fecha y Hora de Acceso	Fecha y Hora de Salida	Propósito del Acceso	Firma

ANEXO 2: Bitácora de vulneraciones a la seguridad de los Datos Personales

Órgano Administrativo: Departamento de Posgrado e Investigación

Responsable del Archivo: Jefe del Departamento de Posgrado e Investigación.

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

N o.	Fecha y Hora Vulneración	Motivo Vulneración	Acciones Correctivas	Acciones Definitivas	Fecha Notificación Titular	Fecha Notificación Autoridad	Datos / Expedientes Afectados

DEPARTAMENTO DE CIENCIAS BÁSICAS

II. NOMBRES DE LOS SISTEMAS DE TRATAMIENTO

Los datos personales en posesión del Departamento de Ciencias Básicas del Instituto Tecnológico Superior de Cintalapa son sometidos a los siguientes tratamientos, derivados de las funciones y actividades descritas en su Documento de Seguridad:

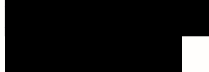
1. Seguimiento académico del personal docente de los diferentes programas educativos, incluyendo el registro y control de evaluaciones, desempeño y cumplimiento de los programas de estudio.
2. Consulta de datos personales de alumnos mediante el sistema institucional MindBox y, en casos específicos, mediante consulta documental de expedientes, para fines de gestión y seguimiento académico.
3. Integración y resguardo de las canalizaciones de asesorías académicas en materias de ciencias básicas, incluyendo canalizaciones y reportes de evidencia, en soporte físico y electrónico.
4. Registro y control de acceso a los documentos y sistemas que contienen datos personales bajo resguardo del Departamento de Ciencias Básicas.
5. Registro, seguimiento y documentación de vulneraciones a la seguridad de los datos personales mediante las bitácoras correspondientes.

III. EL NOMBRE, CARGO Y ADSCRIPCIÓN DEL ADMINISTRADOR DEL SISTEMA DE TRATAMIENTO.

Los responsables del tratamiento de los datos personales en el Departamento de Ciencias Básicas, son los que se describen a continuación:

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 17 y 18 de la Ley de Transparencia y Acceso a la Información Pública (LTAIP) y 136 de la Ley de Transparencia y Acceso a la Información Pública (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación de la información, así como para la elaboración de versiones públicas.”

Responsable	Cargo	Órgano Administrativo	Tratamiento
	Jefe de Departamento de Ciencias Básicas	Instituto Superior Tecnológico de Cintalapa	

IV. LAS FUNCIONES Y OBLIGACIONES DEL RESPONSABLE Y TODAS LAS PERSONAS SERVIDORAS PÚBLICAS QUE TRATEN DATOS PERSONALES.

Funciones:

- Tratar los datos personales con responsabilidad y las medidas de seguridad que se hayan establecido para tal fin.
- Resguardar los datos personales a los que tengan acceso en el ejercicio de sus atribuciones.
- Verificar que el inventario de datos personales y de los sistemas de tratamiento de los mismos, a los que tienen acceso, se encuentren actualizados.
- En caso de que se presente algún incidente de vulneración de seguridad de los datos personales y/o de los sistemas de tratamiento de los mismos, informar sin dilación alguna a la persona titular, a la Autoridad Garante y llevar el registro de los hechos.

Obligaciones:

- Llevar a cabo permanentemente las medidas de seguridad necesarias para la protección de los datos personales, evitando daño, pérdida, alteración, destrucción o uso, acceso o tratamiento no autorizado, así como también garantizar la confidencialidad, integridad y disponibilidad de los mismos.
- Acatar los mecanismos para asegurar que los datos personales a los que tengan acceso en el ejercicio de sus atribuciones no se difundan, distribuyan o comercialicen.
- Guardar confidencialidad sobre la información que se conozca en el desarrollo de sus actividades.

V. LOS DATOS PERSONALES TRATADOS EN LOS SISTEMAS DE TRATAMIENTOS Y/O BASE DE DATOS PERSONALES SON LOS SIGUIENTES:

- Nombres y Apellidos
- Clave Única de Registro de Población
- Domicilio

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

- Número de Teléfono Fijo o Celular
- Correo Electrónico
- Nivel Educativo
- Estado Civil
- Edad
- Género

VI. LA DESCRIPCIÓN DEL SISTEMA DE TRATAMIENTO, SEÑALANDO EL TIPO DE SOPORTE Y LAS CARACTERÍSTICAS DEL LUGAR DONDE SE RESGUARDAN.

Descripción del Sistema de Tratamiento	Tipo de Soporte	Características del lugar de resguardo
Seguimiento Académico de Docentes: Registro y control de la actividad académica del personal docente de los diferentes programas educativos (evaluaciones, desempeño, cumplimiento de programas de estudio).	Documental (físico) y Electrónico.	[REDACTED]
Consulta de Datos Personales de Alumnos: Acceso y consulta de información de los estudiantes de la carrera (datos de identificación, historial académico, avance curricular) para fines de gestión y seguimiento académico.	Electrónico (Mindbox) y consulta documental de expedientes en casos específicos.	[REDACTED]
Integración y Resguardo de canalizaciones de asesorías académicas en materias de ciencias básicas (canalizaciones, reporte de evidencia)	Documental (físico) y Electrónico (copias digitalizadas).	[REDACTED]

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

--	--	--

VII. LOS CONTROLES Y MECANISMOS DE SEGURIDAD PARA LAS TRANSFERENCIAS QUE, EN SU CASO, SE EFECTÚEN.

Con base en la información proporcionada por el Departamento de Ciencias Básicas, no se documentan transferencias específicas de datos personales a terceros dentro de los tratamientos descritos. El área realiza seguimiento académico del personal docente y consulta de información de estudiantes mediante MindBox y, en casos específicos, expedientes documentales. Cuando el cumplimiento de sus atribuciones requiera comunicar información a otra área institucional, deberá utilizarse únicamente la información necesaria y los medios institucionales autorizados, manteniendo el control de acceso y la confidencialidad.

VIII. EL RESGUARDO DE LOS SOPORTES FÍSICOS DE LOS DATOS PERSONALES.

Los expedientes físicos se encuentran resguardos y en custodia de los responsables del sistema de tratamiento de los datos personales en el área asignada para tal efecto.

IX. LAS BITÁCORAS DE ACCESO Y VULNERACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES.

Los datos que se registran en la Bitácora de acceso (anexo 1) son los siguientes:

- Quien accede a los datos personales, cargo y adscripción;
- Fecha y hora en la que se realiza el acceso o se intenta el mismo, así como fecha y hora de salida;
- Propósito del acceso;
- Firma de quien autoriza el acceso.

➤ Los datos que se registran en la Bitácora de vulneraciones (anexo 2) son los siguientes:

- Fecha y hora de la vulneración;
- Motivo de la vulneración;
- Acciones correctivas y definitivas implementadas;
- Persona que resolvió la vulneración;
- Fecha y hora de notificación de la vulneración a los titulares de los datos personales comprometidos o afectados y a la Autoridad Garante en materia de protección de datos personales; y
- Los oficios, documentos, expedientes, estantes o archiveros dañados y los recuperados.

X. EL ANÁLISIS DE RIESGOS.



[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

XI. EL ANÁLISIS DE BRECHA.

✓	[REDACTED]
✓	[REDACTED]
✓	[REDACTED]
✓	[REDACTED]
✓	[REDACTED]
✓	[REDACTED]

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de la Ley de Transparencia y Acceso a la Información Pública (LGTAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de información, así como para la elaboración de versiones públicas.”



✓

XII. LA GESTIÓN DE VULNERACIONES.

En caso de ocurrir alguna vulneración deberá registrarse en la bitácora de vulneraciones, además de informar de forma inmediata a la persona titular de los datos personales y a la Unidad de Transparencia.

XIII. LAS MEDIDAS DE SEGURIDAD FÍSICAS APLICADAS A LAS INSTALACIONES.

XIV. LOS CONTROLES DE IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS.

XV. LOS PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS PERSONALES.

XVI. EL PLAN DE CONTINGENCIA.

➤
➤
➤

- [REDACTED]
- [REDACTED]
- [REDACTED]

XVII. LAS TÉCNICAS UTILIZADAS PARA LA SUPRESIÓN Y BORRADO SEGURO DE LOS DATOS PERSONALES.

- Destrucción segura de documentos: Los documentos y otros medios físicos no deben simplemente desecharse una vez que ya no se utilizan, sino destruirse por ejemplo con triturador o incinerado...
- Destrucción segura de información en equipo de cómputo y medios de almacenamiento electrónico: Herramientas de software que borran archivos electrónicos específicos o dispositivos completos...
- Fijar periodos de retención y destrucción de información: Identificar de manera regular toda la información que ya no es de utilidad...
- Tomar precauciones con los procedimientos de reutilización: Bajo ninguna circunstancia deberían utilizarse documentos con datos personales como papel de reúso.

XVIII. EL PLAN DE TRABAJO.

[REDACTED]

XIX. LOS MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD.

Monitorear y revisar continuamente los riesgos, amenazas, vulnerabilidades, incidentes, modificaciones necesarias a los activos y nuevas amenazas.

XX. EL PROGRAMA GENERAL DE CAPACITACIÓN.

- a) Sensibilización en materia de Protección de Datos Personales en el Departamento de Ciencias Básicas y su importancia en el entorno laboral.
- b) Capacitación a las personas servidoras públicas asignadas como enlaces en materia de datos personales respecto a los mecanismos, medios y procedimientos disponibles para ejercer los Derechos ARCO y Portabilidad de los datos personales.
- c) Concientizar a las personas servidoras públicas que dentro de sus funciones y obligaciones se encuentren la de recabar los datos personales, respecto a la importancia de informar a la

persona titular de los datos personales a través del Aviso de Privacidad, el tratamiento de los mismos.

d) Informar a las personas servidoras públicas que cuentan con la facultad de autorizar, acordar y/o decidir en el Órgano Administrativo, respecto a la implementación de las medidas de seguridad administrativa, técnicas y físicas, para la protección de los datos personales.

e) Asesorar a las personas servidoras públicas que dentro de sus atribuciones se encuentre el tratamiento de los datos personales, respecto a la implementación del Documento de Seguridad, para la protección de los datos personales.

ANEXO 1: BITÁCORA DE ACCESO A LOS DATOS PERSONALES

Órgano Administrativo (o área generadora/resguardante): Departamento de Ciencias Básicas.

Responsable del Archivo: Diego Armando Santos Roque, Jefe de Departamento de Ciencias Básicas.

No.	Nombres y Apellidos	Cargo y Adscripción	Fecha y Hora de Acceso	Fecha y Hora de Salida	Propósito del Acceso	Firma

ANEXO 2: Bitácora de vulneraciones a la seguridad de los Datos Personales

Órgano Administrativo (o área generadora/resguardante): Departamento de Ciencias Básicas.

Responsable del Archivo: Diego Armando Santos Roque, Jefe de Departamento de Ciencias Básicas.

No.	Fecha y Hora Vulneración	Motivo Vulneración	Acciones Correctivas	Acciones Definitivas	Fecha Notificación Titular	Fecha Notificación Autoridad	Datos / Expedientes Afectados

DIVISIÓN DE INGENIERÍA EN DESARROLLO COMUNITARIO

II. NOMBRES DE LOS SISTEMAS DE TRATAMIENTO

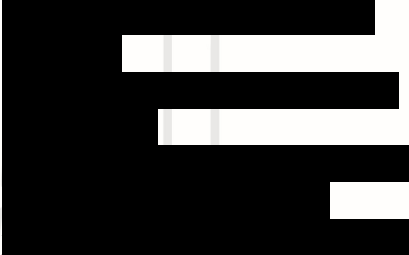
Los datos personales en posesión de la División de Ingeniería en Desarrollo Comunitario del Instituto Tecnológico Superior de Cintalapa son sometidos a los siguientes tratamientos, derivados de las funciones y actividades descritas en su Documento de Seguridad:

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

1. Seguimiento académico del personal docente adscrito a la División de Ingeniería en Desarrollo Comunitario, incluyendo carga horaria, evaluaciones, desempeño y cumplimiento de programas de estudio.
2. Consulta de datos personales de los alumnos de Ingeniería en Desarrollo Comunitario, incluyendo datos de identificación, historial académico y avance curricular, para fines de gestión y seguimiento académico.
3. Integración y resguardo de los expedientes de residencia profesional y/o Formación Dual de los alumnos, incluyendo informes, cartas de aceptación, evaluaciones de la organización receptora y reportes finales.
4. Registro y control de acceso a los expedientes físicos, electrónicos y sistemas institucionales que contienen datos personales de alumnos y docentes.
5. Registro, seguimiento y documentación de vulneraciones a la seguridad de los datos personales mediante las bitácoras correspondientes.

III. EL NOMBRE, CARGO Y ADSCRIPCIÓN DEL ADMINISTRADOR DEL SISTEMA DE TRATAMIENTO.

Los responsables del tratamiento de los datos personales en las Jefaturas de División, son los que se describen a continuación:

Responsable	Cargo	Órgano Administrativo	Tratamiento
	Jefe de División de Ingeniería en Desarrollo Comunitario	Instituto Superior Tecnológico de Cintalapa	

	Coordinador de Carrera de Ingeniería en Desarrollo Comunitario	Instituto Superior Tecnológico de Cintalapa	
--	--	---	--

IV. LAS FUNCIONES Y OBLIGACIONES DEL RESPONSABLE Y TODAS LAS PERSONAS SERVIDORAS PÚBLICAS QUE TRATEN DATOS PERSONALES.

Funciones:

- Tratar los datos personales con responsabilidad y las medidas de seguridad que se hayan establecido para tal fin.
- Resguardar los datos personales a los que tengan acceso en el ejercicio de sus atribuciones.
- Verificar que el inventario de datos personales y de los sistemas de tratamiento de los mismos, a los que tienen acceso, se encuentren actualizados.
- En caso de que se presente algún incidente de vulneración de seguridad de los datos personales y/o de los sistemas de tratamiento de los mismos, informar sin dilación alguna a la persona titular, a la Autoridad Garante y llevar el registro de los hechos.

Obligaciones:

- Llevar a cabo permanentemente las medidas de seguridad necesarias para la protección de los datos personales, evitando daño, pérdida, alteración, destrucción o uso, acceso o tratamiento no autorizado, así como también garantizar la confidencialidad, integridad y disponibilidad de los mismos.
- Acatar los mecanismos para asegurar que los datos personales a los que tengan acceso en el ejercicio de sus atribuciones no se difundan, distribuyan o comercialicen.
- Guardar confidencialidad sobre la información que se conozca en el desarrollo de sus actividades.

V. LOS DATOS PERSONALES TRATADOS EN LOS SISTEMAS DE TRATAMIENTOS Y/O BASE DE DATOS PERSONALES SON LOS SIGUIENTES:

- Nombres y Apellidos
- Clave Única de Registro de Población
- Domicilio
- Número de Teléfono Fijo o Celular

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

- Correo Electrónico
- Nivel Educativo
- Estado Civil
- Edad
- Género

VI. LA DESCRIPCIÓN DEL SISTEMA DE TRATAMIENTO, SEÑALANDO EL TIPO DE SOPORTE Y LAS CARACTERÍSTICAS DEL LUGAR DONDE SE RESGUARDAN.

Descripción del Sistema de Tratamiento	Tipo de Soporte	Características del lugar de resguardo
Seguimiento Académico de Docentes: Registro y control de la actividad académica del personal docente adscrito a la División de Ingeniería en Desarrollo Comunitario (carga horaria, evaluaciones, desempeño, cumplimiento de programas de estudio).	Documental (físico) y Electrónico.	
Consulta de Datos Personales de Alumnos: Acceso y consulta de información de los estudiantes de la carrera (datos de identificación, historial académico, avance curricular) para fines de gestión y seguimiento académico.	Electrónico (Mindbox) y consulta documental de expedientes en casos específicos.	
Integración y Resguardo de Expedientes de Residencia Profesional y/o formación: Compilación y custodia de la documentación generada por los alumnos durante su proceso de residencia profesional (informes, cartas	Documental (físico) y Electrónico (copias digitalizadas).	

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

de aceptación, evaluaciones de la empresa receptora, reportes finales).

VII. LOS CONTROLES Y MECANISMOS DE SEGURIDAD PARA LAS TRANSFERENCIAS QUE, EN SU CASO, SE EFECTÚEN.

En la información proporcionada por la División de Ingeniería en Desarrollo Comunitario no se describe un mecanismo específico de transferencia de datos personales. Los tratamientos documentados comprenden seguimiento académico de docentes, consulta de información de estudiantes y expedientes de Residencia Profesional y/o Formación Dual. Cuando dentro de estos procesos resulte necesario comunicar información a un área institucional o a una organización receptora, la División deberá limitar el envío a los datos necesarios para el trámite, utilizar medios institucionales autorizados y mantener registro y control de las personas que intervengan en el acceso.

VIII. EL RESGUARDO DE LOS SOPORTES FÍSICOS DE LOS DATOS PERSONALES.

Los expedientes físicos se encuentran resguardos y en custodia de los responsables del sistema de tratamiento de los datos personales en el área asignada para tal efecto.

IX. LAS BITÁCORAS DE ACCESO Y VULNERACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES.

Los datos que se registran en la Bitácora de acceso (anexo 1) son los siguientes:

- Quien accede a los datos personales, cargo y adscripción;
- Fecha y hora en la que se realiza el acceso o se intenta el mismo, así como fecha y hora de salida;
- Propósito del acceso;
- Firma de quien autoriza el acceso.

Los datos que se registran en la Bitácora de vulneraciones (anexo 2) son los siguientes:

- Fecha y hora de la vulneración;
- Motivo de la vulneración;
- Acciones correctivas y definitivas implementadas;
- Persona que resolvió la vulneración;
- Fecha y hora de notificación de la vulneración a los titulares de los datos personales comprometidos o afectados y a la Autoridad Garante en materia de protección de datos personales;

[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

XI. EL ANÁLISIS DE BRECHA.

- [REDACTED]
- [REDACTED]
 - [REDACTED]

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

XII. LA GESTIÓN DE VULNERACIONES.

En caso de ocurrir alguna vulneración deberá registrarse en la bitácora de vulneraciones, además de informar de forma inmediata a la persona titular de los datos personales y a la Unidad de Transparencia.

XIII. LAS MEDIDAS DE SEGURIDAD FÍSICAS APLICADAS A LAS INSTALACIONES.

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

XIV. LOS CONTROLES DE IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS.

- [REDACTED]

XV. LOS PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS PERSONALES.

- [REDACTED]

XVI. EL PLAN DE CONTINGENCIA.

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

XVII. LAS TÉCNICAS UTILIZADAS PARA LA SUPRESIÓN Y BORRADO SEGURO DE LOS DATOS PERSONALES.

- **Destrucción segura de documentos:** Los documentos y otros medios físicos no deben simplemente desecharse una vez que ya no se utilizan, sino destruirse por ejemplo con triturador o incinerado...
- **Destrucción segura de información en equipo de cómputo y medios de almacenamiento electrónico:** Herramientas de software que borran archivos electrónicos específicos o dispositivos completos...
- **Fijar periodos de retención y destrucción de información:** Identificar de manera regular toda la información que ya no es de utilidad...
- **Tomar precauciones con los procedimientos de reutilización:** Bajo ninguna circunstancia deberían utilizarse documentos con datos personales como papel de reúso.

XVIII. EL PLAN DE TRABAJO.

[REDACTED]

XIX. LOS MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD.

Monitorear y revisar continuamente los riesgos, amenazas, vulnerabilidades, incidentes, modificaciones necesarias a los activos y nuevas amenazas.

XX. EL PROGRAMA GENERAL DE CAPACITACIÓN.

- a) Sensibilización en materia de Protección de Datos Personales en la Jefatura de División y su importancia en el entorno laboral.
- b) Capacitación a las personas servidoras públicas asignadas como enlaces en materia de datos personales respecto a los mecanismos, medios y procedimientos disponibles para ejercer los Derechos ARCO y Portabilidad de los datos personales.
- c) Concientizar a las personas servidoras públicas que dentro de sus funciones y obligaciones se encuentren la de recabar los datos personales, respecto a la importancia de informar a la

persona titular de los datos personales a través del Aviso de Privacidad, el tratamiento de los mismos.

d) Informar a las personas servidoras públicas que cuentan con la facultad de autorizar, acordar y/o decidir en el Órgano Administrativo, respecto a la implementación de las medidas de seguridad administrativa, técnicas y físicas, para la protección de los datos personales.

e) Asesorar a las personas servidoras públicas que dentro de sus atribuciones se encuentre el tratamiento de los datos personales, respecto a la implementación del Documento de Seguridad, para la protección de los datos personales.

ANEXO 1: BITÁCORA DE ACCESO A LOS DATOS PERSONALES

Órgano Administrativo (o área generadora/resguardante): División de Ingeniería en Desarrollo Comunitario.

Responsable del Archivo: Pablo Ramiro Cruz de la Cruz, Jefe de División de Ingeniería en Desarrollo Comunitario.

No.	Nombres y Apellidos	Cargo y Adscripción	Fecha y Hora de Acceso	Fecha y Hora de Salida	Propósito del Acceso	Firma

ANEXO 2: BITÁCORA DE VULNERACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES

Órgano Administrativo (o área generadora/resguardante): División de Ingeniería en Desarrollo Comunitario.

Responsable del Archivo: Pablo Ramiro Cruz de la Cruz, Jefe de División de Ingeniería en Desarrollo Comunitario.

N o.	Fecha y Hora Vulneración	Motivo Vulneración	Acciones Correctivas	Acciones Definitivas	Fecha Notificación Titular	Fecha Notificación Autoridad	Datos / Expedientes Afectados

DIVISIÓN DE INGENIERÍA CIVIL

II. NOMBRES DE LOS SISTEMAS DE TRATAMIENTO

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

Los datos personales en posesión de la División de Ingeniería Civil del Instituto Tecnológico Superior de Cintalapa son sometidos a los siguientes tratamientos, derivados de las funciones y actividades descritas en su Documento de Seguridad:

1. Seguimiento académico del personal docente adscrito a la División de Ingeniería Civil, incluyendo carga horaria, evaluaciones, desempeño y cumplimiento de programas de estudio.
2. Consulta de datos personales de los alumnos de Ingeniería Civil, incluyendo datos de identificación, historial académico y avance curricular, para fines de gestión y seguimiento académico.
3. Integración y resguardo de los expedientes de residencia profesional y/o Formación Dual de los alumnos, incluyendo informes, cartas de aceptación, evaluaciones de la empresa receptora y reportes finales.
4. Registro y control de acceso a los expedientes físicos, electrónicos y sistemas institucionales que contienen datos personales de alumnos y docentes.
5. Registro, seguimiento y documentación de vulneraciones a la seguridad de los datos personales mediante las bitácoras correspondientes.

III. EL NOMBRE, CARGO Y ADSCRIPCIÓN DEL ADMINISTRADOR DEL SISTEMA DE TRATAMIENTO.

Los responsables del tratamiento de los datos personales en las Jefaturas de División, son los que se describen a continuación:

Responsable	Cargo	Órgano Administrativo	Tratamiento
[REDACTED]	Jefe de División	Instituto Superior Tecnológico de Cintalapa	[REDACTED]

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTIAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

	Coordinadora de Carrera	Instituto Superior Tecnológico de Cintalapa	
--	-------------------------	---	--

IV. LAS FUNCIONES Y OBLIGACIONES DEL RESPONSABLE Y TODAS LAS PERSONAS SERVIDORAS PÚBLICAS QUE TRATEN DATOS PERSONALES.

Funciones:

- Tratar los datos personales con responsabilidad y las medidas de seguridad que se hayan establecido para tal fin.
- Resguardar los datos personales a los que tengan acceso en el ejercicio de sus atribuciones.
- Verificar que el inventario de datos personales y de los sistemas de tratamiento de los mismos, a los que tienen acceso, se encuentren actualizados.
- En caso de que se presente algún incidente de vulneración de seguridad de los datos personales y/o de los sistemas de tratamiento de los mismos, informar sin dilación alguna a la persona titular, a la Autoridad Garante y llevar el registro de los hechos.

Obligaciones:

- Llevar a cabo permanentemente las medidas de seguridad necesarias para la protección de los datos personales, evitando daño, pérdida, alteración, destrucción o uso, acceso o tratamiento no autorizado, así como también garantizar la confidencialidad, integridad y disponibilidad de los mismos.
- Acatar los mecanismos para asegurar que los datos personales a los que tengan acceso en el ejercicio de sus atribuciones no se difundan, distribuyan o comercialicen.
- Guardar confidencialidad sobre la información que se conozca en el desarrollo de sus actividades.

V. LOS DATOS PERSONALES TRATADOS EN LOS SISTEMAS DE TRATAMIENTOS Y/O BASE DE DATOS PERSONALES SON LOS SIGUIENTES:

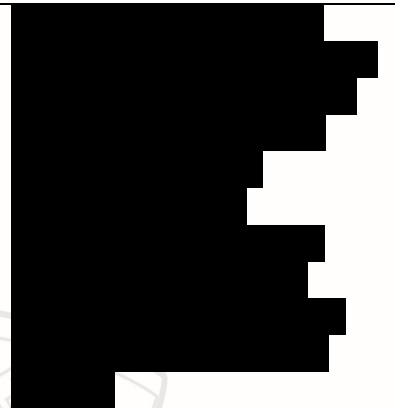
“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPECHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

- Nombres y Apellidos
- Clave Única de Registro de Población
- Domicilio
- Número de Teléfono Fijo o Celular
- Correo Electrónico
- Nivel Educativo
- Estado Civil
- Edad
- Género

VI. LA DESCRIPCIÓN DEL SISTEMA DE TRATAMIENTO, SEÑALANDO EL TIPO DE SOPORTE Y LAS CARACTERÍSTICAS DEL LUGAR DONDE SE RESGUARDAN.

Descripción del Sistema de Tratamiento	Tipo de Soporte	Características del lugar de resguardo
Seguimiento Académico de Docentes: Registro y control de la actividad académica del personal docente adscrito a la División de Ingeniería Civil (carga horaria, evaluaciones, desempeño, cumplimiento de programas de estudio).	Documental (físico) y Electrónico.	[Redacted]
Consulta de Datos Personales de Alumnos: Acceso y consulta de información de los estudiantes de la carrera (datos de identificación, historial académico, avance curricular) para fines de gestión y seguimiento académico.	Electrónico (Mindbox) y consulta documental de expedientes en casos específicos.	[Redacted]

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPECIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

Integración y Resguardo de Expedientes de Residencia Profesional y/o formación : Compilación y custodia de la documentación generada por los alumnos durante su proceso de residencia profesional (informes, cartas de aceptación, evaluaciones de la empresa receptora, reportes finales).	Documental (físico) y Electrónico (copias digitalizadas).	
---	---	---

VII. LOS CONTROLES Y MECANISMOS DE SEGURIDAD PARA LAS TRANSFERENCIAS QUE, EN SU CASO, SE EFECTÚEN.

En la información proporcionada por la División de Ingeniería Civil no se describe un mecanismo específico de transferencia de datos personales. Los tratamientos documentados comprenden seguimiento académico de docentes, consulta de información de estudiantes y expedientes de Residencia Profesional y/o Formación Dual. Cuando dentro de estos procesos resulte necesario comunicar información a un área institucional o a una empresa receptora, la División deberá limitar el envío a los datos necesarios para el trámite, utilizar medios institucionales autorizados y mantener registro y control de las personas que intervengan en el acceso.

VIII. EL RESGUARDO DE LOS SOPORTES FÍSICOS DE LOS DATOS PERSONALES.

Los expedientes físicos se encuentran resguardados y en custodia de los responsables del sistema de tratamiento de los datos personales en el área asignada para tal efecto.

IX. LAS BITÁCORAS DE ACCESO Y VULNERACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES.

Los datos que se registran en la Bitácora de acceso (anexo 1) son los siguientes:

- Quien accede a los datos personales, cargo y adscripción;
- Fecha y hora en la que se realiza el acceso o se intenta el mismo, así como fecha y hora de salida;
- Propósito del acceso;
- Firma de quien autoriza el acceso.

Los datos que se registran en la Bitácora de vulneraciones (anexo 2) son los siguientes:

- Fecha y hora de la vulneración;

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIPI) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

- Motivo de la vulneración;
- Acciones correctivas y definitivas implementadas;
- Persona que resolvió la vulneración;
- Fecha y hora de notificación de la vulneración a los titulares de los datos personales comprometidos o afectados y a la Autoridad Garante en materia de protección de datos personales; y
- Los oficios, documentos, expedientes, estantes o archiveros dañados y los recuperados.

X. EL ANÁLISIS DE RIESGOS.

[Redacted]		
➤	[Redacted]	[Redacted]
	[Redacted]	[Redacted]
➤	[Redacted]	[Redacted]
	[Redacted]	[Redacted]
➤	[Redacted]	[Redacted]
➤	[Redacted]	[Redacted]
➤	[Redacted]	[Redacted]
➤	[Redacted]	[Redacted]
	[Redacted]	[Redacted]
	[Redacted]	[Redacted]
➤	[Redacted]	[Redacted]
➤	[Redacted]	[Redacted]
	[Redacted]	[Redacted]

Amenaza	Vulnerabilidades	Posibles consecuencias
[Redacted]	[Redacted]	[Redacted]

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAI) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”



- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

XII. LA GESTIÓN DE VULNERACIONES.

En caso de ocurrir alguna vulneración deberá registrarse en la bitácora de vulneraciones, además de informar de forma inmediata a la persona titular de los datos personales y a la Autoridad Garante.

XIII. LAS MEDIDAS DE SEGURIDAD FÍSICAS APLICADAS A LAS INSTALACIONES.

[REDACTED]

XIV. LOS CONTROLES DE IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS.

[REDACTED]

XV. LOS PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS PERSONALES.

[REDACTED]

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAI) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPECHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

XVI. EL PLAN DE CONTINGENCIA.

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

XVII. LAS TÉCNICAS UTILIZADAS PARA LA SUPRESIÓN Y BORRADO SEGURO DE LOS DATOS PERSONALES.

- Destrucción segura de documentos: Los documentos y otros medios físicos no deben simplemente desecharse una vez que ya no se utilizan, sino destruirse por ejemplo con triturador o incinerado.
- Destrucción segura de información en equipo de cómputo y medios de almacenamiento electrónico: Herramientas de software que borran archivos electrónicos específicos o dispositivos completos.
- Fijar periodos de retención y destrucción de información: Identificar de manera regular toda la información que ya no es de utilidad.
- Tomar precauciones con los procedimientos de reutilización: Bajo ninguna circunstancia deberían utilizarse documentos con datos personales como papel de reúso.

XVIII. EL PLAN DE TRABAJO.

[REDACTED]

XIX. LOS MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD.

Monitorear y revisar continuamente los riesgos, amenazas, vulnerabilidades, incidentes, modificaciones necesarias a los activos y nuevas amenazas.

XX. EL PROGRAMA GENERAL DE CAPACITACIÓN.

a) Sensibilización en materia de Protección de Datos Personales en la Jefatura de División y su importancia en el entorno laboral.

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIPI) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

- b) Capacitación a las personas servidoras públicas asignadas como enlaces en materia de datos personales respecto a los mecanismos, medios y procedimientos disponibles para ejercer los Derechos ARCO y Portabilidad de los datos personales.
- c) Concientizar a las personas servidoras públicas que dentro de sus funciones y obligaciones se encuentren la de recabar los datos personales, respecto a la importancia de informar a la persona titular de los datos personales a través del Aviso de Privacidad, el tratamiento de los mismos.
- d) Informar a las personas servidoras públicas que cuentan con la facultad de autorizar, acordar y/o decidir en el Órgano Administrativo, respecto a la implementación de las medidas de seguridad administrativa, técnicas y físicas, para la protección de los datos personales.
- e) Asesorar a las personas servidoras públicas que dentro de sus atribuciones se encuentre el tratamiento de los datos personales, respecto a la implementación del Documento de Seguridad, para la protección de los datos personales.

ANEXO 1: Bitácora de acceso a los Datos Personales

Órgano Administrativo (o área generadora/resguardante): División de Ingeniería Civil.

Responsable del Archivo:

No.	Nombres y Apellidos	Cargo y Adscripción	Fecha y Hora de Acceso	Fecha y Hora de Salida	Propósito del Acceso	Firma

ANEXO 2: Bitácora de vulneraciones a la seguridad de los Datos Personales

Órgano Administrativo (o área generadora/resguardante): División de Ingeniería Civil.

Responsable del Archivo: Pablo Díaz Zebadúa, Jefe de División de Ingeniería Civil.

No.	Fecha y Hora Vulneración	Motivo Vulneración	Acciones Correctivas	Acciones Definitivas	Fecha Notificación Titular	Fecha Notificación Autoridad	Datos / Expedientes Afectados

DIVISIÓN DE INGENIERÍA EN ENERGÍAS RENOVABLES

II. NOMBRES DE LOS SISTEMAS DE TRATAMIENTO

Los datos personales en posesión de la División de Ingeniería en Energías Renovables del Instituto Tecnológico Superior de Cintalapa son sometidos a los siguientes tratamientos, derivados de las funciones y actividades descritas en su Documento de Seguridad:

1. Seguimiento académico del personal docente adscrito a la División de Ingeniería en Energías Renovables, incluyendo carga horaria, evaluaciones, desempeño y cumplimiento de programas de estudio.
2. Consulta de datos personales de los alumnos de Ingeniería en Energías Renovables, incluyendo datos de identificación, historial académico y avance curricular, para fines de gestión y seguimiento académico.
3. Integración y resguardo de los expedientes de residencia profesional y/o Formación Dual de los alumnos, incluyendo informes, cartas de aceptación, evaluaciones de la empresa receptora y reportes finales.
4. Registro y control de acceso a los expedientes físicos, electrónicos y sistemas institucionales que contienen datos personales de alumnos y docentes.
5. Registro, seguimiento y documentación de vulneraciones a la seguridad de los datos personales mediante las bitácoras correspondientes.

III. EL NOMBRE, CARGO Y ADSCRIPCIÓN DEL ADMINISTRADOR DEL SISTEMA DE TRATAMIENTO.

Los responsables del tratamiento de los datos personales en las Jefaturas de División, son los que se describen a continuación:

Responsable	Cargo	Órgano Administrativo	Tratamiento
[REDACTED]	Jefe de División	Instituto Superior Tecnológico de Cintalapa	[REDACTED]
[REDACTED]	Coordinadora de Carrera	Instituto Superior Tecnológico de Cintalapa	[REDACTED]

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIPI) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPECHS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

IV. LAS FUNCIONES Y OBLIGACIONES DEL RESPONSABLE Y TODAS LAS PERSONAS SERVIDORAS PÚBLICAS QUE TRATEN DATOS PERSONALES.

Funciones:

- Tratar los datos personales con responsabilidad y las medidas de seguridad que se hayan establecido para tal fin.
- Resguardar los datos personales a los que tengan acceso en el ejercicio de sus atribuciones.
- Verificar que el inventario de datos personales y de los sistemas de tratamiento de los mismos, a los que tienen acceso, se encuentren actualizados.
- En caso de que se presente algún incidente de vulneración de seguridad de los datos personales y/o de los sistemas de tratamiento de los mismos, informar sin dilación alguna a la persona titular, a la Autoridad Garante y llevar el registro de los hechos.

Obligaciones:

- Llevar a cabo permanentemente las medidas de seguridad necesarias para la protección de los datos personales, evitando daño, pérdida, alteración, destrucción o uso, acceso o tratamiento no autorizado, así como también garantizar la confidencialidad, integridad y disponibilidad de los mismos.
- Acatar los mecanismos para asegurar que los datos personales a los que tengan acceso en el ejercicio de sus atribuciones no se difundan, distribuyan o comercialicen.
- Guardar confidencialidad sobre la información que se conozca en el desarrollo de sus actividades.

V. LOS DATOS PERSONALES TRATADOS EN LOS SISTEMAS DE TRATAMIENTOS Y/O BASE DE DATOS PERSONALES SON LOS SIGUIENTES:

- Nombres y Apellidos
- Clave Única de Registro de Población
- Domicilio
- Número de Teléfono Fijo o Celular
- Correo Electrónico
- Nivel Educativo
- Estado Civil
- Edad

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

- Género

VI. LA DESCRIPCIÓN DEL SISTEMA DE TRATAMIENTO, SEÑALANDO EL TIPO DE SOPORTE Y LAS CARACTERÍSTICAS DEL LUGAR DONDE SE RESGUARDAN.

Descripción del Sistema de Tratamiento	Tipo de Soporte	Características del lugar de resguardo
Seguimiento Académico de Docentes: Registro y control de la actividad académica del personal docente adscrito a la División de Ingeniería en Energías Renovables (carga horaria, evaluaciones, desempeño, cumplimiento de programas de estudio).	Documental (físico) y Electrónico.	[REDACTED]
Consulta de Datos Personales de Alumnos: Acceso y consulta de información de los estudiantes de la carrera (datos de identificación, historial académico, avance curricular) para fines de gestión y seguimiento académico.	Electrónico (Mindbox) y consulta documental de expedientes en casos específicos.	[REDACTED]
Integración y Resguardo de Expedientes de Residencia Profesional y/o formación : Compilación y custodia de la documentación generada por los alumnos durante su proceso de residencia profesional (informes, cartas de aceptación, evaluaciones de la empresa receptora, reportes finales).	Documental (físico) y Electrónico (copias digitalizadas).	[REDACTED]

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIIP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

VII. LOS CONTROLES Y MECANISMOS DE SEGURIDAD PARA LAS TRANSFERENCIAS QUE, EN SU CASO, SE EFECTÚEN.

En la información proporcionada por la División de Ingeniería en Energías Renovables no se describe un mecanismo específico de transferencia de datos personales. Los tratamientos documentados comprenden seguimiento académico de docentes, consulta de información de estudiantes y expedientes de Residencia Profesional y/o Formación Dual. Cuando dentro de estos procesos resulte necesario comunicar información a un área institucional o a una organización receptora, la División deberá limitar el envío a los datos necesarios para el trámite, utilizar medios institucionales autorizados y mantener registro y control de las personas que intervengan en el acceso.

VIII. EL RESGUARDO DE LOS SOPORTES FÍSICOS DE LOS DATOS PERSONALES.

Los expedientes físicos se encuentran resguardos y en custodia de los responsables del sistema de tratamiento de los datos personales en el área asignada para tal efecto.

IX. LAS BITÁCORAS DE ACCESO Y VULNERACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES.

Los datos que se registran en la Bitácora de acceso (anexo 1) son los siguientes:

- Quien accede a los datos personales, cargo y adscripción;
- Fecha y hora en la que se realiza el acceso o se intenta el mismo, así como fecha y hora de salida;
- Propósito del acceso;
- Firma de quien autoriza el acceso.

Los datos que se registran en la Bitácora de vulneraciones (anexo 2) son los siguientes:

- Fecha y hora de la vulneración;
- Motivo de la vulneración;
- Acciones correctivas y definitivas implementadas;
- Persona que resolvió la vulneración;
- Fecha y hora de notificación de la vulneración a los titulares de los datos personales comprometidos o afectados y a la Autoridad Garante en materia de protección de datos personales; y
- Los oficios, documentos, expedientes, estantes o archiveros dañados y los recuperados.

X. EL ANÁLISIS DE RIESGOS.

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”



[Redacted]		
[Redacted]		
➤	[Redacted]	
➤	[Redacted]	
[Redacted]		
➤	[Redacted]	
➤	[Redacted]	
➤	[Redacted]	
➤	[Redacted]	
[Redacted]		
[Redacted]		
➤	[Redacted]	
➤	[Redacted]	
[Redacted]		
Amenaza	Vulnerabilidades	Posibles consecuencias
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAI) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”



➤ [REDACTED]

XII. LA GESTIÓN DE VULNERACIONES.

En caso de ocurrir alguna vulneración deberá registrarse en la bitácora de vulneraciones, además de informar de forma inmediata a la persona titular de los datos personales y a la Autoridad Garante.

XIII. LAS MEDIDAS DE SEGURIDAD FÍSICAS APLICADAS A LAS INSTALACIONES.

[REDACTED]

XIV. LOS CONTROLES DE IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS.

[REDACTED]

XV. LOS PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS PERSONALES.

[REDACTED]

XVI. EL PLAN DE CONTINGENCIA.

➤ [REDACTED]
➤ [REDACTED]
➤ [REDACTED]
➤ [REDACTED]
➤ [REDACTED]
➤ [REDACTED]

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAI) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LEIAPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”



XVII. LAS TÉCNICAS UTILIZADAS PARA LA SUPRESIÓN Y BORRADO SEGURO DE LOS DATOS PERSONALES.

- Destrucción segura de documentos: Los documentos y otros medios físicos no deben simplemente desecharse una vez que ya no se utilizan, sino destruirse por ejemplo con triturador o incinerado.
- Destrucción segura de información en equipo de cómputo y medios de almacenamiento electrónico: Herramientas de software que borran archivos electrónicos específicos o dispositivos completos.
- Fijar periodos de retención y destrucción de información: Identificar de manera regular toda la información que ya no es de utilidad.
- Tomar precauciones con los procedimientos de reutilización: Bajo ninguna circunstancia deberían utilizarse documentos con datos personales como papel de reúso.

XVIII. EL PLAN DE TRABAJO.



XIX. LOS MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD.

Monitorear y revisar continuamente los riesgos, amenazas, vulnerabilidades, incidentes, modificaciones necesarias a los activos y nuevas amenazas.

XX. EL PROGRAMA GENERAL DE CAPACITACIÓN.

- a) Sensibilización en materia de Protección de Datos Personales en la Jefatura de División y su importancia en el entorno laboral.
- b) Capacitación a las personas servidoras públicas asignadas como enlaces en materia de datos personales respecto a los mecanismos, medios y procedimientos disponibles para ejercer los Derechos ARCO y Portabilidad de los datos personales.
- c) Concientizar a las personas servidoras públicas que dentro de sus funciones y obligaciones se encuentren la de recabar los datos personales, respecto a la importancia de informar a la persona titular de los datos personales a través del Aviso de Privacidad, el tratamiento de los mismos.
- d) Informar a las personas servidoras públicas que cuentan con la facultad de autorizar, acordar y/o decidir en el Órgano Administrativo, respecto a la implementación de las medidas de seguridad administrativa, técnicas y físicas, para la protección de los datos personales.
- e) Asesorar a las personas servidoras públicas que dentro de sus atribuciones se encuentre el tratamiento de los datos personales, respecto a la implementación del Documento de Seguridad, para la protección de los datos personales.

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIPI) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

ANEXO 1: Bitácora de acceso a los Datos Personales

Órgano Administrativo (o área generadora/resguardante): División de Ingeniería en Energías Renovables.

Responsable del Archivo: Jesús Iván Rendón Robles, Jefe de División de Ingeniería en Energías Renovables.

No.	Nombres y Apellidos	Cargo y Adscripción	Fecha y Hora de Acceso	Fecha y Hora de Salida	Propósito del Acceso	Firma

ANEXO 2: Bitácora de vulneraciones a la seguridad de los Datos Personales

Órgano Administrativo (o área generadora/resguardante): División de Ingeniería en Energías Renovables.

Responsable del Archivo: Jesús Iván Rendón Robles, Jefe de División de Ingeniería en Energías Renovables.

N o.	Fecha y Hora Vulneración	Motivo Vulneración	Acciones Correctivas	Acciones Definitivas	Fecha Notificación Titular	Fecha Notificación Autoridad	Datos / Expedientes Afectados

DIVISIÓN DE INGENIERÍA INDUSTRIAL

II. NOMBRES DE LOS SISTEMAS DE TRATAMIENTO

Los datos personales en posesión de la División de Ingeniería Industrial del Instituto Tecnológico Superior de Cintalapa son sometidos a los siguientes tratamientos, derivados de las funciones y actividades descritas en su Documento de Seguridad:

1. Seguimiento académico del personal docente adscrito a la División de Ingeniería Industrial, incluyendo carga horaria, evaluaciones, desempeño y cumplimiento de programas de estudio.
2. Consulta de datos personales de los alumnos de Ingeniería Industrial, incluyendo datos de identificación, historial académico y avance curricular, para fines de gestión y seguimiento académico.
3. Integración y resguardo de los expedientes de residencia profesional y/o Formación Dual de los alumnos, incluyendo informes, cartas de aceptación, evaluaciones de la empresa receptora y reportes finales.
4. Registro y control de acceso a los expedientes físicos, electrónicos y sistemas institucionales que contienen datos personales de alumnos y docentes.

5. Registro, seguimiento y documentación de vulneraciones a la seguridad de los datos personales mediante las bitácoras correspondientes.

III. EL NOMBRE, CARGO Y ADSCRIPCIÓN DEL ADMINISTRADOR DEL SISTEMA DE TRATAMIENTO.

Los responsables del tratamiento de los datos personales en las Jefaturas de División, son los que se describen a continuación:

Responsable	Cargo	Órgano Administrativo	Tratamiento
[REDACTED]	Jefe de División	Instituto Superior Tecnológico de Cintalapa	[REDACTED]
[REDACTED]	Coordinador de Carrera	Instituto Superior Tecnológico de Cintalapa	[REDACTED]

IV. LAS FUNCIONES Y OBLIGACIONES DEL RESPONSABLE Y TODAS LAS PERSONAS SERVIDORAS PÚBLICAS QUE TRATEN DATOS PERSONALES.

Funciones:

- Tratar los datos personales con responsabilidad y las medidas de seguridad que se hayan establecido para tal fin.
- Resguardar los datos personales a los que tengan acceso en el ejercicio de sus atribuciones.
- Verificar que el inventario de datos personales y de los sistemas de tratamiento de los mismos, a los que tienen acceso, se encuentren actualizados.
- En caso de que se presente algún incidente de vulneración de seguridad de los datos personales y/o de los sistemas de tratamiento de los mismos, informar sin dilación alguna a la persona titular, a la Autoridad Garante y llevar el registro de los hechos.

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

Obligaciones:

- Llevar a cabo permanentemente las medidas de seguridad necesarias para la protección de los datos personales, evitando daño, pérdida, alteración, destrucción o uso, acceso o tratamiento no autorizado, así como también garantizar la confidencialidad, integridad y disponibilidad de los mismos.
- Acatar los mecanismos para asegurar que los datos personales a los que tengan acceso en el ejercicio de sus atribuciones no se difundan, distribuyan o comercialicen.
- Guardar confidencialidad sobre la información que se conozca en el desarrollo de sus actividades.

V. LOS DATOS PERSONALES TRATADOS EN LOS SISTEMAS DE TRATAMIENTOS Y/O BASE DE DATOS PERSONALES SON LOS SIGUIENTES:

- Nombres y Apellidos
- Clave Única de Registro de Población
- Domicilio
- Número de Teléfono Fijo o Celular
- Correo Electrónico
- Nivel Educativo
- Estado Industrial
- Edad
- Género

VI. LA DESCRIPCIÓN DEL SISTEMA DE TRATAMIENTO, SEÑALANDO EL TIPO DE SOPORTE Y LAS CARACTERÍSTICAS DEL LUGAR DONDE SE RESGUARDAN.

Descripción del Sistema de Tratamiento	Tipo de Soporte	Características del lugar de resguardo
Seguimiento Académico de Docentes: Registro y control de la actividad académica del personal docente adscrito a la División de Ingeniería Industrial (carga horaria, evaluaciones, desempeño,	Documental (físico) y Electrónico.	

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAI) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

cumplimiento de programas de estudio).		
Consulta de Datos Personales de Alumnos: Acceso y consulta de información de los estudiantes de la carrera (datos de identificación, historial académico, avance curricular) para fines de gestión y seguimiento académico.	Electrónico (Mindbox) y consulta documental de expedientes en casos específicos.	
Integración y Resguardo de Expedientes de Residencia Profesional y/o formación: Compilación y custodia de la documentación generada por los alumnos durante su proceso de residencia profesional (informes, cartas de aceptación, evaluaciones de la empresa receptora, reportes finales).	Documental (físico) y Electrónico (copias digitalizadas).	

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTIAIP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

VII. LOS CONTROLES Y MECANISMOS DE SEGURIDAD PARA LAS TRANSFERENCIAS QUE, EN SU CASO, SE EFECTÚEN.

En la información proporcionada por la División de Ingeniería Industrial no se describe un mecanismo específico de transferencia de datos personales. Los tratamientos documentados comprenden seguimiento académico de docentes, consulta de información de estudiantes y expedientes de Residencia Profesional y/o Formación Dual. Cuando dentro de estos procesos resulte necesario comunicar información a un área institucional o a una organización receptora, la División deberá limitar el envío a los datos necesarios para el trámite, utilizar medios institucionales autorizados y mantener registro y control de las personas que intervengan en el acceso.

VIII. EL RESGUARDO DE LOS SOPORTES FÍSICOS DE LOS DATOS PERSONALES.

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

Los expedientes físicos se encuentran resguardos y en custodia de los responsables del sistema de tratamiento de los datos personales en el área asignada para tal efecto.

IX. LAS BITÁCORAS DE ACCESO Y VULNERACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES.

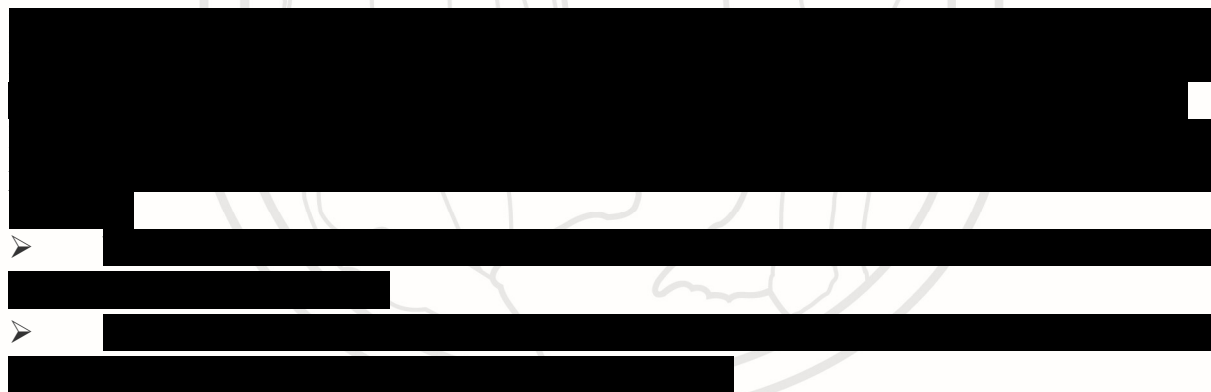
Los datos que se registran en la Bitácora de acceso (anexo 1) son los siguientes:

- Quien accede a los datos personales, cargo y adscripción;
- Fecha y hora en la que se realiza el acceso o se intenta el mismo, así como fecha y hora de salida;
- Propósito del acceso;
- Firma de quien autoriza el acceso.

Los datos que se registran en la Bitácora de vulneraciones (anexo 2) son los siguientes:

- Fecha y hora de la vulneración;
- Motivo de la vulneración;
- Acciones correctivas y definitivas implementadas;
- Persona que resolvió la vulneración;
- Fecha y hora de notificación de la vulneración a los titulares de los datos personales comprometidos o afectados y a la Autoridad Garante en materia de protección de datos personales; y
- Los oficios, documentos, expedientes, estantes o archiveros dañados y los recuperados.

X. EL ANÁLISIS DE RIESGOS.



- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

Amenaza	Vulnerabilidades	Posibles consecuencias
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

XI. EL ANÁLISIS DE BRECHA.

- [REDACTED]

➤ [REDACTED]

[REDACTED]

➤ [REDACTED]

[REDACTED]

➤ [REDACTED]

[REDACTED]

➤ [REDACTED]

[REDACTED]

➤ [REDACTED]

[REDACTED]

XII. LA GESTIÓN DE VULNERACIONES.

En caso de ocurrir alguna vulneración deberá registrarse en la bitácora de vulneraciones, además de informar de forma inmediata a la persona titular de los datos personales y a la Autoridad Garante.

XIII. LAS MEDIDAS DE SEGURIDAD FÍSICAS APLICADAS A LAS INSTALACIONES.

- _____

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”



XIV. LOS CONTROLES DE IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS.

XV. LOS PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS PERSONALES.

XVI. EL PLAN DE CONTINGENCIA.



XVII. LAS TÉCNICAS UTILIZADAS PARA LA SUPRESIÓN Y BORRADO SEGURO DE LOS DATOS PERSONALES.

- Destrucción segura de documentos: Los documentos y otros medios físicos no deben simplemente desecharse una vez que ya no se utilizan, sino destruirse por ejemplo con triturador o incinerado.
- Destrucción segura de información en equipo de cómputo y medios de almacenamiento electrónico: Herramientas de software que borran archivos electrónicos específicos o dispositivos completos.
- Fijar periodos de retención y destrucción de información: Identificar de manera regular toda la información que ya no es de utilidad.

- Tomar precauciones con los procedimientos de reutilización: Bajo ninguna circunstancia deberían utilizarse documentos con datos personales como papel de reúso.

XVIII. EL PLAN DE TRABAJO.

[Redacted content]

XIX. LOS MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD.

Monitorear y revisar continuamente los riesgos, amenazas, vulnerabilidades, incidentes, modificaciones necesarias a los activos y nuevas amenazas.

XX. EL PROGRAMA GENERAL DE CAPACITACIÓN.

- Sensibilización en materia de Protección de Datos Personales en la Jefatura de División y su importancia en el entorno laboral.
- Capacitación a las personas servidoras públicas asignadas como enlaces en materia de datos personales respecto a los mecanismos, medios y procedimientos disponibles para ejercer los Derechos ARCO y Portabilidad de los datos personales.
- Concientizar a las personas servidoras públicas que dentro de sus funciones y obligaciones se encuentren la de recabar los datos personales, respecto a la importancia de informar a la persona titular de los datos personales a través del Aviso de Privacidad, el tratamiento de los mismos.
- Informar a las personas servidoras públicas que cuentan con la facultad de autorizar, acordar y/o decidir en el Órgano Administrativo, respecto a la implementación de las medidas de seguridad administrativa, técnicas y físicas, para la protección de los datos personales.
- Asesorar a las personas servidoras públicas que dentro de sus atribuciones se encuentre el tratamiento de los datos personales, respecto a la implementación del Documento de Seguridad, para la protección de los datos personales.

ANEXO 1: BITÁCORA DE ACCESO A LOS DATOS PERSONALES

Órgano Administrativo (o área generadora/resguardante): División de Ingeniería Industrial.
Responsable del Archivo: Daniel Alberto Zuart Fierros, Jefe de División de Ingeniería Industrial.

No.	Nombres y Apellidos	Cargo y Adscripción	Fecha y Hora de Acceso	Fecha y Hora de Salida	Propósito del Acceso	Firma

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

ANEXO 2: BITÁCORA DE VULNERACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES

Órgano Administrativo (o área generadora/resguardante): División de Ingeniería Industrial.
Responsable del Archivo: Daniel Alberto Zuart Fierros, Jefe de División de Ingeniería Industrial.

N o.	Fecha y Hora Vulneración	Motivo Vulneración	Acciones Correctivas	Acciones Definitivas	Fecha Notificación Titular	Fecha Notificación Autoridad	Datos / Expedientes Afectados

DIVISIÓN DE INGENIERÍA EN INDUSTRIAS ALIMENTARIAS

II. NOMBRES DE LOS SISTEMAS DE TRATAMIENTO

Los datos personales en posesión de la División de Ingeniería en Industrias Alimentarias del Instituto Tecnológico Superior de Cintalapa son sometidos a los siguientes tratamientos, derivados de las funciones y actividades descritas en su Documento de Seguridad:

1. Seguimiento académico del personal docente adscrito a la División de Ingeniería en Industrias Alimentarias, incluyendo carga horaria, evaluaciones, desempeño y cumplimiento de programas de estudio.
2. Consulta de datos personales de los alumnos de Ingeniería en Industrias Alimentarias, incluyendo datos de identificación, historial académico y avance curricular, para fines de gestión y seguimiento académico.
3. Integración y resguardo de los expedientes de residencia profesional y/o Formación Dual de los alumnos, incluyendo informes, cartas de aceptación, evaluaciones de la empresa receptora y reportes finales.
4. Registro y control de acceso a los expedientes físicos, electrónicos y sistemas institucionales que contienen datos personales de alumnos y docentes.
5. Registro, seguimiento y documentación de vulneraciones a la seguridad de los datos personales mediante las bitácoras correspondientes.

III. EL NOMBRE, CARGO Y ADSCRIPCIÓN DEL ADMINISTRADOR DEL SISTEMA DE TRATAMIENTO.

Los responsables del tratamiento de los datos personales en las Jefaturas de División, son los que se describen a continuación:

Responsable	Cargo	Órgano Administrativo	Tratamiento
	Jefa de División	Instituto Tecnológico Superior de Cintalapa	

	Coordinadora Carrera	de Instituto Tecnológico Cintalapa	Superior de
---	---------------------------------	---	------------------------

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIIP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

IV. LAS FUNCIONES Y OBLIGACIONES DEL RESPONSABLE Y TODAS LAS PERSONAS SERVIDORAS PÚBLICAS QUE TRATEN DATOS PERSONALES.

Funciones:

- Tratar los datos personales con responsabilidad y las medidas de seguridad que se hayan establecido para tal fin.
- Resguardar los datos personales a los que tengan acceso en el ejercicio de sus atribuciones.

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

- Verificar que el inventario de datos personales y de los sistemas de tratamiento de los mismos, a los que tienen acceso, se encuentren actualizados.
- En caso de que se presente algún incidente de vulneración de seguridad de los datos personales y/o de los sistemas de tratamiento de los mismos, informar sin dilación alguna a la persona titular, a la Autoridad Garante y llevar el registro de los hechos.

Obligaciones:

- Llevar a cabo permanentemente las medidas de seguridad necesarias para la protección de los datos personales, evitando daño, pérdida, alteración, destrucción o uso, acceso o tratamiento no autorizado, así como también garantizar la confidencialidad, integridad y disponibilidad de los mismos.
- Acatar los mecanismos para asegurar que los datos personales a los que tengan acceso en el ejercicio de sus atribuciones no se difundan, distribuyan o comercialicen.
- Guardar confidencialidad sobre la información que se conozca en el desarrollo de sus actividades.

V. LOS DATOS PERSONALES TRATADOS EN LOS SISTEMAS DE TRATAMIENTOS Y/O BASE DE DATOS PERSONALES SON LOS SIGUIENTES:

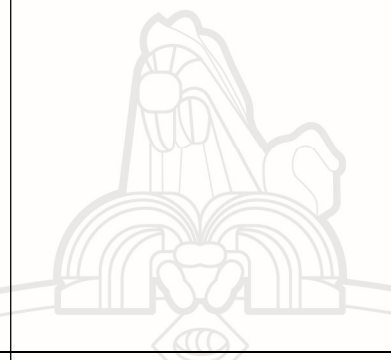
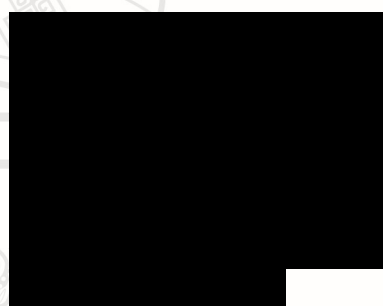
- Nombres y Apellidos
- Clave Única de Registro de Población
- Domicilio
- Número de Teléfono Fijo o Celular
- Correo Electrónico
- Nivel Educativo
- Estado Civil
- Edad
- Género

VI. LA DESCRIPCIÓN DEL SISTEMA DE TRATAMIENTO, SEÑALANDO EL TIPO DE SOPORTE Y LAS CARACTERÍSTICAS DEL LUGAR DONDE SE RESGUARDAN.

Descripción del Sistema de Tratamiento	Tipo de Soporte	Características del lugar de resguardo
Seguimiento Académico de Docentes: Registro y control	Documental (físico) y Electrónico.	

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIPI) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

de la actividad académica del personal docente adscrito a la División de Ingeniería en Industrias Alimentarias (carga horaria, evaluaciones, desempeño, cumplimiento de programas de estudio).		
Consulta de Datos Personales de Alumnos: Acceso y consulta de información de los estudiantes de la carrera (datos de identificación, historial académico, avance curricular) para fines de gestión y seguimiento académico.	Electrónico (Mindbox) y consulta documental de expedientes en casos específicos.	
Integración y Resguardo de Expedientes de Residencia Profesional y/o formación : Compilación y custodia de la documentación generada por los alumnos durante su proceso de residencia profesional (informes, cartas de aceptación, evaluaciones de la empresa receptora, reportes finales).	Documental (físico) y Electrónico (copias digitalizadas).	

VII. LOS CONTROLES Y MECANISMOS DE SEGURIDAD PARA LAS TRANSFERENCIAS QUE, EN SU CASO, SE EFECTÚEN.

En la información proporcionada por la División de Ingeniería en Industrias Alimentarias no se describe un mecanismo específico de transferencia de datos personales. Los tratamientos documentados comprenden seguimiento académico de docentes, consulta de información de estudiantes y expedientes de Residencia Profesional y/o Formación Dual. Cuando dentro de estos procesos resulte necesario comunicar información a un área institucional o a una organización receptora, la División deberá limitar el envío a los datos necesarios para el trámite,

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

utilizar medios institucionales autorizados y mantener registro y control de las personas que intervengan en el acceso.

VIII. EL RESGUARDO DE LOS SOPORTES FÍSICOS DE LOS DATOS PERSONALES.

Los expedientes físicos se encuentran resguardos y en custodia de los responsables del sistema de tratamiento de los datos personales en el área asignada para tal efecto.

IX. LAS BITÁCORAS DE ACCESO Y VULNERACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES.

Los datos que se registran en la Bitácora de acceso (anexo 1) son los siguientes:

- Quien accede a los datos personales, cargo y adscripción;
- Fecha y hora en la que se realiza el acceso o se intenta el mismo, así como fecha y hora de salida;
- Propósito del acceso;
- Firma de quien autoriza el acceso.

Los datos que se registran en la Bitácora de vulneraciones (anexo 2) son los siguientes:

- Fecha y hora de la vulneración;
- Motivo de la vulneración;
- Acciones correctivas y definitivas implementadas;
- Persona que resolvió la vulneración;
- Fecha y hora de notificación de la vulneración a los titulares de los datos personales comprometidos o afectados y a la Autoridad Garante en materia de protección de datos personales; y
- Los oficios, documentos, expedientes, estantes o archiveros dañados y los recuperados.

X. EL ANÁLISIS DE RIESGOS.

[Redacted content]

➤ [Redacted content]

[Redacted content]

➤ [Redacted content]

[Redacted content]

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIPI) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”



- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

Amenaza	Vulnerabilidades	Posibles consecuencias
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”



XI. EL ANÁLISIS DE BRECHA.

-
-
-
-
-
-
-
-

XII. LA GESTIÓN DE VULNERACIONES.

En caso de ocurrir alguna vulneración deberá registrarse en la bitácora de vulneraciones, además de informar de forma inmediata a la persona titular de los datos personales y a la Autoridad Garante...

XIII. LAS MEDIDAS DE SEGURIDAD FÍSICAS APLICADAS A LAS INSTALACIONES.

-
-
-
-

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPECCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

XIV. LOS CONTROLES DE IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS.

XV. LOS PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS PERSONALES.

XVI. EL PLAN DE CONTINGENCIA.

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

XVII. LAS TÉCNICAS UTILIZADAS PARA LA SUPRESIÓN Y BORRADO SEGURO DE LOS DATOS PERSONALES.

- Destrucción segura de documentos: Los documentos y otros medios físicos no deben simplemente desecharse una vez que ya no se utilizan, sino destruirse por ejemplo con triturador o incinerado.
- Destrucción segura de información en equipo de cómputo y medios de almacenamiento electrónico: Herramientas de software que borran archivos electrónicos específicos o dispositivos completos.
- Fijar periodos de retención y destrucción de información: Identificar de manera regular toda la información que ya no es de utilidad.
- Tomar precauciones con los procedimientos de reutilización: Bajo ninguna circunstancia deberían utilizarse documentos con datos personales como papel de reúso.

XVIII. EL PLAN DE TRABAJO.



XIX. LOS MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD.

Monitorear y revisar continuamente los riesgos, amenazas, vulnerabilidades, incidentes, modificaciones necesarias a los activos y nuevas amenazas.

XX. EL PROGRAMA GENERAL DE CAPACITACIÓN.

- Sensibilización en materia de Protección de Datos Personales en la Jefatura de División y su importancia en el entorno laboral.
- Capacitación a las personas servidoras públicas asignadas como enlaces en materia de datos personales respecto a los mecanismos, medios y procedimientos disponibles para ejercer los Derechos ARCO y Portabilidad de los datos personales.
- Concientizar a las personas servidoras públicas que dentro de sus funciones y obligaciones se encuentren la de recabar los datos personales, respecto a la importancia de informar a la persona titular de los datos personales a través del Aviso de Privacidad, el tratamiento de los mismos.
- Informar a las personas servidoras públicas que cuentan con la facultad de autorizar, acordar y/o decidir en el Órgano Administrativo, respecto a la implementación de las medidas de seguridad administrativa, técnicas y físicas, para la protección de los datos personales.
- Asesorar a las personas servidoras públicas que dentro de sus atribuciones se encuentre el tratamiento de los datos personales, respecto a la implementación del Documento de Seguridad, para la protección de los datos personales.

ANEXO 1: BITÁCORA DE ACCESO A LOS DATOS PERSONALES

Órgano Administrativo (o área generadora/resguardante): División de Ingeniería en Industrias Alimentarias.

Responsable del Archivo: Ana Karen Espinosa Arriola, Jefa de División de Ingeniería en Industrias Alimentarias.

No.	Nombres y Apellidos	Cargo y Adscripción	Fecha y Hora de Acceso	Fecha y Hora de Salida	Propósito del Acceso	Firma

ANEXO 2: BITÁCORA DE VULNERACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES

Órgano Administrativo (o área generadora/resguardante): División de Ingeniería en Industrias Alimentarias.

Responsable del Archivo: Ana Karen Espinosa Arriola, Jefa de División de Ingeniería en Industrias Alimentarias.

N o.	Fecha y Hora Vulneración	Motivo Vulneración	Acciones Correctivas	Acciones Definitivas	Fecha Notificación Titular	Fecha Notificación Autoridad	Datos / Expedientes Afectados

DIVISIÓN DE INGENIERÍA INFORMÁTICA

II. NOMBRES DE LOS SISTEMAS DE TRATAMIENTO

Los datos personales en posesión de la División de Ingeniería Informática del Instituto Tecnológico Superior de Cintalapa son sometidos a los siguientes tratamientos, derivados de las funciones y actividades descritas en su Documento de Seguridad:

1. Seguimiento académico del personal docente adscrito a la División de Ingeniería Informática, incluyendo carga horaria, evaluaciones, desempeño y cumplimiento de programas de estudio.
2. Consulta de datos personales de los alumnos de Ingeniería Informática, incluyendo datos de identificación, historial académico y avance curricular, para fines de gestión y seguimiento académico.
3. Integración y resguardo de los expedientes de residencia profesional y/o Formación Dual de los alumnos, incluyendo informes, cartas de aceptación, evaluaciones de la empresa receptora y reportes finales.
4. Registro y control de acceso a los expedientes físicos, electrónicos y sistemas institucionales que contienen datos personales de alumnos y docentes.
5. Registro, seguimiento y documentación de vulneraciones a la seguridad de los datos personales mediante las bitácoras correspondientes.

III. EL NOMBRE, CARGO Y ADSCRIPCIÓN DEL ADMINISTRADOR DEL SISTEMA DE TRATAMIENTO.

Los responsables del tratamiento de los datos personales en las Jefaturas de División, son los que se describen a continuación:

Responsable	Cargo	Órgano Administrativo	Tratamiento
[REDACTED]	Jefe de División	Instituto Superior Tecnológico de Cintalapa	[REDACTED]
[REDACTED]	Coordinadora de Carrera	Instituto Superior Tecnológico de Cintalapa	[REDACTED]

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIPI) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

IV. LAS FUNCIONES Y OBLIGACIONES DEL RESPONSABLE Y TODAS LAS PERSONAS SERVIDORAS PÚBLICAS QUE TRATEN DATOS PERSONALES.

Funciones:

- Tratar los datos personales con responsabilidad y las medidas de seguridad que se hayan establecido para tal fin.
- Resguardar los datos personales a los que tengan acceso en el ejercicio de sus atribuciones.
- Verificar que el inventario de datos personales y de los sistemas de tratamiento de los mismos, a los que tienen acceso, se encuentren actualizados.
- En caso de que se presente algún incidente de vulneración de seguridad de los datos personales y/o de los sistemas de tratamiento de los mismos, informar sin dilación alguna a la persona titular, a la Autoridad Garante y llevar el registro de los hechos.

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

Obligaciones:

- Llevar a cabo permanentemente las medidas de seguridad necesarias para la protección de los datos personales, evitando daño, pérdida, alteración, destrucción o uso, acceso o tratamiento no autorizado, así como también garantizar la confidencialidad, integridad y disponibilidad de los mismos.
- Acatar los mecanismos para asegurar que los datos personales a los que tengan acceso en el ejercicio de sus atribuciones no se difundan, distribuyan o comercialicen.
- Guardar confidencialidad sobre la información que se conozca en el desarrollo de sus actividades.

V. LOS DATOS PERSONALES TRATADOS EN LOS SISTEMAS DE TRATAMIENTOS Y/O BASE DE DATOS PERSONALES SON LOS SIGUIENTES:

- Nombres y Apellidos
- Clave Única de Registro de Población
- Domicilio
- Número de Teléfono Fijo o Celular
- Correo Electrónico
- Nivel Educativo
- Estado Civil
- Edad
- Género

VI. LA DESCRIPCIÓN DEL SISTEMA DE TRATAMIENTO, SEÑALANDO EL TIPO DE SOPORTE Y LAS CARACTERÍSTICAS DEL LUGAR DONDE SE RESGUARDAN.

Descripción del Sistema de Tratamiento	Tipo de Soporte	Características del lugar de resguardo
Seguimiento Académico de Docentes: Registro y control de la actividad académica del personal docente adscrito a la División de Ingeniería Informática (carga horaria, evaluaciones, desempeño, cumplimiento de programas de estudio).	Documental (físico) y Electrónico.	

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIPI) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPECHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

Consulta de Datos Personales de Alumnos: Acceso y consulta de información de los estudiantes de la carrera (datos de identificación, historial académico, avance curricular) para fines de gestión y seguimiento académico.	Electrónico (Mindbox) y consulta documental de expedientes en casos específicos.	
Integración y Resguardo de Expedientes de Residencia Profesional y/o formación : Compilación y custodia de la documentación generada por los alumnos durante su proceso de residencia profesional (informes, cartas de aceptación, evaluaciones de la empresa receptora, reportes finales).	Documental (físico) y Electrónico (copias digitalizadas).	

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAI) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

VII. LOS CONTROLES Y MECANISMOS DE SEGURIDAD PARA LAS TRANSFERENCIAS QUE, EN SU CASO, SE EFECTÚEN.

En la información proporcionada por la División de Ingeniería Informática no se describe un mecanismo específico de transferencia de datos personales. Los tratamientos documentados comprenden seguimiento académico de docentes, consulta de información de estudiantes y expedientes de Residencia Profesional y/o Formación Dual. Cuando dentro de estos procesos resulte necesario comunicar información a un área institucional o a una organización receptora, la División deberá limitar el envío a los datos necesarios para el trámite, utilizar medios institucionales autorizados y mantener registro y control de las personas que intervengan en el acceso.

VIII. EL RESGUARDO DE LOS SOPORTES FÍSICOS DE LOS DATOS PERSONALES.

Los expedientes físicos se encuentran resguardos y en custodia de los responsables del sistema de tratamiento de los datos personales en el área asignada para tal efecto.

IX. LAS BITÁCORAS DE ACCESO Y VULNERACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES.

Los datos que se registran en la Bitácora de acceso (anexo 1) son los siguientes:

- Quien accede a los datos personales, cargo y adscripción;
- Fecha y hora en la que se realiza el acceso o se intenta el mismo, así como fecha y hora de salida;
- Propósito del acceso;
- Firma de quien autoriza el acceso.

Los datos que se registran en la Bitácora de vulneraciones (anexo 2) son los siguientes:

- Fecha y hora de la vulneración;
- Motivo de la vulneración;
- Acciones correctivas y definitivas implementadas;
- Persona que resolvió la vulneración;
- Fecha y hora de notificación de la vulneración a los titulares de los datos personales comprometidos o afectados y a la Autoridad Garante en materia de protección de datos personales; y
- Los oficios, documentos, expedientes, estantes o archiveros dañados y los recuperados.

X. EL ANÁLISIS DE RIESGOS.

[Redacted content]

➤ [Redacted content]

➤ [Redacted content]

➤ [Redacted content]

➤ [Redacted content]

➤ [Redacted content]

➤ [Redacted content]

➤ [Redacted content]

[Redacted content]

[Redacted content]

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIIP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”



Amenaza	Vulnerabilidades	Posibles consecuencias
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAI) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPECHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”



--	--	--	--

XI. EL ANÁLISIS DE BRECHA.

-
-
-
-
-
-
-
-

XII. LA GESTIÓN DE VULNERACIONES.

En caso de ocurrir alguna vulneración deberá registrarse en la bitácora de vulneraciones, además de informar de forma inmediata a la persona titular de los datos personales y a la Autoridad Garante.

XIII. LAS MEDIDAS DE SEGURIDAD FÍSICAS APLICADAS A LAS INSTALACIONES.

-
-
-
-

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIPI) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

XIV. LOS CONTROLES DE IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS.

[Redacted content]

XV. LOS PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS PERSONALES.

[Redacted content]

XVI. EL PLAN DE CONTINGENCIA.

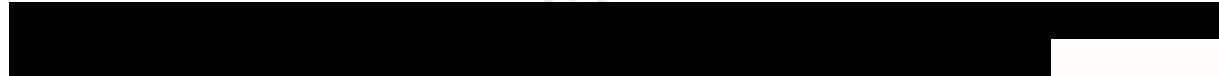
- [Redacted content]
- [Redacted content]
- [Redacted content]
- [Redacted content]
- [Redacted content]
- [Redacted content]

XVII. LAS TÉCNICAS UTILIZADAS PARA LA SUPRESIÓN Y BORRADO SEGURO DE LOS DATOS PERSONALES.

- Destrucción segura de documentos: Los documentos y otros medios físicos no deben simplemente desecharse una vez que ya no se utilizan, sino destruirse por ejemplo con triturador o incinerado.
- Destrucción segura de información en equipo de cómputo y medios de almacenamiento electrónico: Herramientas de software que borran archivos electrónicos específicos o dispositivos completos.
- Fijar periodos de retención y destrucción de información: Identificar de manera regular toda la información que ya no es de utilidad.
- Tomar precauciones con los procedimientos de reutilización: Bajo ninguna circunstancia deberían utilizarse documentos con datos personales como papel de reúso.

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIIP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

XVIII. EL PLAN DE TRABAJO.



XIX. LOS MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD.

Monitorear y revisar continuamente los riesgos, amenazas, vulnerabilidades, incidentes, modificaciones necesarias a los activos y nuevas amenazas.

XX. EL PROGRAMA GENERAL DE CAPACITACIÓN.

- Sensibilización en materia de Protección de Datos Personales en la Jefatura de División y su importancia en el entorno laboral.
- Capacitación a las personas servidoras públicas asignadas como enlaces en materia de datos personales respecto a los mecanismos, medios y procedimientos disponibles para ejercer los Derechos ARCO y Portabilidad de los datos personales.
- Concientizar a las personas servidoras públicas que dentro de sus funciones y obligaciones se encuentren la de recabar los datos personales, respecto a la importancia de informar a la persona titular de los datos personales a través del Aviso de Privacidad, el tratamiento de los mismos.
- Informar a las personas servidoras públicas que cuentan con la facultad de autorizar, acordar y/o decidir en el Órgano Administrativo, respecto a la implementación de las medidas de seguridad administrativa, técnicas y físicas, para la protección de los datos personales.
- Asesorar a las personas servidoras públicas que dentro de sus atribuciones se encuentre el tratamiento de los datos personales, respecto a la implementación del Documento de Seguridad, para la protección de los datos personales.

ANEXO 1: BITÁCORA DE ACCESO A LOS DATOS PERSONALES

Órgano Administrativo (o área generadora/resguardante): División de Ingeniería Informática.
Responsable del Archivo: Arturo Montesinos Cervantes, Jefe de División de Ingeniería Informática.

No.	Nombres y Apellidos	Cargo y Adscripción	Fecha y Hora de Acceso	Fecha y Hora de Salida	Propósito del Acceso	Firma

ANEXO 2: BITÁCORA DE VULNERACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES

Órgano Administrativo (o área generadora/resguardante): División de Ingeniería Informática.

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTIAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

Responsable del Archivo: Arturo Montesinos Cervantes, Jefe de División de Ingeniería Informática.

No.	Fecha y Hora Vulneración	Motivo Vulneración	Acciones Correctivas	Acciones Definitivas	Fecha Notificación Titular	Fecha Notificación Autoridad	Datos / Expedientes Afectados

DEPARTAMENTO DE PERSONAL

II. NOMBRES DE LOS SISTEMAS DE TRATAMIENTO

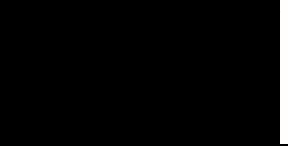
Los datos personales en posesión del Departamento de Personal del Instituto Tecnológico Superior de Cintalapa son sometidos a los siguientes tratamientos, derivados de las funciones y actividades descritas en su Documento de Seguridad:

1. Recepción, integración, actualización y resguardo de los expedientes únicos de las personas servidoras públicas del Instituto, incluyendo la documentación del personal de nuevo ingreso y del personal dado de baja.
2. Registro y actualización de datos del personal en los sistemas institucionales y gubernamentales utilizados para la administración de recursos humanos.
3. Integración, cálculo, procesamiento y resguardo de la información necesaria para el pago de nómina del personal del Instituto.
4. Registro y control de asistencia del personal adscrito al Instituto mediante los sistemas correspondientes.
5. Trámites de incorporación, afiliación, actualización y movimientos ante el Instituto Mexicano del Seguro Social (IMSS).
6. Trámites de incorporación y afiliación al Seguro de Vida Institucional.
7. Integración y resguardo de las hojas de aceptación y gestión de la Firma Electrónica de Chiapas de las personas servidoras públicas.
8. Incorporación y actualización de la base de datos de las personas servidoras públicas en el Sistema de Administración de Recursos de los Institutos Tecnológicos Descentralizados (SARITD).
9. Alta, baja y actualización de información del personal en los sistemas de declaración patrimonial y resguardo de los acuses correspondientes.
10. Elaboración y expedición de credenciales para la identificación institucional del personal.

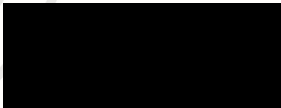
11. Integración y elaboración de información del personal para la estadística 911.9 y demás reportes institucionales.
12. Elaboración, captura y actualización de los datos del personal en los sistemas de transparencia, conforme a las obligaciones aplicables.
13. Elaboración y resguardo de oficios y documentación administrativa relacionada con la gestión del personal.
14. Elaboración y tratamiento de la información necesaria para los pagos y trámites relacionados con personas pensionadas.
15. Atención de solicitudes para el ejercicio de derechos ARCO y de portabilidad relacionadas con los datos personales bajo resguardo del Departamento de Personal.
16. Registro y control de acceso a los expedientes, bases de datos y sistemas que contienen datos personales del personal.
17. Registro, seguimiento y documentación de vulneraciones a la seguridad de los datos personales mediante las bitácoras correspondientes.

III. EL NOMBRE, CARGO Y ADSCRIPCIÓN DEL ADMINISTRADOR DEL SISTEMA DE TRATAMIENTO.

Los responsables del tratamiento de los datos personales en el Departamento de Personal son los que se describen a continuación:

Responsable	Cargo	Órgano Administrativo	Tratamiento
	Jefe del Departamento	Departamento de Personal	
	Jefe de Oficina	Departamento de Personal	

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

	Analista Especializado	Departamento de Personal	

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

[REDACTED]	Técnico Especializado	Departamento de Personal	[REDACTED]
[REDACTED]	Secretaria De Jefe Departamento	Departamento de Personal	[REDACTED]

IV. LAS FUNCIONES Y OBLIGACIONES DEL RESPONSABLE Y TODAS LAS PERSONAS SERVIDORAS PÚBLICAS QUE TRATEN DATOS PERSONALES.

Funciones:

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

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIIP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

- Resguardar los datos personales a los que tengan acceso en el ejercicio de sus atribuciones.
- Verificar que el inventario de datos personales y de los sistemas de tratamiento de los mismos, a los que tienen acceso, se encuentren actualizados.
- Llevar un registro de las personas servidoras públicas que accedan a los datos personales y llevar a cabo las acciones necesarias para la autenticación de los usuarios.
- Mantener actualizada la relación de usuarios que traten datos personales.
- En caso de que se presente algún incidente de vulneración de seguridad de los datos personales y/o de los sistemas de tratamiento de los mismos, informar sin dilación alguna a la persona titular, a la Autoridad Garante y llevar el registro de los hechos.

Obligaciones:

- Llevar a cabo permanentemente las medidas de seguridad necesarias para la protección de los datos personales, evitando daño, pérdida, alteración, destrucción o uso, acceso o tratamiento no autorizado, así como también garantizar la confidencialidad, integridad y disponibilidad de los mismos.
- Acatar los mecanismos para asegurar que los datos personales a los que tengan acceso en el ejercicio de sus atribuciones no se difundan, distribuyan o comercialicen.
- Guardar confidencialidad sobre la información que se conozca en el desarrollo de sus actividades.

V. LOS DATOS PERSONALES TRATADOS EN LOS SISTEMAS DE TRATAMIENTOS Y/O BASE DE DATOS PERSONALES SON LOS SIGUIENTES:

- Nombres y Apellidos
- Credencial para Votar
- Clave Única de Registro de Población
- Registro Federal de Contribuyente
- Domicilio
- Número de Teléfono Fijo o Celular
- Correo Electrónico
- Acta de Nacimiento
- Número de Seguridad Social
- Firma

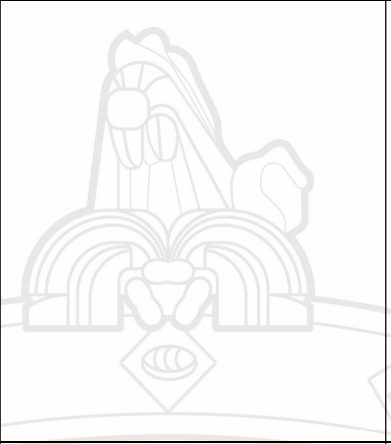
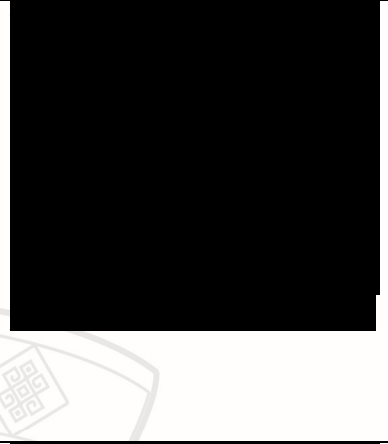
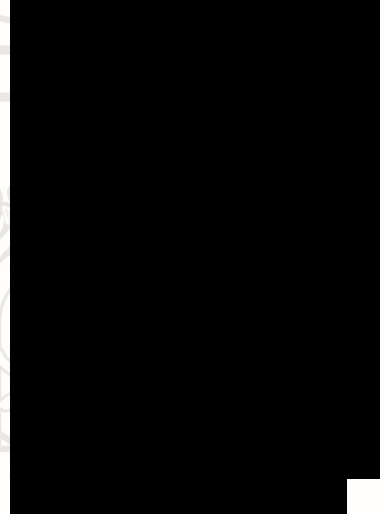
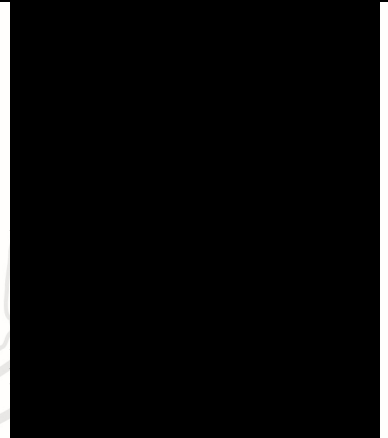
Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

- Nivel Educativo
- Títulos o Constancias Académicas
- Datos Bancarios
- Curriculum Vitae
- Estado Civil
- Edad
- Género
- Certificado Médico
- Lugar y Fecha de Nacimiento

VI. LA DESCRIPCIÓN DEL SISTEMA DE TRATAMIENTO, SEÑALANDO EL TIPO DE SOPORTE Y LAS CARACTERÍSTICAS DEL LUGAR DONDE SE RESGUARDAN.

Descripción del Sistema de Tratamiento	Tipo de Soporte	Características del lugar de resguardo
1. Se elaboran los expedientes de cada persona servidora pública, para el control y seguimiento de los datos personales tratados para: - Alimentar el Sistema de Nóminas del Estado de Chiapas (NECH), y el Software de Control de Asistencia de Personal (NominaPlus.T&A.NET). - Afiliación al Seguro Social (IMSS). - Guarda y custodia en los expedientes de las personas servidoras públicas dadas de baja. - Dar cumplimiento a las solicitudes de derechos ARCO y de portabilidad.	Físico y Electrónico	
2. Se integran y resguardan las hojas de nómina quincenal firmadas por cada persona	Físico y Electrónico	

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAPCHS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

servidora pública, de conformidad al pago de salario del periodo correspondiente, mismas que pueden ser transferidas a la persona titular para trámites de pensión o por jubilación, a la Autoridad Garante en materia de transparencia y a las instancias facultadas de la administración pública para solventar juicios en materia laboral o auditorías.		
3. Se integran y resguardan las hojas de aceptación de firma electrónica por cada persona servidora pública, mediante el cual manifiesta tener conocimiento de las obligaciones legales que conlleva el uso de dicha firma; así mismo los datos personales son adjuntados y digitalizados en los sistemas generadores de la firma electrónica.	Físico y Electrónico	
4. Los datos personales son tratados para integrar el directorio de servidores públicos del Estado de Chiapas.	Físico	

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAPCHS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

--	--	--

VII. LOS CONTROLES Y MECANISMOS DE SEGURIDAD PARA LAS TRANSFERENCIAS QUE, EN SU CASO, SE EFECTÚEN.

Para las transferencias de datos personales que realice el Departamento de Personal en el cumplimiento de sus atribuciones (incluidos los trámites ante el IMSS, el Seguro de Vida Institucional, la Firma Electrónica de Chiapas, SARITD, los sistemas de declaración patrimonial, transparencia y demás instancias o sistemas oficiales señalados en este documento) sólo deberá comunicarse la información necesaria para la finalidad correspondiente. La transferencia deberá realizarse por medios institucionales y con control de las personas autorizadas, atendiendo al aviso de privacidad y a las disposiciones aplicables.

A. Traslado de soportes físicos: Cuando el trámite requiera entregar formularios, constancias, oficios o copias de documentos del expediente del personal, éstos deberán remitirse únicamente a la instancia competente, mediante mecanismos institucionales de entrega y recepción que permitan conservar el control de la documentación.

B. Traslado físico de soportes electrónicos: Cuando sea indispensable entregar archivos mediante un dispositivo de almacenamiento autorizado, el Departamento deberá limitar el contenido a la información necesaria para el trámite, mantener el medio bajo custodia y entregarlo únicamente a la persona o instancia destinataria autorizada.

C. Traslado sobre redes electrónicas: Las cargas de información en sistemas oficiales y los envíos electrónicos relacionados con nómina, afiliaciones, firma electrónica, declaraciones, transparencia o reportes institucionales deberán efectuarse mediante cuentas, plataformas y credenciales autorizadas, evitando el uso de medios personales o no institucionales.

VIII. EL RESGUARDO DE LOS SOPORTES FÍSICOS DE LOS DATOS PERSONALES.

Los expedientes físicos se encuentran resguardos y en custodia de los responsables del sistema de tratamiento de los datos personales en el área asignada para tal efecto.

IX. LAS BITÁCORAS DE ACCESO Y VULNERACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES.

Los datos que se registran en la Bitácora de acceso (anexo 1) son los siguientes:

- Quien accede a los datos personales, cargo y adscripción;
- Fecha y hora en la que se realiza el acceso o se intenta el mismo, así como fecha de salida;
- Propósito del acceso;
- Firma de quien autoriza el acceso.

Los datos que se registran en la Bitácora de vulneraciones (anexo 2) son los siguientes:

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTIIP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

- Fecha y hora de la vulneración;
- Motivo de la vulneración;
- Acciones correctivas y definitivas implementadas;
- Persona que resolvió la vulneración;
- Fecha y hora de notificación de la vulneración a los titulares de los datos personales comprometidos o afectados y a la Autoridad Garante en materia de protección de datos personales; y
- Los oficios, documentos, expedientes, estantes o archiveros dañados y los recuperados.

X. EL ANÁLISIS DE RIESGOS.

[Redacted]		
➤	[Redacted]	[Redacted]
➤	[Redacted]	[Redacted]
➤	[Redacted]	[Redacted]
➤	[Redacted]	[Redacted]
➤	[Redacted]	[Redacted]
➤	[Redacted]	[Redacted]
➤	[Redacted]	[Redacted]
➤	[Redacted]	[Redacted]
➤	[Redacted]	[Redacted]
➤	[Redacted]	[Redacted]
Amenaza	Vulnerabilidades	Posibles consecuencias
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIPI) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”



[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIPI) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

[REDACTED]	[REDACTED]	[REDACTED]

XI. EL ANÁLISIS DE BRECHA.

- [REDACTED]

> [REDACTED]

[REDACTED]

> [REDACTED]

> [REDACTED]

[REDACTED]

> [REDACTED]

[REDACTED]

> [REDACTED]

[REDACTED]

> [REDACTED]

[REDACTED]

> [REDACTED]

[REDACTED]

XII. LA GESTIÓN DE VULNERACIONES.

En caso de ocurrir alguna vulneración deberá registrarse en la bitácora de contingencias, además de informar de forma inmediata a la persona titular de los datos personales y a la Autoridad Garante.

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIPI) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

XIII. LAS MEDIDAS DE SEGURIDAD FÍSICAS APLICADAS A LAS INSTALACIONES.

[REDACTED]

XIV. LOS CONTROLES DE IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS.

[REDACTED]

XV. LOS PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS PERSONALES.

[REDACTED]

XVI. EL PLAN DE CONTINGENCIA.

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

XVII. LAS TÉCNICAS UTILIZADAS PARA LA SUPRESIÓN Y BORRADO SEGURO DE LOS DATOS PERSONALES.

- Destrucción segura de documentos: Los documentos y otros medios físicos no deben simplemente desecharse una vez que ya no se utilizan, sino destruirse.
- Destrucción segura de información en equipo de cómputo y medios de almacenamiento electrónico: Herramientas de software que borran archivos electrónicos específicos o dispositivos completos.

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIPI) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

- Fijar periodos de retención y destrucción de información: Identificar de manera regular toda la información que ya no es de utilidad.
 - Tomar precauciones con los procedimientos de reutilización: Bajo ninguna circunstancia deberían utilizarse documentos con datos personales como papel de reúso.
- Lo anterior con base en el artículo 28, 29 y 30 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas.

XVIII. EL PLAN DE TRABAJO.



XIX. LOS MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD.

Monitorear y revisar continuamente los riesgos, amenazas, vulnerabilidades, incidentes, modificaciones necesarias a los activos y nuevas amenazas.

XX. EL PROGRAMA GENERAL DE CAPACITACIÓN.

- Sensibilización en materia de Protección de Datos Personales en el Departamento de Personal y su importancia en el entorno laboral.
- Capacitación a las personas servidoras públicas asignadas como enlaces en materia de datos personales respecto a los mecanismos, medios y procedimientos disponibles para ejercer los Derechos ARCO y Portabilidad de los datos personales.
- Concientizar a las personas servidoras públicas que dentro de sus funciones y obligaciones se encuentren la de recabar los datos personales, respecto a la importancia de informar a la persona titular de los datos personales a través del Aviso de Privacidad, el tratamiento de los mismos.
- Informar a las personas servidoras públicas que cuentan con la facultad de autorizar, acordar y/o decidir en el Órgano Administrativo, respecto a la implementación de las medidas de seguridad administrativa, técnicas y físicas, para la protección de los datos personales.
- Asesorar a las personas servidoras públicas que dentro de sus atribuciones se encuentre el tratamiento de los datos personales, respecto a la implementación del Documento de Seguridad, para la protección de los datos personales.

ANEXO 1: BITÁCORA DE ACCESO A LOS DATOS PERSONALES

Órgano Administrativo (o área generadora/resguardante): Departamento de Personal.
Responsable del Archivo: Rafael Mauricio Camacho Camacho, Jefe del Departamento de Personal.

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIIP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

No. Cons.	Nombres y Apellidos	Fecha de Acceso	Fecha de Salida	Propósito del Acceso	Firma

ANEXO 2: BITÁCORA DE VULNERACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES

Órgano Administrativo (o área generadora/resguardante): Departamento de Personal.
Responsable del Archivo: Rafael Mauricio Camacho Camacho, Jefe del Departamento de Personal.

No. Cons.	Fecha y Hora Vulneración	Motivo Vulneración	Acciones Correctivas	Acciones Definitivas	Fecha Notificación Titular	Fecha Notificación Autoridad	Expedientes Afectados

DEPARTAMENTO DE DIFUSIÓN Y CONCERTACIÓN

II. NOMBRES DE LOS SISTEMAS DE TRATAMIENTO.

Los datos personales en posesión del Departamento de Difusión y Concertación son sometidos a los siguientes tratamientos:

1. Recepción, integración, control y resguardo de documentos de cesión de derechos de imagen de estudiantes y demás personas participantes en actividades institucionales.
2. Captación, selección, edición y resguardo de fotografías y videos utilizados para la difusión de actividades académicas y administrativas.
3. Integración y manejo de datos de identificación, nombre, apellidos y carrera vinculados con publicaciones y materiales institucionales.
4. Elaboración y difusión de elementos gráficos, notas y publicaciones institucionales que incorporen imagen o datos personales, conforme a las finalidades autorizadas.

III. EL NOMBRE, CARGO Y ADSCRIPCIÓN DEL ADMINISTRADOR DEL SISTEMA DE TRATAMIENTO.

Los responsables del tratamiento de los datos personales del Departamento de Difusión y Concertación, son los que describen a continuación:

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

Responsable	Cargo	Órgano Administrativo	Tratamiento
[REDACTED]	Jefa del Departamento de Difusión y Concertación Responsable de la Supervisión y revisión de la información electrónica, así como de la recepción del documento de cesión de derechos de imagen.	Departamento de Difusión y Concertación	[REDACTED]
[REDACTED]	Secretario de Dirección General Interino Responsable de la toma de fotografías, videos y diseños para publicaciones institucionales	Departamento de Difusión y Concertación	[REDACTED]
[REDACTED]	Secretario de Jefe de Departamento Responsable de la toma de fotografías y videos, así como edición de los mismos para publicaciones institucionales.	Departamento de Difusión y Concertación	[REDACTED]

IV. LAS FUNCIONES Y OBLIGACIONES DEL RESPONSABLE Y TODAS LAS PERSONAS SERVIDORAS PÚBLICAS QUE TRATEN DATOS PERSONALES.

Las funciones y obligaciones del responsable y de todas las personas servidoras públicas que traten datos personales en el Departamento de Difusión y Concertación son las siguientes:

Funciones:

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAI) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

- Dar a los datos personales un tratamiento responsable, conforme a las medidas de seguridad establecidas para tal efecto;
- Salvaguardar los datos personales a los que se tenga acceso con motivo del ejercicio de sus funciones;
- Conservar actualizado el listado de personas usuarias que den tratamiento a datos personales;
- Ante un incidente de vulneración de seguridad de los datos personales o de sus sistemas de tratamiento, notificar de inmediato a la persona titular y documentar los hechos, mediante el Anexo 2.

Obligaciones:

6. Guardar confidencialidad respecto de los datos personales a los que se tenga acceso, incluso después de concluida la relación laboral;
7. Limitar el tratamiento de los datos personales a las finalidades previstas en el aviso de privacidad correspondiente;
8. Abstenerse de transferir, difundir o divulgar datos personales sin el consentimiento de la persona titular o sin fundamento legal que lo autorice o bien sea una función a fin a sus actividades laborales;

V. LOS DATOS PERSONALES TRATADOS EN LOS SISTEMAS DE TRATAMIENTOS Y/O BASE DE DATOS PERSONALES SON LOS SIGUIENTES:

Datos:

1. Nombres y Apellidos
2. Carrera

Documentos:

- [REDACTED]

VI. LA DESCRIPCIÓN DEL SISTEMA DE TRATAMIENTO, SEÑALANDO EL TIPO DE SOPORTE Y LAS CARACTERÍSTICAS DEL LUGAR DONDE SE RESGUARDAN.

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIPI) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y de clasificación de la información, así como para la elaboración de versiones públicas.”

Descripción del Sistema de Tratamiento	Tipo de Soporte	Características del lugar de resguardo
1. Integración de datos en carpeta física. Archivo que resguarda los documentos firmados de sesiones de derechos de imagen de los estudiantes que han participado en la campaña de oferta educativa de los programas educativos vigentes de la institución.	Físico	

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

VII. LOS CONTROLES Y MECANISMOS DE SEGURIDAD PARA LAS TRANSFERENCIAS QUE, EN SU CASO, SE EFECTÚEN.

A continuación, se detalla las áreas tanto internas como externas que reciben información del Departamento de Difusión y Concertación:

- Dirección General

Uso de información:

- Tomar decisiones institucionales;
- Resolver casos especiales que requieran su intervención.

Mecanismos de seguridad:

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

Para implementar las medidas de seguridad aplicables a la transferencia de datos personales el receptor de los datos personales asumirá el carácter de responsable conforme a la legislación en la materia al recibir dicha información mediante el traslado de soportes físicos, por lo que deberá tratar los datos personales atendiendo y apegándose al aviso de privacidad del Departamento de Difusión y Concertación, mismo que se encuentra publicado en:

<https://cintalapa.tecnm.mx/aviso-privacidad>

En cada una de estas modalidades se deberá sujetarse a lo siguiente:

- **Traslado de soportes físicos:** Los datos personales se trasladan en documentos impresos que pueden leerse directamente, sin necesidad de un dispositivo que procese su contenido para consultarlo, modificarlo o almacenarlo.

Por ejemplo: cuando el Departamento de Difusión y Concertación remite a la Dirección General por petición de la misma.

VIII. EL RESGUARDO DE LOS SOPORTES FÍSICOS DE LOS DATOS PERSONALES.

Los expedientes físicos se encuentran resguardos y en custodia de los responsables del sistema de tratamiento de los datos personales en el área asignada para tal efecto.

IX. LAS BITÁCORAS DE ACCESO Y VULNERACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES.

Los datos que se registran en la Bitácora de acceso (anexo 1) son los siguientes:

- Número consecutivo;
- Quien accede a los datos personales (Nombre completo);
- Cargo;
- Área de adscripción;
- Propósito del acceso;
- Tipo de soporte utilizado (Expediente o registro electrónico);
- Fecha en formato mes y año (Al que corresponde la bitácora).

Los datos que se registran en la Bitácora de vulneraciones (anexo 2) son los siguientes:

- Número consecutivo;
- Fecha y hora de la vulneración;
- Documento o información vulnerada;
- Motivo de la vulneración;
- Acciones correctivas y definitivas implementadas;
- Persona que resolvió la vulneración;

- Fecha y hora de notificación de la vulneración a los titulares de los datos personales comprometidos;
- Fecha en formato mes y año (Al que corresponde la bitácora).

X. EL ANÁLISIS DE RIESGOS.

[REDACTED]		
[REDACTED]		
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

XI. EL ANÁLISIS DE BRECHA.

[REDACTED]	
[REDACTED]	
[REDACTED]	

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LTGAIIP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPECIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

- [REDACTED]
- [REDACTED]
- [REDACTED]
 - [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]

XII. LA GESTIÓN DE VULNERACIONES.

En caso de ocurrir alguna vulneración deberá registrarse en la bitácora de contingencias (Anexo 2), y se llevará a cabo conforme al siguiente procedimiento:

- **Detección y aviso interno:** El personal del departamento que detecte o sospeche de una vulneración lo comunicará de inmediato a la Jefatura del Departamento de Difusión y Concertación, preservando el estado de los documentos, equipos o sistemas involucrados.
- **Contención:** Se ejecutarán acciones inmediatas para evitar mayor afectación, tales como resguardar el archivo, suspender accesos, cambiar contraseñas o desconectar el equipo comprometido.

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIIP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

- **Registro inicial:** Se asentará en la bitácora la fecha y hora de la vulneración, el documento o información vulnerada y el motivo de la vulneración.
- **Evaluación:** La Jefatura determinará el alcance del incidente, las personas titulares afectadas y si se comprometen sus derechos patrimoniales o morales.
- **Acciones correctivas y definitivas:** Se implementarán las medidas para restablecer la información y eliminar la causa, y se registrarán en la bitácora junto con el nombre de la persona que resolvió la vulneración.
- **Notificación:** Se informará a las personas titulares, sin dilación alguna y dentro del plazo no mayor a 3 días (72 horas), la notificación incluirá la naturaleza del incidente, los datos personales comprometidos, las recomendaciones para la persona titular, las acciones correctivas realizadas y los medios para obtener mayor información. Se registrará en la bitácora la fecha y hora de cada notificación.
- **Cierre y prevención.** La Jefatura revisará las medidas de seguridad vigentes y ajustará las que resulten necesarias para evitar que el incidente se repita.

XIII. LAS MEDIDAS DE SEGURIDAD FÍSICAS APLICADAS A LAS INSTALACIONES.

- [Redacted]
- [Redacted]

XIV. LOS CONTROLES DE IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS.

- [Redacted]
- [Redacted]

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

XV. LOS PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS PERSONALES.

- [Redacted]
- [Redacted]

XVI. EL PLAN DE CONTINGENCIA.

- [Redacted]
- [Redacted]

XVII. LAS TÉCNICAS UTILIZADAS PARA LA SUPRESIÓN Y BORRADO SEGURO DE LOS DATOS PERSONALES.

- Los documentos físicos que contengan datos personales o cesiones de derechos de imagen sólo podrán eliminarse una vez cumplida su finalidad y los periodos de conservación que correspondan. Cuando proceda su eliminación, deberán destruirse de forma que los nombres, firmas y demás datos no puedan reconstruirse ni reutilizarse.
- Los documentos con datos personales no deberán utilizarse como papel de reúso ni desecharse íntegros en depósitos de basura común.

XVIII. EL PLAN DE TRABAJO.

- [Redacted]
- [Redacted]

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPECHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

XIX. LOS MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD.

- La Jefatura verificará periódicamente el estado del archivero, el control de llaves, los registros de acceso, las vulneraciones y el cumplimiento de las medidas aplicables a la utilización de datos e imagen en publicaciones institucionales.
- Cuando se detecte un nuevo riesgo, un cambio en la forma de resguardo o un incidente, deberán revisarse las medidas de seguridad y actualizarse la documentación del área.

XX. EL PROGRAMA GENERAL DE CAPACITACIÓN.

- El personal que interviene en la captación, edición, resguardo y publicación de fotografías, videos, nombres y demás datos personales deberá recibir capacitación sobre confidencialidad, aviso de privacidad, alcance de las cesiones de derechos de imagen, uso limitado de la información, manejo de bitácoras y atención de vulneraciones.
- La capacitación deberá reforzar especialmente el uso de la información únicamente para las finalidades institucionales autorizadas.

ANEXO 1: BITÁCORA DE ACCESO A LOS DATOS PERSONALES

Órgano Administrativo (o área generadora/resguardante):

Instituto Tecnológico Superior de Cintalapa
Departamento de Difusión y Concertación.

Responsable del Archivo:

Alondra de Jesús Venegas Contreras
Jefa del Departamento de Difusión y Concertación

Número consecutivo	Quien accede a los datos personales (Nombre completo)	Cargo	Área de adscripción	Propósito del acceso	Número de control del alumno y/o egresado	Tipo de soporte utilizado (Expediente o registro electronico)	Fecha en formato mes y año (Al que corresponde la bitácora)

ANEXO 2: Bitácora de vulneraciones a la seguridad de los Datos Personales

Órgano Administrativo (o área generadora/resguardante):

Instituto Tecnológico Superior de Cintalapa
Departamento de Difusión y Concertación.

Responsable del Archivo:

Alondra de Jesús Venegas Contreras

Jefa del Departamento de Difusión y Concertación

Número consecutivo	Fecha y Hora Vulneración	Documento o información vulnerada	Motivo de la vulneración	Acciones correctivas y definitivas implementadas	Persona que resolvió la vulneración	Fecha y hora de notificación de la vulneración a los titulares de los datos personales comprometidos	Fecha en formato mes y año (Al que corresponde la bitácora)

DEPARTAMENTO DE RECURSOS FINANCIEROS

II. NOMBRES DE LOS SISTEMAS DE TRATAMIENTO.

Los datos personales en posesión del Departamento de Recursos Financieros son sometidos a los siguientes tratamientos:

1. Validación de datos para el pago de cuotas de inscripción mediante el Sistema de Gestión de Matrícula Escolar MindBox.
2. Emisión, timbrado, entrega y resguardo de comprobantes fiscales digitales (CFDI/facturas).
3. Integración, control y resguardo de expedientes contables, estados financieros mensuales y documentación de la Cuenta Pública Trimestral.
4. Gestión, validación y control de pagos a proveedores, prestadores de servicios y viáticos del personal comisionado mediante transferencias electrónicas o cheques.
5. Integración y resguardo de información financiera, contable, presupuestal y documental requerida para auditorías y procesos de rendición de cuentas.

III. EL NOMBRE, CARGO Y ADSCRIPCIÓN DEL ADMINISTRADOR DEL SISTEMA DE TRATAMIENTO.

Los responsables del tratamiento de los datos personales del Departamento de Recursos Financieros, son los que describen a continuación:

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

Responsable	Cargo	Órgano Administrativo	Tratamiento
[REDACTED]	Jefe del Departamento de Recursos Financieros. Responsable de la Supervisión y revisión de la información Financiera, Contable y Administrativa.	Departamento de Recursos Financieros.	[REDACTED]
[REDACTED]	Secretaria de subdirector Responsable del área de caja	Departamento de Recursos Financieros.	[REDACTED]
[REDACTED]	Técnico especializado Responsable del pago a proveedores, prestadores de servicios y viáticos a personal comisionado.	Departamento de Recursos Financieros.	[REDACTED]
[REDACTED]	Secretaria de subdirector Responsable de la captura e integración	Departamento de Recursos Financieros.	[REDACTED]

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

	de la información contable y presupuestal.		
	Programador Responsable en la captura e integración del soporte de la información solicitadas en las auditorías.	Departamento de Recursos Financieros.	

IV. LAS FUNCIONES Y OBLIGACIONES DEL RESPONSABLE Y TODAS LAS PERSONAS SERVIDORAS PÚBLICAS QUE TRATEN DATOS PERSONALES.

Las funciones y obligaciones del personal adscrito al Departamento de Recursos Financieros en materia de protección de datos personales son:

Funciones:

- Dar a los datos personales (financieros, fiscales y de identidad) un tratamiento responsable, conforme a las medidas de seguridad establecidas.
- Salvaguardar la información personal y contable a la que se tenga acceso con motivo de las funciones financieras.
- Comprobar que el inventario de datos personales y de los sistemas de tratamiento estén ordenados y resguardados conforme a los periodos fiscales y normativos aplicables.
- Conservar actualizado el listado de personas usuarias que dan tratamiento a datos personales en el área financiera.
- Notificar de inmediato ante cualquier vulneración de seguridad de los datos personales y documentar los hechos mediante el Anexo correspondiente.

Obligaciones:

- Guardar estricta confidencialidad respecto a los datos personales, fiscales y económicos a los que se tenga acceso, incluso después de concluir la relación laboral.
- Limitar el tratamiento de los datos personales a las finalidades presupuestales, contables y fiscales previstas.
- Abstenerse de transferir, difundir o divulgar datos personales y financieros sin consentimiento o fundamento legal.

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

- Utilizar exclusivamente equipos, sistemas y medios institucionales autorizados.
- Custodiar los expedientes físicos y electrónicos en espacios con acceso restringido.

V. LOS DATOS PERSONALES TRATADOS EN LOS SISTEMAS DE TRATAMIENTOS Y/O BASE DE DATOS PERSONALES SON LOS SIGUIENTES:

Datos:

3. Nombre completo
4. Domicilio
5. Teléfono

➤ Documentos:

- [REDACTED]
- [REDACTED]

VI. LA DESCRIPCIÓN DEL SISTEMA DE TRATAMIENTO, SEÑALANDO EL TIPO DE SOPORTE Y LAS CARACTERÍSTICAS DEL LUGAR DONDE SE RESGUARDAN.

Descripción del Sistema de Tratamiento	Tipo de Soporte	Características del lugar de resguardo
1. Validación para el pago de la cuota de inscripción a la carrera seleccionada. ➤ Los datos obtenidos para el cobro de inscripción son únicamente de visualización.	Electronico. Sistema de Gestión de Matrícula Escolar; MindBox.	[REDACTED]

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

Descripción del Sistema de Tratamiento	Tipo de Soporte	Características del lugar de resguardo
2. Emisión, timbrado y envío de los comprobantes fiscales digitales (CFDI / facturas). ➤ Para el proceso de inscripción de los alumnos de nuevo ingreso, una vez verificando los datos en el Sistema de Gestión de Matrícula Escolar “MindBox”; se lleva a cabo el cobro correspondiente, a través de transferencias o del cobro en tarjeta; para posteriormente emitir el comprobante fiscal digital (CFDI / facturas); mismo que es entregado de forma inmediata al alumno, para los trámites correspondientes. ➤ Guarda y custodia en los expedientes para archivo y control.	Físico.	

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

Descripción del Sistema de Tratamiento	Tipo de Soporte	Características del lugar de resguardo
3. Integración de los estados financieros mensuales y cuenta pública trimestral e integración de los expedientes generados con las pólizas contables y su soporte. ➤ Se lleva a cabo el proceso, validación y consolidación de manera automatizada de las operaciones contables, presupuestarias y programáticas, permitiendo la generación oportuna de los estados financieros mensuales y su respectiva integración para la presentación de la Cuenta Pública Trimestral conforme a la normatividad aplicable. ➤ Guarda y custodia en los expedientes integrados con las pólizas correspondientes y su soporte	Físico y electrónico.	

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

Descripción del Sistema de Tratamiento	Tipo de Soporte	Características del lugar de resguardo
documental, para archivo y control.		
4. Pago a proveedores, prestadores de servicios y viáticos a personal comisionado. Se lleva a cabo el proceso de pago a través de transferencias electrónicas o la emisión de cheques; mediante la validación de facturas, contrarecibos, comprobantes, conciliación bancaria y control de flujo de efectivo para la dispersión oportuna y mediante la solicitud correspondiente para los viáticos solicitados.	Físico y electrónico	

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIPI) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

VII. LOS CONTROLES Y MECANISMOS DE SEGURIDAD PARA LAS TRANSFERENCIAS QUE, EN SU CASO, SE EFECTÚEN.

A continuación, se detalla las áreas tanto internas como externas que reciben información del Departamento de Recursos Financieros:

Áreas Internas:

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

➤ Subdirección de Servicios Administrativos

Uso de información:

- Integrar la información para dar seguimiento a los reportes oficiales;
- Atender solicitudes de información del TecNM, SEP y las autoridades, así como auditorías y requerimientos de transparencia.

Áreas externas:

- Secretaría de Finanzas

Uso de información:

- Reportar y reintegrar los ingresos obtenidos.
- Atender auditorías, evaluaciones, acreditaciones y requerimientos de rendición de cuentas.

MECANISMOS DE SEGURIDAD:

Para implementar las medidas de seguridad aplicables a la transferencia de datos personales, el receptor de la información asumirá el carácter de responsable conforme a la legislación en la materia al recibir dicha información mediante el traslado de soportes físicos, electrónicos o a través del correo electrónico institucional, por lo que deberá tratar los datos personales atendiendo y apegándose al aviso de privacidad del Departamento de Recursos Financieros, mismo que se encuentra publicado en:

<https://cintalapa.tecnm.mx/aviso-privacidad>

En cada una de estas modalidades se deberá sujetarse a lo siguiente:

A. Traslado de soportes físicos: Los datos personales se trasladan en documentos impresos que pueden leerse directamente, sin necesidad de un dispositivo que procese su contenido para consultarlo, modificarlo o almacenarlo.

Por ejemplo: cuando se emite la factura y se resguarda en los expedientes correspondientes.

B. Traslado físico de soportes electrónicos: Los datos personales se entregan al destinatario mediante archivos electrónicos almacenados en medios que requieren un dispositivo con circuitos electrónicos para consultar, modificar o almacenar su contenido.

Por ejemplo: cuando el Departamento de Recursos Financieros entrega mediante una memoria USB con los archivos digitalizados de expedientes para las entidades fiscalizadoras o las entidades requerientes.

[illegible]

XI. EL ANÁLISIS DE BRECHA.

- [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTIAIP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTIAPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones publicas.”

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

- [Redacted text block]
- [Redacted text block]
 - [Redacted text block]
 - [Redacted text block]
 - ❖ [Redacted text block]
 - ❖ [Redacted text block]

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

XII. LA GESTIÓN DE VULNERACIONES.

En caso de ocurrir alguna vulneración deberá registrarse en la bitácora de contingencias (Anexo 1), y se llevará a cabo conforme al siguiente procedimiento:

- **Detección y aviso interno:** El personal del departamento que detecte o sospeche de una vulneración, lo comunicará de inmediato a la Jefatura del Departamento, preservando el estado de los documentos, equipos o sistemas involucrados.
- **Contención:** Se ejecutarán acciones inmediatas para evitar mayor afectación, tales como resguardar el archivo, suspender accesos, cambiar contraseñas o desconectar el equipo comprometido.
- **Registro inicial:** Se asentará en la bitácora la fecha y hora de la vulneración, el documento o información vulnerada y el motivo de la vulneración.
- **Evaluación:** La Jefatura determinará el alcance del incidente, las personas titulares afectadas y si se comprometen sus derechos patrimoniales o morales.

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

- **Acciones correctivas y definitivas:** Se implementarán las medidas para restablecer la información y eliminar la causa, y se registrarán en la bitácora junto con el nombre de la persona que resolvió la vulneración.
- **Notificación:** Se informará a las personas titulares, dentro del plazo no mayor a 3 días (72 horas), la notificación incluirá la naturaleza del incidente, los datos personales comprometidos, las recomendaciones para la persona titular, las acciones correctivas realizadas y los medios para obtener más información. Se registrará en la bitácora la fecha y hora de cada notificación.
- **Cierre y prevención.** La Jefatura revisará las medidas de seguridad vigentes y ajustará las que resulten necesarias para evitar que el incidente se repita.

XIII. LAS MEDIDAS DE SEGURIDAD FÍSICAS APLICADAS A LAS INSTALACIONES.

[Redacted content]

XIV. LOS CONTROLES DE IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS.

[Redacted content]

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIPI) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPECHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

XV. LOS PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS PERSONALES.

XVI. EL PLAN DE CONTINGENCIA.

XVII. LAS TÉCNICAS UTILIZADAS PARA LA SUPRESIÓN Y BORRADO SEGURO DE LOS DATOS PERSONALES.

La documentación financiera, fiscal y contable sólo podrá suprimirse cuando hayan concluido los periodos de conservación y obligaciones fiscales, contables y archivísticas aplicables. Los documentos físicos cuya eliminación proceda deberán destruirse de manera que no puedan reconstruirse; los archivos electrónicos deberán borrarse de los equipos y medios institucionales mediante mecanismos que eviten su recuperación no autorizada.

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAI) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”



No deberán reutilizarse como papel de borrador pólizas, comprobantes, facturas u otros documentos que contengan datos personales, fiscales o bancarios.

XVIII. EL PLAN DE TRABAJO.

[Redacted text]

[Redacted text]

XIX. LOS MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD.

La Jefatura verificará los accesos a los equipos y sistemas, el estado de los expedientes físicos, las transferencias de información, las vulneraciones registradas y la disponibilidad de los respaldos institucionales.

Los resultados de las revisiones e incidentes deberán utilizarse para actualizar los controles y las medidas de seguridad cuando sea necesario.

XX. EL PROGRAMA GENERAL DE CAPACITACIÓN.

El personal del Departamento de Recursos Financieros deberá recibir capacitación sobre confidencialidad de datos financieros, fiscales y bancarios, uso seguro de MindBox y de los equipos institucionales, manejo de CFDI y expedientes contables, transferencias de información, bitácoras y respuesta a vulneraciones.

La capacitación deberá reforzarse cuando se modifiquen los procesos, plataformas, responsables o riesgos identificados por el Departamento.

ANEXO 1: Bitácora de vulneraciones a la seguridad de los Datos Personales

Órgano Administrativo (o área generadora/resguardante):

Instituto Tecnológico Superior de Cintalapa
Departamento de Recursos Financieros.

Responsable del Archivo:

Everardo Córdova Mandayapa
Jefe del Departamento de Recursos Financieros

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPECHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

Número consecutivo	Fecha y Hora Vulneración	Documento o información vulnerada	Motivo de la vulneración	Acciones correctivas y definitivas implementadas	Persona que resolvió la vulneración	Fecha y hora de notificación de la vulneración a los titulares de los datos personales comprometidos	Fecha en formato mes y año (Al que corresponde la bitácora)

ANEXO 2: Bitácora de vulneraciones a la seguridad de los Datos Personales

Órgano Administrativo (o área generadora/resguardante):

Instituto Tecnológico Superior de Cintalapa
Departamento de Recursos Financieros.

Responsable del Archivo:

Everardo Córdova Mandayapa
Jefe del Departamento de Recursos Financieros

Número consecutivo	Fecha y Hora Vulneración	Documento o información vulnerada	Motivo de la vulneración	Acciones correctivas y definitivas implementadas	Persona que resolvió la vulneración	Fecha y hora de notificación de la vulneración a los titulares de los datos personales comprometidos	Fecha en formato mes y año (Al que corresponde la bitácora)

DEPARTAMENTO DE RECURSOS MATERIALES Y SERVICIOS

II. NOMBRES DE LOS SISTEMAS DE TRATAMIENTO.

Los datos personales en posesión del Departamento de Recursos Materiales y Servicios son sometidos a los siguientes tratamientos:

1. Integración, revisión, control y resguardo de expedientes físicos y electrónicos de proveedores y contratistas.
2. Recepción y descarga de documentación de proveedores y contratistas remitida mediante correo electrónico institucional para su incorporación a expedientes.
3. Validación de documentación de identificación, fiscal, bancaria, domiciliaria y de representación legal necesaria para la contratación, adquisición de bienes o prestación de servicios.
4. Integración y transferencia controlada de documentación al Departamento de Recursos Financieros para la gestión y ejecución de pagos a proveedores y contratistas.

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

III. EL NOMBRE, CARGO Y ADSCRIPCIÓN DEL ADMINISTRADOR DEL SISTEMA DE TRATAMIENTO.

Los responsables del tratamiento de los Datos Personales del Departamento de Recursos Materiales y Servicios, son los que a continuación se describen:

Responsable	Cargo	Órgano Administrativo	Tratamiento
[REDACTED]	Jefa del Departamento de Recursos Materiales y Servicios. Responsable de la revisión de la documentación de los Proveedores y Contratistas, física y electrónica.	Departamento de Recursos Materiales y Servicios.	[REDACTED]
[REDACTED]	Vigilante Responsable de la entrega de documentación al Departamento de Recursos Financieros para que puedan emitir el pago correspondiente.	Departamento de Recursos Materiales y Servicios– Área de Apoyo.	[REDACTED]

IV. LAS FUNCIONES Y OBLIGACIONES DEL RESPONSABLE Y TODAS LAS PERSONAS SERVIDORAS PÚBLICAS QUE TRATEN DATOS PERSONALES.

Las funciones y obligaciones del responsable y de todas las personas servidoras públicas que traten datos personales en el Departamento de Recursos Materiales y Servicios son las siguientes:

Funciones:

- Dar a los datos personales de los proveedores un tratamiento responsable, conforme a las medidas de seguridad establecidas para tal efecto;
- Salvaguardar los datos personales a los que se tenga acceso;
- Comprobar que el inventario de datos personales y de los sistemas de tratamiento a los que tengan acceso estén ordenados, y su resguardo corresponda a su periodo de atención y gestión;
- Conservar el listado actualizado de personas usuarias que den tratamiento a datos personales;

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIPI) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

- Ante un incidente de vulneración de seguridad de los datos personales o de sus sistemas de tratamiento, notificar de inmediato a la persona titular y documentar los hechos, mediante el Anexo 2.

Obligaciones:

9. Llevar a cabo permanentemente las medidas de seguridad necesarias para la protección de los datos personales, evitando daño, pérdida, alteración, destrucción o uso, acceso o tratamiento no autorizado, así como también garantizar la confidencialidad, integridad y disponibilidad de los mismos.
10. Acatar los mecanismos para asegurar que los datos personales a los que tengan acceso en el ejercicio de sus atribuciones no se difundan, distribuyan o comercialicen.
11. Utilizar únicamente los equipos, sistemas y medios institucionales autorizados para el tratamiento de los datos personales;
12. Guardar confidencialidad sobre la información que se conozca en el desarrollo de sus actividades.

V. LOS DATOS PERSONALES TRATADOS EN LOS SISTEMAS DE TRATAMIENTOS Y/O BASE DE DATOS PERSONALES SON LOS SIGUIENTES:

Datos:

- Nombres y Apellidos.
- Credencial para Votar.
- Clave Única de Registro de Población.
- Registro Federal de Contribuyente.
- Comprobante de Domicilio.
- Número de Teléfono Fijo o Celular.
- Correo Electrónico.
- Número de Seguridad Social.
- Firma.
- Datos Bancarios.
- Poder Notarial.
- Constancia de Situación Fiscal.

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

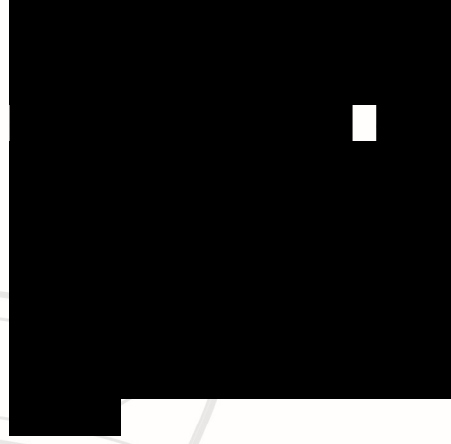
Documentos:

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

VI. LA DESCRIPCIÓN DEL SISTEMA DE TRATAMIENTO, SEÑALANDO EL TIPO DE SOPORTE Y LAS CARACTERÍSTICAS DEL LUGAR DONDE SE RESGUARDAN.

Descripción del Sistema de Tratamiento	Tipo de Soporte	Características del lugar de resguardo
1. Integración de datos personales de los proveedores o contratistas se resguardan de manera Físicas y electrónicas.	Físico y Electrónico.	[REDACTED]

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAI) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

2. Los datos personales son descargados del correo electrónico posterior ingresados en los expedientes.	Físico y Electrónico 	
--	---	--

VII. LOS CONTROLES Y MECANISMOS DE SEGURIDAD PARA LAS TRANSFERENCIAS QUE, EN SU CASO, SE EFECTÚEN.

A continuación, se detalla las áreas tanto internas como externas que reciben información del Departamento de Recursos Materiales y Servicios:

Áreas Internas:

- Subdirección de Servicios Administrativos.
- Departamento de Financieros

Uso de información:

- Elaboración de los formatos del pago de proveedores o contratistas.
- Entrega de documentación al Departamento de Recursos Financieros para que ejecute su respectivo pago;
- Atender solicitudes de compra con proveedores o contratistas.
- Subdirección de Servicios Administrativos.

Uso de información:

- Analizar y dictaminar la documentación del proveedor que sea factible para adquirir el servicio o la adquisición de productos;
- Firmar y validar documentos.
- Departamento de Recursos Financieros.

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

Uso de información:

- Revisión de documentos;
- Entrega documentación firmada y validada para su respectivo pago.

Mecanismos de seguridad:

Para implementar las medidas de seguridad aplicables a la transferencia de datos personales el receptor de los datos personales asumirá el carácter de responsable conforme a la legislación en la materia al recibir dicha información mediante el traslado de soportes físicos, electrónicos o a través del correo electrónico institucional, por lo que deberá tratar los datos personales atendiendo y apegándose al aviso de privacidad del Departamento de Recursos Materiales y Servicios, mismo que se encuentra publicado en:

<https://cintalapa.tecnm.mx/aviso-privacidad>

En cada una de estas modalidades se deberá sujetarse a lo siguiente:

A. Traslado de soportes físicos: Los datos personales se trasladan en documentos impresos que pueden leerse directamente, sin necesidad de un dispositivo que procese su contenido para consultarlo, modificarlo o almacenarlo. Por ejemplo: cuando el Departamento de Recursos Materiales y Servicios remite por correo electrónico institucional oficial oficios, formatos, o copias de documentos del expediente del los proveedores o contratistas al Departamento de Financieros.

B. Traslado físico de soportes electrónicos: En esta modalidad se trasladan físicamente para entregar al destinatario los datos personales en archivos electrónicos contenidos en medios de almacenamiento que requieren el uso de algún aparato con circuitos electrónicos que procesen su contenido para examinar, modificar o almacenar la información.

Por ejemplo: cuando el Departamento de Recursos Materiales y Servicios entrega a otra por mensajería oficial un archivo electrónico con datos personales contenidos en discos compactos o dispositivos de memoria USB, entre otros.

C. Traslado sobre redes electrónicas: Los datos personales se transmiten en archivos electrónicos a través de una red electrónica.

Por ejemplo: cuando se envía un archivo electrónico con la información de los proveedores a una Dependencia o Entidad por internet.

VIII. EL RESGUARDO DE LOS SOPORTES FÍSICOS DE LOS DATOS PERSONALES.

Los expedientes físicos se encuentran resguardos y en custodia de los responsables del sistema de tratamiento de los datos personales en el departamento asignada para tal efecto.

IX. LAS BITÁCORAS DE ACCESO Y VULNERACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES.

Los datos que se registran en la Bitácora de acceso (anexo 1) son los siguientes:

- Número consecutivo;
- Quien accede a los datos personales (Nombre completo);
- Cargo;
- Área o departamento de adscripción;
- Propósito del acceso;
- Tipo de soporte utilizado (Expediente o registro electrónico);
- Fecha en formato mes y año (Al que corresponde la bitácora).

Los datos que se registran en la Bitácora de vulneraciones (anexo 2) son los siguientes:

- Número consecutivo;
- Fecha y hora de la vulneración;
- Documento o información vulnerada;
- Motivo de la vulneración;
- Acciones correctivas y definitivas implementadas;
- Persona que resolvió la vulneración;
- Fecha y hora de notificación de la vulneración a los titulares de los datos personales comprometidos;
- Fecha en formato mes y año (Al que corresponde la bitácora).

X. EL ANÁLISIS DE RIESGOS.



“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPECHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”



[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

- [REDACTED]
- ❖ [REDACTED]
- ❖ [REDACTED]
- ❖ [REDACTED]
- [REDACTED]
- ❖ [REDACTED]
- ❖ [REDACTED]

XII. LA GESTIÓN DE VULNERACIONES.

En caso de ocurrir alguna vulneración deberá registrarse en la bitácora de contingencias (Anexo 2), y se llevará a cabo conforme al siguiente procedimiento:

- **Detección y aviso interno:** El personal del departamento que detecte o sospeche de una vulneración lo comunicará de inmediato a la Jefatura del Departamento de Recursos Materiales y Servicios, preservando el estado de los documentos, equipos o sistemas involucrados.
- **Contención:** Se ejecutarán acciones inmediatas para evitar mayor afectación, tales como resguardar el archivo, suspender accesos, cambiar contraseñas o desconectar el equipo comprometido.
- **Registro inicial:** Se asentará en la bitácora la fecha y hora de la vulneración, el documento o información vulnerada y el motivo de la vulneración.
- **Evaluación:** La Jefatura determinará el alcance del incidente, las personas titulares afectadas y si se comprometen sus derechos patrimoniales o morales.
- **Acciones correctivas y definitivas:** Se implementarán las medidas para restablecer la información y eliminar la causa, y se registrarán en la bitácora junto con el nombre de la persona que resolvió la vulneración.
- **Notificación:** Se informará a las personas titulares, sin dilación alguna y dentro del plazo no mayor a 3 días (72 horas), la notificación incluirá la naturaleza del incidente, los datos personales comprometidos, las recomendaciones para la persona titular, las acciones correctivas realizadas y los medios para obtener mayor información. Se registrará en la bitácora la fecha y hora de cada notificación.
- **Cierre y prevención.** El Departamento revisará las medidas de seguridad vigentes y ajustará las que resulten necesarias para evitar que el incidente se repita.

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”



XIII. LAS MEDIDAS DE SEGURIDAD FÍSICAS APLICADAS A LAS INSTALACIONES.

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

XIV. LOS CONTROLES DE IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS.

- [Redacted]

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAI) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPECHS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

➤ [Redacted]

XV. LOS PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS PERSONALES.

➤ [Redacted]

➤ [Redacted]

XVI. EL PLAN DE CONTINGENCIA.

➤ [Redacted]

➤ [Redacted]

XVII. LAS TÉCNICAS UTILIZADAS PARA LA SUPRESIÓN Y BORRADO SEGURO DE LOS DATOS PERSONALES.

- Los expedientes de proveedores y contratistas y sus archivos electrónicos sólo podrán eliminarse cuando hayan cumplido los plazos de conservación y las obligaciones administrativas, contractuales, fiscales y archivísticas aplicables. Los documentos físicos cuya eliminación proceda deberán destruirse de manera que los datos de identificación, fiscales y bancarios no puedan reconstruirse; los archivos electrónicos deberán eliminarse de forma segura.
- No deberán reutilizarse como papel de borrador documentos que contengan identificaciones, RFC, datos bancarios, poderes notariales, firmas u otros datos personales.

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIIP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

XVIII. EL PLAN DE TRABAJO.



XIX. LOS MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD.

- La Jefatura deberá revisar el estado de los archiveros y equipos, los accesos a la información, las transferencias documentales, las bitácoras de acceso y vulneraciones y los respaldos de archivos electrónicos.
- Los cambios en los procesos o la aparición de nuevos riesgos deberán reflejarse en la actualización de las medidas de seguridad del área.

XX. EL PROGRAMA GENERAL DE CAPACITACIÓN.

- El personal que trate expedientes de proveedores y contratistas deberá recibir capacitación sobre confidencialidad de datos de identificación, fiscales y bancarios, manejo seguro del correo institucional y equipos de cómputo, transferencias al Departamento de Recursos Financieros, uso de bitácoras y atención de vulneraciones.
- La capacitación deberá reforzarse cuando cambien los procesos, el personal autorizado o los riesgos identificados.

ANEXO 1: BITÁCORA DE ACCESO A LOS DATOS PERSONALES

Órgano Administrativo (o área generadora/resguardante):

Instituto Tecnológico Superior de Cintalapa
Departamento de Recursos Materiales y Servicios.

Responsable del Archivo:

Laura Elena Cruz Ángel
Jefa del Departamento de Recursos Materiales y Servicios

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

Número consecutivo	Quien accede a los datos personales (Nombre completo)	Cargo	Área de adscripción	Propósito del acceso	Tipo de soporte utilizado (Expediente o registro electrónico)	Fecha en formato mes y año (Al que corresponde la bitácora)

ANEXO 2: Bitácora de vulneraciones a la seguridad de los Datos Personales

Órgano Administrativo (o área generadora/resguardante):

Instituto Tecnológico Superior de Cintalapa

Departamento de Recursos Materiales y Servicios.

Responsable del Archivo:

Laura Elena Cruz Ángel

Jefa del Departamento de Recursos Materiales y Servicios

Número consecutivo	Fecha y Hora Vulneración	Documento o información vulnerada	Motivo de la vulneración	Acciones correctivas y definitivas implementadas	Persona que resolvió la vulneración	Fecha y hora de notificación de la vulneración a los titulares de los datos personales comprometidos	Fecha en formato mes y año (Al que corresponde la bitácora)

DEPARTAMENTO DE RESIDENCIAS PROFESIONALES Y SERVICIO SOCIAL

II. NOMBRES DE LOS SISTEMAS DE TRATAMIENTO.

Los datos personales en posesión del Departamento de Residencias Profesionales y Servicio Social son sometidos a los siguientes tratamientos:

- Registro y validación de constancias de vigencia de seguro IMSS.
- Integración, control y resguardo de expedientes digital y físico de los asesores (SIGA).

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

- Integración, control y resguardo de expedientes digital y físico de los educandos (SIGA).
- Registro y validación de expedientes de los alumnos a la aseguradora THONA.

III. EL NOMBRE, CARGO Y ADSCRIPCIÓN DEL ADMINISTRADOR DEL SISTEMA DE TRATAMIENTO.

Los responsables del tratamiento de los datos personales del Departamento de Residencias Profesionales y Servicio Social son los que se describen a continuación:

Responsable	Cargo	Órgano Administrativo	Tratamiento
[REDACTED]	Subdirectora	Subdirectora De Vinculación	[REDACTED]
[REDACTED]	Jefe Del Departamento	Departamento Residencia Profesional Y Servicio Social	[REDACTED]

IV. LAS FUNCIONES Y OBLIGACIONES DEL RESPONSABLE Y TODAS LAS PERSONAS SERVIDORAS PÚBLICAS QUE TRATEN DATOS PERSONALES.

Funciones:

- Tratar los datos personales de la comunidad estudiantil con responsabilidad y bajo las medidas de seguridad que se hayan establecido para tal fin en los procesos de Residencias Profesionales y Servicio Social.
- Resguardar los expedientes físicos y electrónicos de Residencias Profesionales y Servicio Social a los que tengan acceso en el ejercicio de sus atribuciones.

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIIP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

- Verificar que el inventario de datos personales contenidos en los Anexos del manual del TecNM y los sistemas de tratamiento de los mismos se encuentren permanentemente actualizados.
- Llevar un registro de las personas servidoras públicas y personal de apoyo del departamento que accedan a los datos personales, implementando acciones necesarias para la autenticación de usuarios.
- Mantener actualizada la relación de usuarios autorizados que traten datos de alumnos de la institución.
- En caso de que se presente algún incidente de vulneración de seguridad de los datos personales y/o de los archivos físicos o electrónicos del Departamento de Residencias Profesionales y Servicio Social, informar sin dilación alguna a la persona superior jerárquica y a la Autoridad Garante.

Obligaciones:

- Llevar a cabo permanentemente las medidas de seguridad necesarias para la protección de los datos personales de los estudiantes, evitando daño, pérdida, alteración, destrucción o uso, acceso o tratamiento no autorizado, así como también garantizar la confidencialidad, integridad y disponibilidad de los mismos.
- Acatar los mecanismos para asegurar que las calificaciones, historiales académicos y datos de contacto a los que tengan acceso no se difundan, distribuyan o comercialicen con entes ajenos a los fines institucionales.
- Guardar estricta confidencialidad sobre la información médica, de salud o el desempeño cualitativo de los alumnos que conozcan en el desarrollo de sus actividades.

V. LOS DATOS PERSONALES TRATADOS EN LOS SISTEMAS DE TRATAMIENTOS Y/O BASE DE DATOS PERSONALES SON LOS SIGUIENTES:

- Nombres y Apellidos
- Número de Control Escolar
- Carrera y Plan de Estudios
- Clave Única de Registro de Población (CURP)
- Registro Federal de Contribuyentes (RFC)
- Domicilio Particular
- Número de Teléfono Fijo o Celular

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

- Correo Electrónico Institucional y Personal
- Número de Seguridad Social / Afiliación Médica (IMSS, ISSSTE, etc.)
- Firma del Estudiante
- Historial Académico / Créditos Cursados
- Datos Generales de la Dependencia o Empresa Receptora
- Nombre del Asesor Interno y Asesor Externo
- Evaluaciones de Desempeño Cualitativo y Cuantitativo
- Edad
- Género
- Lugar y Fecha de Nacimiento

Adicional a lo anterior, se recaban datos personales que se consideran sensibles, como lo es el estado de salud y afecciones físicas detalladas en los términos de responsabilidades médicas para riesgos y accidentes de trabajo en Residencias Profesionales, así como padecimientos especiales reportados para la asignación de Servicio Social comunitario.

VI. LA DESCRIPCIÓN DEL SISTEMA DE TRATAMIENTO, SEÑALANDO EL TIPO DE SOPORTE Y LAS CARACTERÍSTICAS DEL LUGAR DONDE SE RESGUARDAN.

Descripción del Sistema de Tratamiento	Tipo de Soporte	Características del lugar de resguardo
1. Los datos personales son de los alumnos para inscripción IMSS (constancia de vigencia de derecho).	Físico	[REDACTED]
2. Los datos personales para tramites del SEGUROS THONA	Físicos y Digitales	[REDACTED]
3. Los datos personales de los asesores del programa Chiapas Puede	Físicos y Digitales	[REDACTED]

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPECHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

		
➤ Los datos personales de los educandos del programa Chiapas Puede	digitales	

VII. LOS CONTROLES Y MECANISMOS DE SEGURIDAD PARA LAS TRANSFERENCIAS QUE, EN SU CASO, SE EFECTÚEN.

Para implementar las medidas de seguridad aplicables a las transferencias de datos personales realizadas por el Departamento de Residencias Profesionales y Servicio Social para los trámites y sistemas descritos en este documento, la información deberá remitirse únicamente a las empresas, dependencias, organismos receptores, aseguradora o plataformas oficiales que correspondan a la finalidad del tratamiento. Sólo se transferirán los datos necesarios y se utilizarán medios institucionales, atendiendo al aviso de privacidad y a las disposiciones aplicables.

- **Traslado de soportes físicos:** En esta modalidad los datos personales se trasladan en medios de almacenamiento que se descifran a simple vista y que no requieren de ningún aparato que procese su contenido para examinar, modificar o almacenar la información. por ejemplo, todos los documentos se encuentran en recopiladores. en el departamento de residencias profesionales y servicio social.
- **Traslado físico de soportes electrónicos:** En esta modalidad se trasladan físicamente para entregar al destinatario los datos personales en archivos electrónicos contenidos en medios de almacenamiento que requieren el uso de algún aparato con circuitos electrónicos que procesen su contenido para examinar, modificar o almacenar la información. Por ejemplo, cuando se entrega en memoria USB.
- **Traslado sobre redes electrónicas:** En esta modalidad se transmiten archivos o se capturan datos mediante redes y plataformas oficiales. Esto comprende, según el tratamiento correspondiente, la carga de información en THONA SEGUROS y en SIGA Chiapas Puede, así como los envíos institucionales indispensables para el seguimiento de Residencias Profesionales y Servicio Social.

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

VIII. EL RESGUARDO DE LOS SOPORTES FÍSICOS DE LOS DATOS PERSONALES.

Los expedientes físicos que contienen la documentación de Residencias Profesionales Y Servicio Social, de los alumnos se encuentran resguardados y en custodia del personal autorizado en el área asignada para tal efecto dentro de las oficinas, concretamente en el edificio de la Subdirección de Vinculación del Instituto Tecnológico Superior de Cintalapa.

IX. LAS BITÁCORAS DE ACCESO Y VULNERACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES.

Los datos que se registran en la Bitácora de acceso (Anexo 1) para revisar expedientes y registros del Departamento de Residencias Profesionales y Servicio Social son los siguientes:

- Quien accede a los datos personales del alumno, cargo y adscripción;
- Fecha y hora en la que se realiza el acceso o se intenta el mismo, así como fecha y hora de salida;
- Propósito del acceso (ej. validación de liberación de créditos o auditoría académica);
- Número de control o del expediente utilizado;
- Tipo de soporte; y
- Firma de quien autoriza el acceso.

Los datos que se registran en la Bitácora de vulneraciones (Anexo 2) son los siguientes:

- Fecha y hora de la vulneración;
- Motivo de la vulneración (ej. pérdida de expediente físico, robo de equipo informático o acceso no autorizado a carpetas compartidas);
- Acciones correctivas y definitivas implementadas;
- Persona que resolvió la vulneración;
- Fecha y hora de notificación de la vulneración a los estudiantes afectados y a la Autoridad Garante en materia de protección de datos personales; y
- Los oficios, documentos, expedientes, estantes o archiveros dañados y los recuperados.

X. EL ANÁLISIS DE RIESGOS.



“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIPI) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

➤ [Redacted text]

➤ [Redacted text]

➤ [Redacted text]

➤ [Redacted text]

➤ [Redacted text]

➤ [Redacted text]

[Redacted text]

Amenaza	Vulnerabilidades	Posibles consecuencias
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

XI. EL ANÁLISIS DE BRECHA.

- [illegible]

XII. LA GESTIÓN DE VULNERACIONES.

En caso de ocurrir alguna vulneración de seguridad que afecte la confidencialidad, integridad o disponibilidad de los expedientes físicos, bases de datos o sistemas de control del Departamento de Residencias Profesionales Y Servicio Social (tales como la pérdida de formatos de

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIIP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

evaluación, extravío de reportes bimestrales o filtración de datos de los residentes, datos de las instituciones privadas), será obligatorio registrar el evento sin dilación en la bitácora de vulneraciones del área. Asimismo, se deberá informar de forma inmediata a la Dirección del Instituto, al Comité de Transparencia institucional y a la Autoridad Garante competente.

Tan pronto como se confirme la vulneración y se inicien las acciones técnicas y administrativas para dimensionar el alcance de la afectación, el Jefe del Departamento de Residencias Profesionales Y Servicio Social (o el administrador del sistema de tratamiento) notificará formalmente a la persona afectada para que este pueda tomar las medidas conducentes a la defensa de sus derechos. Dicha notificación oficial deberá contener, como mínimo, los siguientes elementos:

- **La naturaleza del incidente:** Descripción detallada del tipo de vulneración ocurrida en los archivos del departamento (físico, electrónico o de red).
- **Los datos personales comprometidos:** Listado específico de la información expuesta.
- **Recomendaciones de protección:** Acciones y medidas preventivas sugeridas que la persona afectada puede adoptar de forma inmediata para salvaguardar sus intereses personales.
- **Acciones correctivas inmediatas:** Detalle de las contingencias técnicas o administrativas aplicadas por el departamento para contener la vulneración y mitigar el riesgo.
- **Medios de contacto institucionales:** Canales informativos oficiales del Instituto donde el titular puede solicitar orientación y seguimiento sobre el estatus de su información.

Una vez contenida la eventualidad, el jefe del Departamento de Residencias Profesionales Y Servicio Social, en coordinación con el personal auxiliar y el área de sistemas del Instituto, analizará de manera colegiada las causas raíz que originaron la falla. Las conclusiones del análisis se integrarán formalmente como acciones preventivas y correctivas dentro del plan de trabajo anual del departamento, con el objetivo de robustecer los controles físicos y digitales y evitar la reincidencia del incidente.

Finalmente, el responsable del Departamento establecerá los mecanismos de supervisión necesarios para asegurar que toda persona servidora pública, asesora interna, personal de apoyo o prestadora de servicio que intervenga en el tratamiento de datos de Residencias Profesionales, Servicio Social, IMSS, THONA SEGUROS o SIGA Chiapas Puede guarde estricta confidencialidad. Esta obligación subsistirá incluso después de concluida la relación laboral, académica o de prestación de servicios con el área.



XIII. LAS MEDIDAS DE SEGURIDAD FÍSICAS APLICADAS A LAS INSTALACIONES.

- [REDACTED]
- [REDACTED]
- [REDACTED]

XIV. LOS CONTROLES DE IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS.

[REDACTED]

XV. LOS PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS PERSONALES.

[REDACTED]

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

XVI. EL PLAN DE CONTINGENCIA.

-
-
-
-
-
-
-

XVII. LAS TÉCNICAS UTILIZADAS PARA LA SUPRESIÓN Y BORRADO SEGURO DE LOS DATOS PERSONALES.

A fin de dar cumplimiento al principio de temporalidad y asegurar que la información confidencial de alumnos o entidades particulares no permanezca expuesta tras haber cumplido

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

su finalidad legal y académica, el departamento implementará los siguientes mecanismos de eliminación definitiva:

- **Destrucción segura de documentos físicos:** Los formatos, copias de identificaciones oficiales, historiales académicos o borradores erróneos que contengan datos personales de los estudiantes no serán desechados bajo ninguna circunstancia en contenedores de basura común. Una vez transcurridos los plazos de retención académica obligatorios, los documentos impresos deberán ser destruidos en su totalidad mediante el uso de una máquina trituradora de papel de corte cruzado o por medio de incineración controlada en las instalaciones del Instituto.
- **Borrado seguro de archivos digitales y medios electrónicos:**
Para la depuración de los equipos de cómputo del departamento, servidores locales o unidades portátiles (USB o discos externos), se emplearán herramientas de software autorizadas por el área de sistemas de la universidad que realicen un borrado lógico e irreversible. Este procedimiento asegura que los datos personales contenidos en hojas de cálculo de control interno o versiones preliminares de reportes de residencia no puedan ser recuperados mediante programas de reconstrucción informática.
- **Fijación de periodos de retención institucional:** El Jefe del Departamento de Residencias Profesionales Y Servicio Social en estricto apego al catálogo de disposición documental del TecNM, revisará anualmente el archivo de trámite y concentración de la oficina para identificar los expedientes históricos de alumnos liberados que ya hayan cumplido sus vigencias de conservación técnica y legal, programando su depuración formal.
- **Prohibición de reutilización de soportes documentales:** Queda estrictamente prohibido utilizar como papel de reúso para notas internas, borradores de correspondencia o actividades administrativas diarias de la oficina, cualquier tipo de documento impreso que contenga nombres, números de control, datos médicos, calificaciones o firmas autógrafas de los estudiantes o de los asesores externos de los sectores productivos.

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

XVIII. EL PLAN DE TRABAJO.

❖	
❖	
❖	
❖	

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

XIX. LOS MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD.

El resguardo de los datos personales tratados por el Departamento de Residencias Profesionales y Servicio Social exige una supervisión continua. La Jefatura del Departamento revisará periódicamente los riesgos, amenazas, vulnerabilidades, incidentes y la efectividad de los controles aplicados a los expedientes físicos, archivos electrónicos y plataformas utilizadas en sus tratamientos.

Dichos mecanismos se ejecutarán mediante las siguientes directrices:

- Auditoría física semestral: La Jefatura del Departamento de Residencias Profesionales y Servicio Social realizará revisiones de control a las gavetas, archiveros y expedientes del área, verificando la integridad de las cerraduras, la ausencia de factores de riesgo físico y el correcto llenado de la Bitácora de Acceso (Anexo 1).
- Monitoreo digital y de accesos: Revisión periódica de los privilegios y contraseñas de acceso a los archivos electrónicos y a las plataformas THONA SEGUROS y SIGA Chiapas Puede, procurando que sólo el personal autorizado pueda consultar o modificar la información tratada por el Departamento.

- **Evaluación de incidentes e integración de nuevas amenazas:** Ante la detección de cualquier falla menor en los sistemas informáticos o en el manejo físico de los documentos, el departamento evaluará de forma inmediata las causas del incidente, actualizando la matriz de riesgos y modificando el presente documento normativo si las circunstancias tecnológicas o el entorno universitario lo demandan.

XX. EL PROGRAMA GENERAL DE CAPACITACIÓN.

Con el propósito de concientizar a los actores involucrados en el flujo de información de Residencias Profesionales Y Servicio Social y mitigar los riesgos derivados del factor humano, se formaliza el siguiente programa general de capacitación en la materia:

13. **Sensibilización institucional en el aula y la oficina:** Diseñar campañas informativas breves dirigidas a los alumnos solicitantes y al personal administrativo del departamento respecto a la importancia de proteger su privacidad y el manejo restringido de su información en el entorno universitario laboral.
14. **Capacitación sobre Derechos ARCO y Portabilidad de Datos:** Instruir puntualmente a las personas servidoras públicas y enlaces asignados a las ventanillas de atención del departamento sobre los mecanismos, medios y plazos legales disponibles para orientar de manera correcta al estudiante que desee ejercer sus derechos de Acceso, Rectificación, Cancelación u Oposición sobre sus expedientes de Servicio Social y Residencias.
15. **Concientización sobre el uso del Aviso de Privacidad:** Capacitar de manera obligatoria al personal encargado de recabar los datos de los estudiantes sobre el deber ineludible de poner a la vista e informar de manera presencial o digital el Aviso de Privacidad correspondiente antes de capturar cualquier dato personal.
16. **Formación específica sobre directrices de seguridad:** Instruir periódicamente a la Jefatura del Departamento, al personal administrativo y a las personas que intervengan en los trámites de Residencias Profesionales y Servicio Social sobre el resguardo de expedientes, el uso seguro de THONA SEGUROS y SIGA Chiapas Puede, el manejo de información de afiliación al IMSS y la aplicación de las medidas administrativas, físicas y técnicas previstas en este Documento de Seguridad.
17. **Asesoramiento práctico para la mejora continua del área:** Brindar acompañamiento técnico continuo al personal de apoyo de la oficina para asegurar el correcto llenado de las bitácoras internas de contingencia, las pruebas de borrado seguro de datos digitales y la observancia general de este Documento de Seguridad para garantizar el blindaje permanente de la información estudiantil.

ANEXO 1: BITÁCORA DE ACCESO A LOS DATOS PERSONALES DEL DEPARTAMENTO DE RESIDENCIA PROFESIONALES Y SERVICIO SOCIAL.

Órgano Administrativo: Departamento de Residencia Profesional y Servicio Social.

Responsable del Archivo: Jefe(a) del Departamento de Residencia Profesional y Servicio Social.

No. Seg.	Nombres y Apellidos	Cargo y Adscripción	Fecha y Hora de Entrada	Fecha y Hora de Salida	Motivo del Acceso	Número de Control	Tipo de Soporte	Firma De Vo. Bo.
1								

ANEXO 2: BITÁCORA DE VULNERACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES DEL DEPARTAMENTO DE RESIDENCIA PROFESIONALES Y SERVICIO SOCIAL.

Órgano Administrativo: Departamento de Residencia Profesional y Servicio Social.

Responsable del Archivo: Jefe(a) del Departamento de Residencia Profesional y Servicio Social.

No. Seg.	Fecha y Hora Vulneración	Causa e Identificación de Vulneración	Acciones Correctivas Aplicadas	Acciones Definitivas de Blindaje	Fecha de Notificación al Titular	Fecha de Notificación a la Autoridad	Datos/ Expedientes Afectados
1							

SUBDIRECCION DE VINCULACION

II. NOMBRES DE LOS SISTEMAS DE TRATAMIENTO.

Los datos personales en posesión de la subdirección de Vinculación son sometidos a los siguientes tratamientos:

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

- Validación de solicitudes para la asignación y cumplimiento del Servicio Social.
- Integración, control y resguardo de expedientes escolares de prestadores de Servicio Social.
- Validación de cartas de presentación oficiales de Servicio Social dirigidas a dependencias externas.
- Emisión y validación de constancias de terminación y liberación de Servicio Social.
- Validación de convenios específicos y bases de concertación con los sectores productivos, públicos y privados para Residencias Profesionales.
- Validación emisión de cartas de presentación oficiales para residentes hacia las empresas u organismos receptores.
- Validación y resguardo de los reportes preliminares, reportes finales y formatos de evaluación cualitativa de la Residencia Profesional.

III. EL NOMBRE, CARGO Y ADSCRIPCIÓN DEL ADMINISTRADOR DEL SISTEMA DE TRATAMIENTO.

Los responsables del tratamiento de los datos personales en la Subdirección de Vinculación y sus áreas adscritas son los que se describen a continuación:

Responsable	Cargo	Órgano Administrativo	Tratamiento
[REDACTED]	Subdirectora	Subdirectora De Vinculación	[REDACTED]
[REDACTED]	Jefe del Departamento de Vinculación	Departamento de Vinculación	[REDACTED]
[REDACTED]	Auxiliar de Oferta Educativa	Departamento de Vinculación	[REDACTED]
[REDACTED]	Jefe Del Departamento	Departamento Residencia Profesional Y Servicio Social	[REDACTED]

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIPI) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHEIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

--	--	--	--

IV. LAS FUNCIONES Y OBLIGACIONES DEL RESPONSABLE Y TODAS LAS PERSONAS SERVIDORAS PÚBLICAS QUE TRATEN DATOS PERSONALES.

Funciones:

- Tratar los datos personales de la comunidad estudiantil con responsabilidad y bajo las medidas de seguridad que se hayan establecido para tal fin en los procesos de vinculación y residencias profesionales y servicio social.
- Resguardar los expedientes físicos y electrónicos en los procesos de vinculación y residencias profesionales y servicio social.
- Verificar que el inventario de datos personales contenidos en los Anexos del manual del TecNM y los sistemas de tratamiento de los mismos se encuentren permanentemente actualizados.
- Llevar un registro de las personas servidoras públicas y personal de apoyo del departamento que accedan a los datos personales, implementando acciones necesarias para la autenticación de usuarios.
- Mantener actualizada la relación de usuarios autorizados que traten datos de alumnos de la institución.
- En caso de que se presente algún incidente de vulneración de seguridad de los datos personales y/o de los archivos físicos de vinculación, informar sin dilación alguna a la persona superior jerárquica y a la Autoridad Garante.

Obligaciones:

- Llevar a cabo permanentemente las medidas de seguridad necesarias para la protección de los datos personales de los estudiantes, evitando daño, pérdida, alteración, destrucción o uso, acceso o tratamiento no autorizado, así como también garantizar la confidencialidad, integridad y disponibilidad de los mismos.
- Acatar los mecanismos para asegurar que las calificaciones, historiales académicos y datos de contacto a los que tengan acceso no se difundan, distribuyan o comercialicen con entes ajenos a los fines institucionales.
- Guardar estricta confidencialidad sobre la información médica, de salud o el desempeño cualitativo de los alumnos que conozcan en el desarrollo de sus actividades.

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

V. LOS DATOS PERSONALES TRATADOS EN LOS SISTEMAS DE TRATAMIENTOS Y/O BASE DE DATOS PERSONALES SON LOS SIGUIENTES:

- Nombres y Apellidos
- Número de Control Escolar
- Carrera y Plan de Estudios
- Clave Única de Registro de Población (CURP)
- Registro Federal de Contribuyentes (RFC)
- Domicilio Particular
- Número de Teléfono Fijo o Celular
- Correo Electrónico Institucional y Personal
- Número de Seguridad Social / Afiliación Médica (IMSS, ISSSTE, etc.)
- Firma del Estudiante
- Historial Académico / Créditos Cursados
- Datos Generales de la Dependencia o Empresa Receptora
- Nombre del Asesor Interno y Asesor Externo
- Evaluaciones de Desempeño Cualitativo y Cuantitativo
- Edad
- Género
- Lugar y Fecha de Nacimiento

Adicional a lo anterior, se recaban datos personales que se consideran sensibles, como lo es el estado de salud y afecciones físicas detalladas en los términos de responsabilidades médicas para riesgos y accidentes de trabajo en Residencias Profesionales, así como padecimientos especiales reportados para la asignación de Servicio Social comunitario.

VI. LA DESCRIPCIÓN DEL SISTEMA DE TRATAMIENTO, SEÑALANDO EL TIPO DE SOPORTE Y LAS CARACTERÍSTICAS DEL LUGAR DONDE SE RESGUARDAN.

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

Descripción del Sistema de Tratamiento	Tipo de Soporte	Características del lugar de resguardo
1. Los datos personales son inscritos en la Solicitud de Servicio Social y la Carta Compromiso, integrándose formalmente al expediente individual de control de vinculación.	Físico	[Redacted]
2. Se emite la Carta de Presentación de Servicio Social, transfiriendo el nombre, número de control y carrera a las dependencias públicas o privadas que fungen como unidades receptoras autorizadas.	Físico y Electrónico	[Redacted]
3. Los Reportes Bimestrales y los Formatos de Evaluación Cualitativa son recopilados periódicamente para registrar los niveles de desempeño (excelente, notable, bueno, suficiente) de los prestadores.	Físico y Electrónico	[Redacted]
4. Se elaboran los expedientes de control y seguimiento de candidatos a Residencias Profesionales, validando su estatus y adjuntando la Carta de Presentación oficial hacia los sectores productivos o sociales.	Físico y Electrónico	[Redacted]

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”



5. Integración y resguardo de las bases de concertación y convenios específicos de Residencia Profesional.	Físico y Electrónico	
6. Emisión de la Constancia de Terminación de Servicio Social y actas de acreditación de Residencia para ser enviadas al Departamento de Servicios Escolares para su validación final.	Físico y Electrónico	
7. Los datos personales son de los alumnos para inscripción IMSS (constancia de vigencia de derecho).	Físico	
8. Los datos personales para tramites del SEGUROS THONA	Físicos y Digitales	
9. Los datos personales de los asesores del programa Chiapas Puede	Físicos y Digitales	

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIPI) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

o Los datos personales de los educandos del programa Chiapas Puede	digitales	

VII. LOS CONTROLES Y MECANISMOS DE SEGURIDAD PARA LAS TRANSFERENCIAS QUE, EN SU CASO, SE EFECTÚEN.

Para implementar las medidas de seguridad aplicables a la transferencia de datos personales de los estudiantes con las empresas, dependencias y organismos receptores en el ejercicio de sus atribuciones, el receptor externo de los datos personales asumirá el carácter de responsable conforme a la legislación en la materia y deberá tratar los datos personales atendiendo a dicha legislación y a lo convenido en el aviso de privacidad que le será comunicado por el Departamento de Vinculación y Departamento de Residencia Profesional y Servicio Social, quien deberá considerar la modalidad por la cual se envían los datos personales a los destinatarios, pudiendo hacerse mediante el traslado de soportes físicos, electrónicos o a través del correo electrónico institucional. Cada una de estas modalidades deberá sujetarse a lo siguiente:

VIII. EL RESGUARDO DE LOS SOPORTES FÍSICOS DE LOS DATOS PERSONALES.

Los expedientes físicos que contienen la documentación de Servicio Social, convenios y Residencias Profesionales de los alumnos se encuentran resguardados y en custodia del personal autorizado en el área asignada para tal efecto dentro de las oficinas del Departamento de Vinculación y Departamento de Residencia Profesional y Servicio Social, concretamente en el edificio de la Subdirección de Vinculación del Instituto Tecnológico Superior de Cintalapa.

IX. LAS BITÁCORAS DE ACCESO Y VULNERACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES.

Los datos que se registran en la Bitácora de acceso (Anexo 1) para revisar expedientes estudiantiles de vinculación son los siguientes:

- Quien accede a los datos personales del alumno, cargo y adscripción;
- Fecha y hora en la que se realiza el acceso o se intenta el mismo, así como fecha y hora de salida;

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

“Se están las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

XI. EL ANÁLISIS DE BRECHA.

[illegible]

XII. LA GESTIÓN DE VULNERACIONES.

En caso de ocurrir alguna vulneración de seguridad que afecte la confidencialidad, integridad o disponibilidad de los expedientes físicos, bases de datos, archivos o plataformas utilizadas por la Subdirección de Vinculación y sus áreas adscritas, será obligatorio registrar el evento sin

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTIAIP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTIPCCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

dilación en la bitácora de vulneraciones. Asimismo, deberá informarse a las instancias institucionales y a la autoridad competente conforme a las disposiciones aplicables.

Tan pronto como se confirme la vulneración y se inicien las acciones para dimensionar su alcance, la Subdirectora de Vinculación, en coordinación con las jefaturas de las áreas adscritas que correspondan al tratamiento afectado, dará seguimiento a la notificación de la persona titular conforme al procedimiento institucional aplicable. La comunicación deberá contener, como mínimo, los siguientes elementos:

- **La naturaleza del incidente:** Descripción detallada del tipo de vulneración ocurrida en los archivos del departamento (físico, electrónico o de red).
- **Los datos personales comprometidos:** Listado específico de la información expuesta.
- **Recomendaciones de protección:** Acciones y medidas preventivas sugeridas que la persona afectada puede adoptar de forma inmediata para salvaguardar sus intereses personales.
- **Acciones correctivas inmediatas:** Detalle de las contingencias técnicas o administrativas aplicadas por el departamento para contener la vulneración y mitigar el riesgo.
- **Medios de contacto institucionales:** Canales informativos oficiales del Instituto donde el titular puede solicitar orientación y seguimiento sobre el estatus de su información.

Una vez contenida la eventualidad, la Subdirectora de Vinculación, las jefaturas de las áreas adscritas involucradas y, cuando corresponda, el área de tecnologías de la información del Instituto analizarán las causas del incidente. Las conclusiones se integrarán como acciones preventivas y correctivas para fortalecer los controles físicos y digitales de la Subdirección.

La Subdirección establecerá mecanismos de supervisión para asegurar que las personas servidoras públicas, personal docente, personal de apoyo y prestadores de servicio que intervengan en cualquiera de sus tratamientos guarden confidencialidad sobre los datos personales. Esta obligación subsistirá incluso después de concluida la relación laboral, académica o de prestación de servicios.

XIII. LAS MEDIDAS DE SEGURIDAD FÍSICAS APLICADAS A LAS INSTALACIONES.

•

•

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAI) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”



-

-

XIV. LOS CONTROLES DE IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS.

[Redacted content]

XV. LOS PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS PERSONALES.

[Redacted content]

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTIP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIIP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

XVI. EL PLAN DE CONTINGENCIA.

XVII. LAS TÉCNICAS UTILIZADAS PARA LA SUPRESIÓN Y BORRADO SEGURO DE LOS DATOS PERSONALES.

A fin de dar cumplimiento al principio de temporalidad y asegurar que la información confidencial de alumnos o entidades particulares no permanezca expuesta tras haber cumplido su finalidad legal y académica, el departamento implementará los siguientes mecanismos de eliminación definitiva:

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

- **Destrucción segura de documentos físicos:** Los formatos, copias de identificaciones oficiales, historiales académicos o borradores erróneos que contengan datos personales de los estudiantes no serán desechados bajo ninguna circunstancia en contenedores de basura común. Una vez transcurridos los plazos de retención académica obligatorios, los documentos impresos deberán ser destruidos en su totalidad mediante el uso de una máquina trituradora de papel de corte cruzado o por medio de incineración controlada en las instalaciones del Instituto.
- **Borrado seguro de archivos digitales y medios electrónicos:**
Para la depuración de los equipos de cómputo del departamento, servidores locales o unidades portátiles (USB o discos externos), se emplearán herramientas de software autorizadas por el área de sistemas de la universidad que realicen un borrado lógico e irreversible. Este procedimiento asegura que los datos personales contenidos en hojas de cálculo de control interno o versiones preliminares de reportes de residencia no puedan ser recuperados mediante programas de reconstrucción informática.
- **Fijación de periodos de retención institucional:** La Subdirección de Vinculación y las jefaturas de las áreas adscritas revisarán los expedientes y archivos bajo su responsabilidad para identificar aquellos que hayan cumplido los periodos de conservación aplicables y, cuando proceda, gestionar su disposición conforme a los instrumentos archivísticos correspondientes.
- **Prohibición de reutilización de soportes documentales:** Queda estrictamente prohibido utilizar como papel de reúso para notas internas, borradores de correspondencia o actividades administrativas diarias de la oficina, cualquier tipo de documento impreso que contenga nombres, números de control, datos médicos, calificaciones o firmas autógrafas de los estudiantes o de los asesores externos de los sectores productivos.

XVIII. EL PLAN DE TRABAJO.



“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIIP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”



XIX. LOS MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD.

El resguardo de los datos personales tratados por la Subdirección de Vinculación exige una supervisión continua; por tanto, la Subdirección y las jefaturas de sus áreas adscritas implementarán mecanismos de revisión para evaluar riesgos, amenazas, vulnerabilidades, incidentes y la efectividad de los controles establecidos.

Dichos mecanismos se ejecutarán mediante las siguientes directrices:

- Auditoría física semestral: La Subdirectora de Vinculación y las jefaturas de las áreas adscritas revisarán las gavetas, archiveros y espacios de resguardo, verificando cerraduras, condiciones físicas y el correcto llenado de las bitácoras de acceso correspondientes.
- Monitoreo digital y de accesos: Se revisarán periódicamente los privilegios y contraseñas de los archivos electrónicos, bases de datos y plataformas utilizadas por las áreas adscritas, incluidos los registros de convenios, Servicio Social, Residencias Profesionales, THONA SEGUROS y SIGA Chiapas Puede.
- Evaluación de incidentes e integración de nuevas amenazas: Ante la detección de fallas en los sistemas informáticos o en el manejo físico de documentos, la Subdirección y el área adscrita involucrada evaluarán las causas del incidente y actualizarán las medidas de seguridad cuando las condiciones tecnológicas u operativas lo requieran.

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIIP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPECHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

XX. EL PROGRAMA GENERAL DE CAPACITACIÓN.

Con el propósito de fortalecer la protección de los datos personales tratados por la Subdirección de Vinculación y sus áreas adscritas, se establece el siguiente programa general de capacitación:

Sensibilización institucional: Desarrollar acciones informativas dirigidas a estudiantes y al personal de la Subdirección y sus áreas adscritas sobre la importancia de proteger la privacidad y mantener restringido el acceso a la información utilizada en los trámites de vinculación.

Capacitación sobre Derechos ARCOP: Instruir a las personas servidoras públicas y enlaces de la Subdirección y sus áreas adscritas sobre los mecanismos y procedimientos institucionales para orientar a las personas titulares respecto del ejercicio de sus derechos sobre los datos tratados en Servicio Social, Residencias Profesionales y demás procesos de vinculación.

Concientización sobre el uso del Aviso de Privacidad: Capacitar de manera obligatoria al personal encargado de recabar los datos de los estudiantes sobre el deber ineludible de poner a la vista e informar de manera presencial o digital el Aviso de Privacidad correspondiente antes de capturar cualquier dato personal.

Formación específica sobre directrices de seguridad: Instruir periódicamente a la Subdirectora de Vinculación, a las jefaturas de las áreas adscritas y al personal autorizado sobre el resguardo de convenios y expedientes, las transferencias a unidades receptoras, el manejo de información de Servicio Social y Residencias Profesionales, el uso seguro de THONA SEGUROS y SIGA Chiapas Puede y la aplicación de las medidas administrativas, físicas y técnicas previstas en este Documento de Seguridad.

Asesoramiento práctico para la mejora continua: Brindar acompañamiento al personal de la Subdirección y sus áreas adscritas para el correcto uso de bitácoras, la aplicación de los procedimientos de respaldo y borrado seguro y la observancia del presente Documento de Seguridad.

ANEXO 1: BITÁCORA DE ACCESO A LOS DATOS PERSONALES DEL DEPARTAMENTO DE RESIDENCIA PROFESIONALES Y SERVICIO SOCIAL.

Órgano Administrativo:
Responsable del Archivo:

No. Seg.	Nombres y Apellidos	Cargo y Adscripción	Fecha y Hora de Entrada	Fecha y Hora de Salida	Motivo del Acceso	Número de Control	Tipo de Soporte	Firma De Vo. Bo.
1								

ANEXO 2: BITÁCORA DE VULNERACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES DEL DEPARTAMENTO DE RESIDENCIA PROFESIONALES Y SERVICIO SOCIAL.

Órgano Administrativo:

Responsable del Archivo:

No. Seg.	Fecha y Hora Vulneración	Causa e Identificación de Vulneración	Acciones Correctivas Aplicadas	Acciones Definitivas de Blindaje	Fecha de Notificación al Titular	Fecha Notificación a la Autoridad	Datos/ Expedientes Afectados

SUBDIRECCIÓN ACADÉMICA

II. NOMBRES DE LOS SISTEMAS DE TRATAMIENTO.

Los datos personales en posesión de la Subdirección Académica del Instituto Tecnológico Superior de Cintalapa son sometidos a los siguientes tratamientos:

1. Atención, integración, seguimiento y resolución de los procesos académicos atendidos por el Comité Académico del Instituto.
2. Consulta, gestión y resguardo del historial académico de los seis programas educativos vigentes de la institución mediante el sistema MindBox.
3. Integración y validación de datos de aspirantes para los procesos de examen de nuevo ingreso y gestión administrativa correspondiente.

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

4. Descarga, creación e integración de bases de datos de aspirantes para la transferencia de información al Tecnológico Nacional de México, conforme a los procesos institucionales señalados en este documento.
5. Integración de la estadística institucional y elaboración de reportes oficiales relacionados con matrícula, ingreso, egreso, titulación, deserción, reprobación y eficiencia terminal.
6. Seguimiento de la trayectoria académica de los estudiantes, incluyendo aprobación, reprobación, rezago, deserción y, en su caso, reincorporación conforme a los lineamientos vigentes del Tecnológico Nacional de México.
7. Operación y seguimiento de los programas de tutoría, asesoría académica, círculos de lectura y atención a estudiantes en riesgo de abandono escolar, incluyendo la expedición de constancias de créditos cuando corresponda.
8. Gestión y seguimiento de procesos de acreditación de programas educativos, opciones de titulación, servicio social y residencia profesional, en coordinación con las áreas institucionales correspondientes.
9. Integración, consulta, manejo y resguardo de expedientes y documentos académicos, incluyendo minutas del Comité Académico, constancias, kardex y credencial de la escuela.
10. Transferencia de información académica y estadística a las áreas internas y externas autorizadas señaladas en el presente documento, para el cumplimiento de funciones institucionales, administrativas, de planeación, evaluación, acreditación y rendición de cuentas.

III. EL NOMBRE, CARGO Y ADSCRIPCIÓN DEL ADMINISTRADOR DEL SISTEMA DE TRATAMIENTO.

Los responsables del tratamiento de los datos personales de la Subdirección Académica son los que se describen a continuación:

Responsable	Cargo	Órgano Administrativo	Tratamiento
	Subdirectora Académica Responsable del tratamiento de los datos personales relacionados con los procesos atendidos por el Comité Académico del Instituto,	Subdirección Académica	

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIPI) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

	Responsable de la Supervisión, seguimiento y resguardo de la información de la Dirección Académica		
--	--	--	--

IV. LAS FUNCIONES Y OBLIGACIONES DEL RESPONSABLE Y TODAS LAS PERSONAS SERVIDORAS PÚBLICAS QUE TRATEN DATOS PERSONALES.

Las funciones y obligaciones del responsable y de todas las personas servidoras públicas que traten datos personales en la Subdirección Académica son las siguientes:

Funciones:

- Dar a los datos personales un tratamiento responsable, conforme a las medidas de seguridad establecidas para tal efecto;
- Salvaguardar los datos personales a los que se tenga acceso con motivo del ejercicio de sus funciones;
- Comprobar que el inventario de datos personales y de los sistemas de tratamiento a los que tengan acceso estén ordenados, y su resguardo corresponda a su periodo de atención y gestión;
- Conservar actualizado el listado de personas usuarias que den tratamiento a datos personales;
- Ante un incidente de vulneración de seguridad de los datos personales o de sus sistemas de tratamiento, notificar de inmediato a la persona titular y documentar los hechos, mediante el Anexo 2.

Obligaciones:

- Guardar confidencialidad respecto de los datos personales a los que se tenga acceso, incluso después de concluida la relación laboral;
- Limitar el tratamiento de los datos personales a las finalidades previstas en el aviso de privacidad correspondiente;
- Abstenerse de transferir, difundir o divulgar datos personales sin el consentimiento de la persona titular o sin fundamento legal que lo autorice o bien sea una función a fin a sus actividades laborales;
- Utilizar únicamente los equipos, sistemas y medios institucionales autorizados para el tratamiento de los datos personales;
- Custodiar los expedientes físicos y electrónicos en espacios con acceso restringido, controlado y autorizado.

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx



V. LOS DATOS PERSONALES TRATADOS EN LOS SISTEMAS DE TRATAMIENTOS Y/O BASE DE DATOS PERSONALES SON LOS SIGUIENTES:

Datos:

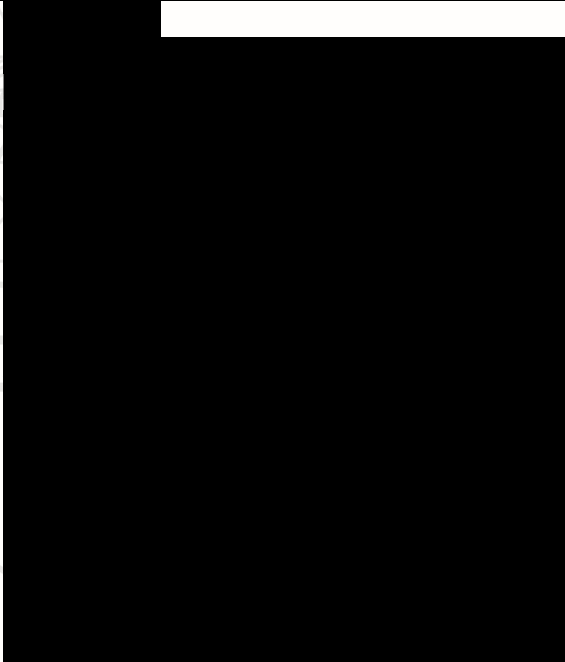
- ❖ CURP
- ❖ Número de Control
- ❖ Nombres y Apellidos
- ❖ Firma
- ❖ Nivel Educativo
- ❖ Dirección
- ❖ Código postal
- ❖ Localidad
- ❖ Municipio y entidad federativa.
- ❖ Estado Civil
- ❖ Nacionalidad
- ❖ Edad
- ❖ Género
- ❖ Lugar y Fecha de Nacimiento
- ❖ Tipo de Sangre
- ❖ Discapacidad
- ❖ Escuela de procedencia
- ❖ Fecha de egreso de la preparatoria
- ❖ Promedio de egreso
- ❖ Licenciatura que estudiara
- ❖ Número de Seguridad Social
- ❖ Número de Teléfono Fijo o Celular
- ❖ Correo electrónico
- ❖ Tutor
- ❖ Teléfono de Tutor
- ❖ Calificaciones
- ❖ Historial académico
- ❖ Status escolar

Documentos:

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAI) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

VI. La descripción del sistema de tratamiento, señalando el tipo de soporte y las características del lugar donde se resguardan.

Descripción del Sistema de Tratamiento	Tipo de Soporte	Características del lugar de resguardo
1. Integración de datos electrónicos mediante base de datos relacionados con los procesos atendidos por el Comité Académico del Instituto, así como para consulta y gestión administrativa estudiantil; MindBox. Sistema que resguarda y gestiona el historial académico de los 6 programas educativos vigentes de la institución. - Validación de datos digitales serán utilizados para la atención del comité académico y resoluciones de procedimientos académicos - Descarga y creación de bases de datos para examen de nuevo ingreso que contienen datos generales de	Electrónico / Físico MindBox/ Archivero	

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

aspirantes vigentes para realizar Transferencia de datos al Tecnológico Nacional de México, en calidad de líder federal de la red de Tecnológicos. - Integración de la estadística institucional y reportes oficiales para Dirección General. - Integración de la estadística institucional y reportes oficiales para Dirección General. - Expedición de constancias de créditos para círculos de lecturas y tutorías; mismos que son entregados a los estudiantes titulares del		
---	--	--

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

trámite y de la información que integra dichos documentos escolares.		
--	--	--

VII. LOS CONTROLES Y MECANISMOS DE SEGURIDAD PARA LAS TRANSFERENCIAS QUE, EN SU CASO, SE EFECTÚEN.

A continuación, se detalla las áreas tanto internas como externas que reciben información de la Subdirección Académica:

Áreas Internas:

- Dirección de Planeación y Vinculación

Uso de información:

- Integrar la estadística institucional (matrícula, ingreso, egreso, titulación, deserción, reprobación y eficiencia terminal) para dar seguimiento a los KPI'S, reportes oficiales, y reportes presentados ante los miembros de la Junta Directiva Institucional, Comité Académico y Gestión Administrativa estudiantil.
- Elaborar y dar seguimiento a los programas institucionales, indicadores y metas, así como a los procesos de evaluación y acreditación;
- Atender solicitudes de información del TecNM, SEP y las autoridades, así como auditorías y requerimientos de transparencia.
- Coordinar los procesos inscripción y de acreditación de programas educativos y las opciones de titulación en vinculación con el Departamento de Control Escolar.
- Coordinar los procesos de acreditación de Servicio Social y Residencia profesional de los programas educativos, en vinculación con la Subdirección de Vinculación.

- Dirección Académica

Uso de información:

- Dar seguimiento a la trayectoria académica de los alumnos (aprobación, reprobación, rezago y deserción y posible reincorporación con programa RegresaTec apegados a los lineamientos vigentes de TecNM Federal);
- Manejo de expedientes y acuerdos del Comité Académico

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

- Operar los programas de tutoría, asesoría académica y atención a alumnos en riesgo de abandono escolar;
- Analizar y dictaminar casos de alumnos con estatus de equivalencia, revalidación, baja, reingreso o situaciones académicas especiales;
- Coordinar los procesos de acreditación de programas educativos y las opciones de titulación en vinculación con el Departamento de Desarrollo Académico.



➤ Dirección General

Uso de información:

- Tomar decisiones institucionales;
- Elaborar los informes de rendición de cuentas ante las autoridades y órganos de gobierno;
- Atender los requerimientos del TecNM, la SEP Federal, estatal y otras instancias fiscalizadoras o de control;
- Firmar y validar documentos oficiales, como constancias, convocatorias;
- Resolver casos especiales que requieran su intervención.

Áreas externas:

➤ Tecnológico Nacional de México

Uso de información:

- Integrar la estadística institucional y los reportes oficiales de matrícula, ingreso, egreso, deserción, reprobación y titulación.
- Alimentar y validar los sistemas de información del TecNM Federal.
- Supervisar los procesos de examen de nuevo ingreso y evaluación docente de acuerdo a la normatividad académica y administrativa. Vigente.
- Atender auditorías, evaluaciones, acreditaciones y requerimientos de rendición de cuentas federales.
- Dar seguimiento a los programas y apoyos federales que operan a través del TecNM.

➤ Secretaría de Educación Pública del Estado

Uso de información:

- Integrar la estadística educativa estatal con los datos otorgados por parte de la Institución Educativa;
- Registrar y validar la información de estudiantes, egresados y titulados para efectos oficiales.
- Atender revisiones, auditorías y requerimientos de control del programa a nivel federal.

Mecanismos de seguridad:

Para implementar las medidas de seguridad aplicables a la transferencia de datos personales el receptor de los datos personales asumirá el carácter de responsable conforme a la legislación en

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

la materia al recibir dicha información mediante el traslado de soportes físicos, electrónicos o a través del correo electrónico institucional, por lo que deberá tratar los datos personales atendiendo y apegándose al aviso de privacidad de la Subdirección Académica, mismo que se encuentra publicado en:

<https://cintalapa.tecnm.mx/aviso-privacidad>

En cada una de estas modalidades se deberá sujetarse a lo siguiente:

A. Traslado de soportes físicos: Los datos personales se trasladan en documentos impresos que pueden leerse directamente, sin necesidad de un dispositivo que procese su contenido para consultarlo, modificarlo o almacenarlo.

Por ejemplo: cuando e la Subdirección Académica remite por correo electrónico institucional oficial oficios, formatos, constancias o copias de documentos del expediente del alumno o del egresado a la Dirección Académica.

B. Traslado físico de soportes electrónicos: Los datos personales se entregan al destinatario mediante archivos electrónicos almacenados en medios que requieren un dispositivo con circuitos electrónicos para consultar, modificar o almacenar su contenido.

Por ejemplo: cuando e la Subdirección Académica entrega mediante una memoria USB con los archivos digitalizados de expedientes.

C. Traslado sobre redes electrónicas: Los datos personales se transmiten en archivos electrónicos a través de una red electrónica.

Por ejemplo: cuando e la Subdirección Académica realiza carga de las bases de datos con información requerida en las plataformas oficiales del Tecnológico Nacional de México.

VIII. El resguardo de los soportes físicos de los datos personales.

Los expedientes físicos se encuentran resguardados y en custodia de los responsables del sistema de tratamiento de los datos personales en el área asignada para tal efecto.

IX. Las bitácoras de acceso y vulneraciones a la seguridad de los datos personales.

Los datos que se registran en la Bitácora de acceso (anexo 1) son los siguientes:

- Número consecutivo;
- Quien accede a los datos personales (Nombre completo);
- Cargo;
- Área de adscripción;
- Propósito del acceso;
- Número de control del alumno y/o egresado;
- Tipo de soporte utilizado (Expediente o registro electrónico);
- Fecha en formato mes y año (Al que corresponde la bitácora).

Los datos que se registran en la Bitácora de vulneraciones (anexo 2) son los siguientes:

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx



- Número consecutivo;
- Fecha y hora de la vulneración;
- Documento o información vulnerada;
- Motivo de la vulneración;
- Acciones correctivas y definitivas implementadas;
- Persona que resolvió la vulneración;
- Fecha y hora de notificación de la vulneración a los titulares de los datos personales comprometidos;
- Fecha en formato mes y año (Al que corresponde la bitácora).

X. El análisis de riesgos.

[Redacted]			
[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”



XI. El análisis de brecha.

18. [Redacted]
- [Redacted]
 - [Redacted]
 - [Redacted]
 - [Redacted]
 - [Redacted]
19. [Redacted]
- [Redacted]
 - [Redacted]
20. [Redacted]
- [Redacted]
 - [Redacted]
 - [Redacted]
21. [Redacted]

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

- [REDACTED]
- [REDACTED]
- [REDACTED]
- 22. [REDACTED]
- [REDACTED]
- [REDACTED]

XII. La gestión de vulneraciones.

En caso de ocurrir alguna vulneración deberá registrarse en la bitácora de contingencias (Anexo 2), y se llevará a cabo conforme al siguiente procedimiento:

8. **Detección y aviso interno:** El personal del departamento que detecte o sospeche de una vulneración lo comunicará de inmediato a la Subdirección Académica, preservando el estado de los documentos, equipos o sistemas involucrados.
9. **Contención:** Se ejecutarán acciones inmediatas para evitar mayor afectación, tales como resguardar el archivo, suspender accesos, cambiar contraseñas o desconectar el equipo comprometido.
10. **Registro inicial:** Se asentará en la bitácora la fecha y hora de la vulneración, el documento o información vulnerada y el motivo de la vulneración.
11. **Evaluación:** La Subdirección determinará el alcance del incidente, las personas titulares afectadas y si se comprometen sus derechos patrimoniales o morales.
12. **Acciones correctivas y definitivas:** Se implementarán las medidas para reestablecer la información y eliminar la causa, y se registrarán en la bitácora junto con el nombre de la persona que resolvió la vulneración.
13. **Notificación:** Se informará a las personas titulares, dentro del plazo no mayor a 3 días (72 horas), la notificación incluirá la naturaleza del incidente, los datos personales comprometidos, las recomendaciones para la persona titular, las acciones correctivas realizadas y los medios para obtener mayor información. Se registrará en la bitácora la fecha y hora de cada notificación.
14. **Cierre y prevención.** La Subdirección revisará las medidas de seguridad vigentes y ajustará las que resulten necesarias para evitar que el incidente se repita.

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”



XIII. Las medidas de seguridad físicas aplicadas a las instalaciones.

6. [Redacted]
7. [Redacted]
8. [Redacted]
9. [Redacted]

XIV. LOS CONTROLES DE IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS.

10. [Redacted]

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAI) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPECHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

11.

[Redacted text]

XV. LOS PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS PERSONALES.

12.

[Redacted text]

13.

[Redacted text]

XVI. EL PLAN DE CONTINGENCIA.

14.

[Redacted text]

15.

[Redacted text]

XVII. LAS TÉCNICAS UTILIZADAS PARA LA SUPRESIÓN Y BORRADO SEGURO DE LOS DATOS PERSONALES.

16. Los expedientes, minutas, constancias, kardex, credenciales y demás documentos que contengan datos personales sólo podrán suprimirse una vez cumplidos los periodos de conservación académica y archivística aplicables. Los documentos físicos cuya eliminación proceda deberán destruirse de manera que no puedan reconstruirse y los archivos electrónicos deberán borrarse de forma segura.
17. No deberán utilizarse como papel de reúso documentos que contengan datos personales o académicos.

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LTGAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

XVIII. EL PLAN DE TRABAJO.

18. [REDACTED]
19. [REDACTED]

XIX. LOS MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD.

20. La Subdirección Académica realizará el monitoreo de los controles de acceso físico y electrónico, las bitácoras, los permisos de MindBox, las transferencias de información y el estado de los respaldos institucionales.
21. Los incidentes, cambios de sistema o nuevos riesgos deberán analizarse para determinar la actualización de las medidas de seguridad y de este Documento de Seguridad.

XX. EL PROGRAMA GENERAL DE CAPACITACIÓN.

22. El personal que intervenga en los tratamientos de la Subdirección Académica deberá recibir capacitación sobre confidencialidad, avisos de privacidad, derechos ARCOP, uso autorizado de MindBox, manejo de expedientes del Comité Académico, transferencias de información, bitácoras y respuesta a vulneraciones.
23. La capacitación deberá reforzarse ante cambios en sistemas, procedimientos, personal o riesgos de seguridad.

ANEXO 1: Bitácora de acceso a los Datos Personales

Órgano Administrativo (o área generadora/resguardante):

Instituto Tecnológico Superior de Cintalapa
Subdirección Académica

Responsable del Archivo:

Adriana Gabriela Hernández Farrera
Subdirectora Académica

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAI) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

Núm ero Progresivo	Nombre complet o (de quien accede a los datos personal es	Car go	Ár ea de adscripción	Propó sito del acceso	Núm ero de control del alumno y/o egresado	Ti po de soporte utilizado (Expediente o registro electrónico)	Fec ha en formato (al que corresponde la bitácora) día, mes y año

ANEXO 2: Bitácora de vulneraciones a la seguridad de los Datos Personales

Órgano Administrativo (o área generadora/resguardante):

Instituto Tecnológico Superior de Cintalapa

Subdirección Académica

Responsable del Archivo:

Adriana Gabriela Hernández Farrera

Subdirectora Académica

Número progresiv o	Fecha y Hora de Vulnera ción	Documento o información vulnerada	Motivo de la vulneració n	Acciones correctivas y definitivas implementadas	Persona que resolvió la vulneració n	Fecha y hora de notificación de la vulneración a los titulares de los datos personales comprometid os	Fecha en formato (al que correspon de la bitácora) día, mes y año

DEPARTAMENTO DE DESARROLLO ACADEMICO

II. NOMBRES DE LOS SISTEMAS DE TRATAMIENTO.

Los datos personales en posesión del Departamento de Desarrollo Académico del Instituto Tecnológico Superior de Cintalapa son sometidos a los siguientes tratamientos:

- Integración, consulta y manejo de datos electrónicos de aspirantes y estudiantes mediante el sistema MindBox, para los procesos de nuevo ingreso y la gestión académica institucional.

2. Descarga y creación de reportes y bases de datos que contienen datos generales de aspirantes para el examen de nuevo ingreso y de estudiantes vigentes para la gestión, adquisición y seguimiento de programas de formación integral.
3. Gestión y seguimiento de asesorías académicas de estudiantes vigentes, mediante formatos físicos y la generación de reportes correspondientes.
4. Integración y resguardo de fichas de canalización de estudiantes vigentes para la atención psicológica, las cuales contienen información de identidad y datos personales.
5. Integración, registro y resguardo de los formatos físicos y electrónicos de consulta y préstamo de libros de estudiantes vigentes en el Área de Biblioteca.
6. Integración y actualización de expedientes físicos para el control y seguimiento de los datos personales y sensibles tratados en los procesos de formación integral de los estudiantes, incluyendo tutorías, fichas de canalización, asesorías académicas y consulta y préstamo de libros.
7. Integración de la estadística institucional y elaboración de reportes oficiales derivados de la información académica y de los procesos atendidos por el Departamento de Desarrollo Académico.
8. Transferencia de datos de aspirantes al Tecnológico Nacional de México para los procesos de examen de nuevo ingreso y demás finalidades institucionales señaladas en el presente documento.

III. El nombre, cargo y adscripción del administrador del sistema de tratamiento.

Los responsables del tratamiento de los datos personales del Departamento de Desarrollo Académico, son los que describen a continuación:

Responsable	Cargo	Órgano Administrativo	Tratamiento
[REDACTED]	Jefa del Departamento de Desarrollo Académico. Responsable de la Supervisión y seguimiento de la formación integral de los estudiantes, de manera física y electrónica.	Departamento de Desarrollo Académico.	[REDACTED]

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIPI) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

	Psicóloga Responsable de la atención psicológica de los alumnos, de archivo físico del estudiantado vigente y no vigente.	Departamento de Desarrollo Académico – Área de Psicología.	
	Responsable de Biblioteca Responsable de la Biblioteca. archivo físico y electrónico de las bitácoras de préstamos de libros de los estudiantes.	Departamento de Desarrollo Académico – Área de Biblioteca	

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPECHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

IV. Las funciones y obligaciones del responsable y todas las personas servidoras públicas que traten datos personales.

Las funciones y obligaciones del responsable y de todas las personas servidoras públicas que traten datos personales en el Departamento de Desarrollo Académico son las siguientes:

Funciones:

- Dar a los datos personales un tratamiento responsable, conforme a las medidas de seguridad establecidas para tal efecto;
- Salvaguardar los datos personales a los que se tenga acceso con motivo del ejercicio de sus funciones;
- Comprobar que el inventario de datos personales y de los sistemas de tratamiento a los que tengan acceso estén ordenados, y su resguardo corresponda a su periodo de atención y gestión;
- Conservar actualizado el listado de personas usuarias que den tratamiento a datos personales;
- Ante un incidente de vulneración de seguridad de los datos personales o de sus sistemas de tratamiento, notificar de inmediato a la persona titular y documentar los hechos, mediante el Anexo 2.

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

Obligaciones:

- Guardar confidencialidad respecto de los datos personales a los que se tenga acceso, incluso después de concluida la relación laboral;
- Limitar el tratamiento de los datos personales a las finalidades previstas en el aviso de privacidad correspondiente;
- Abstenerse de transferir, difundir o divulgar datos personales sin el consentimiento de la persona titular o sin fundamento legal que lo autorice o bien sea una función a fin a sus actividades laborales;
- Utilizar únicamente los equipos, sistemas y medios institucionales autorizados para el tratamiento de los datos personales;
- Custodiar los expedientes físicos y electrónicos en espacios con acceso restringido, controlado y autorizado.

V. Los datos personales tratados en los sistemas de tratamientos y/o base de datos personales son los siguientes:

Datos:

- ❖ CURP
- ❖ Número de Control
- ❖ Nombres y Apellidos
- ❖ Firma
- ❖ Nivel Educativo
- ❖ Dirección
- ❖ Código postal
- ❖ Localidad
- ❖ Municipio y entidad federativa.
- ❖ Estado Civil
- ❖ Nacionalidad
- ❖ Edad
- ❖ Género
- ❖ Lugar y Fecha de Nacimiento
- ❖ Tipo de Sangre
- ❖ Discapacidad
- ❖ Escuela de procedencia
- ❖ Fecha de egreso de la preparatoria
- ❖ Promedio de egreso
- ❖ Licenciatura que estudiara
- ❖ Número de Seguridad Social
- ❖ Número de Teléfono Fijo o Celular
- ❖ Correo electrónico

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

- ❖ Tutor
- ❖ Teléfono de Tutor

Documentos:

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

VI. La descripción del sistema de tratamiento, señalando el tipo de soporte y las características del lugar donde se resguardan.

Descripción del Sistema de Tratamiento	Tipo de Soporte	Características del lugar de resguardo
1. Integración de datos electrónicos mediante base de datos de alumnos de nuevo ingreso; MindBox. Sistema que resguarda y gestiona el historial académico de los 6 programas educativos vigentes de la institución. • Descarga y creación de reportes que contienen datos generales de aspirantes para el examen de nuevo ingreso y estudiantes vigentes para la gestión, adquisición y seguimiento de programas de formación integral como asesorías académicas, fichas	Electronico. MindBox.	[REDACTED]

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIIP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

de canalización y préstamos de libros. • Descarga y creación de bases de datos para examen de nuevo ingreso que contienen datos generales de aspirantes vigentes para realizar Transferencia de datos al Tecnológico Nacional de México, en calidad de líder federal de la red de Tecnológicos. • Integración de la estadística institucional y reportes oficiales para Dirección General. • Expedición de constancias de créditos para círculos de lecturas y tutorías; mismos que son entregados a los estudiantes titulares del trámite y de la información que integra dichos		
--	--	--

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

documentos escolares.		
2. Se integran y actualizan los expedientes de cada persona de acuerdo al periodo vigente, para el control y seguimiento de los datos personales y sensibles tratados para la educación integral de los estudiantes: Tutorías, fichas de canalización, asesorías académicas y consulta y préstamo de libros.	Físico.	

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

VII. Los controles y mecanismos de seguridad para las transferencias que, en su caso, se efectúen.

A continuación, se detalla las áreas tanto internas como externas que reciben información del Departamento de Desarrollo Académico:

Áreas Internas:

- Dirección de Planeación y Vinculación

Uso de información:

- Integrar la estadística institucional (matrícula, ingreso, egreso, titulación, deserción, reprobación y eficiencia terminal) para dar seguimiento a los KPI'S, reportes oficiales, y reportes presentados ante los miembros de la Junta Directiva Institucional y Comité Académico
- Elaborar y dar seguimiento a los programas institucionales, indicadores y metas, así como a los procesos de evaluación y acreditación;

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

- Atender solicitudes de información del TecNM, SEP y las autoridades, así como auditorías y requerimientos de transparencia.
- Coordinar los procesos inscripción y de acreditación de programas educativos y las opciones de titulación en vinculación con el Departamento de Control Escolar.
- Coordinar los procesos de acreditación de Servicio Social y Residencia profesional de los programas educativos, en vinculación con la Subdirección de Vinculación.

➤ **Dirección Académica**

Uso de información:

- Dar seguimiento a la trayectoria académica de los alumnos (aprobación, reprobación, rezago y deserción y posible reincorporación con programa RegresaTec apegados a los lineamientos vigentes de TecNM Federal);
- Operar los programas de tutoría, asesoría académica y atención a alumnos en riesgo de abandono escolar;
- Analizar y dictaminar casos de alumnos con estatus de equivalencia, revalidación, baja, reingreso o situaciones académicas especiales;
- Coordinar los procesos de acreditación de programas educativos y las opciones de titulación en vinculación con el Departamento de Desarrollo Académico.



➤ **Dirección General**

Uso de información:

- Tomar decisiones institucionales;
- Elaborar los informes de rendición de cuentas ante las autoridades y órganos de gobierno;
- Atender los requerimientos del TecNM, la SEP Federal, estatal y otras instancias fiscalizadoras o de control;
- Firmar y validar documentos oficiales, como constancias, convocatorias;
- Resolver casos especiales que requieran su intervención.

Áreas externas:

➤ **Tecnológico Nacional de México**

Uso de información:

- Integrar la estadística institucional y los reportes oficiales de matrícula, ingreso, egreso, deserción, reprobación y titulación.
- Alimentar y validar los sistemas de información del TecNM Federal.
- Supervisar los procesos de examen de nuevo ingreso y evaluación docente de acuerdo a la normatividad académica y administrativa. Vigente.

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

- Atender auditorías, evaluaciones, acreditaciones y requerimientos de rendición de cuentas federales.
- Dar seguimiento a los programas y apoyos federales que operan a través del TecNM.

➤ Secretaría de Educación Pública del Estado

Uso de información:

- Integrar la estadística educativa estatal con los datos otorgados por parte de la Institución Educativa;
- Registrar y validar la información de estudiantes, egresados y titulados para efectos oficiales.
- Atender revisiones, auditorías y requerimientos de control del programa a nivel federal.

Mecanismos de seguridad:

Para implementar las medidas de seguridad aplicables a la transferencia de datos personales el receptor de los datos personales asumirá el carácter de responsable conforme a la legislación en la materia al recibir dicha información mediante el traslado de soportes físicos, electrónicos o a través del correo electrónico institucional, por lo que deberá tratar los datos personales atendiendo y apegándose al aviso de privacidad del Departamento de Desarrollo Académico, mismo que se encuentra publicado en:

<https://cintalapa.tecnm.mx/aviso-privacidad>

En cada una de estas modalidades se deberá sujetarse a lo siguiente:

A. Traslado de soportes físicos: Los datos personales se trasladan en documentos impresos que pueden leerse directamente, sin necesidad de un dispositivo que procese su contenido para consultarlo, modificarlo o almacenarlo.

Por ejemplo: cuando el Departamento de Desarrollo Académico remite por correo electrónico institucional oficial oficios, formatos, constancias o copias de documentos del expediente del alumno o del egresado a la Dirección Académica.

B. Traslado físico de soportes electrónicos: Los datos personales se entregan al destinatario mediante archivos electrónicos almacenados en medios que requieren un dispositivo con circuitos electrónicos para consultar, modificar o almacenar su contenido.

Por ejemplo: cuando el Departamento de Desarrollo Académico entrega mediante una memoria USB con los archivos digitalizados de expedientes.

C. Traslado sobre redes electrónicas: Los datos personales se transmiten en archivos electrónicos a través de una red electrónica.

Por ejemplo: cuando el Departamento de Desarrollo Académico realiza carga de las bases de datos de aspirantes para el examen a alumnos de nuevo ingreso en las plataformas oficiales del Tecnológico Nacional de México.

VIII. El resguardo de los soportes físicos de los datos personales.

Los expedientes físicos se encuentran resguardados y en custodia de los responsables del sistema de tratamiento de los datos personales en el área asignada para tal efecto.

IX. Las bitácoras de acceso y vulneraciones a la seguridad de los datos personales.

Los datos que se registran en la Bitácora de acceso (anexo 1) son los siguientes:

- Número consecutivo;
- Quien accede a los datos personales (Nombre completo);
- Cargo;
- Área de adscripción;
- Propósito del acceso;
- Número de control del alumno y/o egresado;
- Tipo de soporte utilizado (Expediente o registro electrónico);
- Fecha en formato mes y año (Al que corresponde la bitácora).

Los datos que se registran en la Bitácora de vulneraciones (anexo 2) son los siguientes:

- Número consecutivo;
- Fecha y hora de la vulneración;
- Documento o información vulnerada;
- Motivo de la vulneración;
- Acciones correctivas y definitivas implementadas;
- Persona que resolvió la vulneración;
- Fecha y hora de notificación de la vulneración a los titulares de los datos personales comprometidos;
- Fecha en formato mes y año (Al que corresponde la bitácora).

X. El análisis de riesgos.



“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAPCHS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”



[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

XI. El análisis de brecha.

23. [REDACTED]
- [REDACTED]
 - [REDACTED]

- [Redacted]
- [Redacted]
- [Redacted]
- 24. [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- 25. [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- 26. [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- 27. [Redacted]
- [Redacted]
- [Redacted]

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIIP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

XII. La gestión de vulneraciones.

En caso de ocurrir alguna vulneración deberá registrarse en la bitácora de contingencias (Anexo 2), y se llevará a cabo conforme al siguiente procedimiento:

15. Detección y aviso interno: El personal del departamento que detecte o sospeche de una vulneración lo comunicará de inmediato a la Jefatura del Departamento de Desarrollo Académico, preservando el estado de los documentos, equipos o sistemas involucrados.

16. Contención: Se ejecutarán acciones inmediatas para evitar mayor afectación, tales como resguardar el archivo, suspender accesos, cambiar contraseñas o desconectar el equipo comprometido.

- 17. Registro inicial:** Se asentará en la bitácora la fecha y hora de la vulneración, el documento o información vulnerada y el motivo de la vulneración.
- 18. Evaluación:** La Jefatura determinará el alcance del incidente, las personas titulares afectadas y si se comprometen sus derechos patrimoniales o morales.
- 19. Acciones correctivas y definitivas:** Se implementarán las medidas para reestablecer la información y eliminar la causa, y se registrarán en la bitácora junto con el nombre de la persona que resolvió la vulneración.
- 20. Notificación:** Se informará a las personas titulares, dentro del plazo no mayor a 3 días (72 horas), la notificación incluirá la naturaleza del incidente, los datos personales comprometidos, las recomendaciones para la persona titular, las acciones correctivas realizadas y los medios para obtener mayor información. Se registrará en la bitácora la fecha y hora de cada notificación.
- 21. Cierre y prevención.** La Jefatura revisará las medidas de seguridad vigentes y ajustará las que resulten necesarias para evitar que el incidente se repita.

XIII. LAS MEDIDAS DE SEGURIDAD FÍSICAS APLICADAS A LAS INSTALACIONES.

- 24.** [REDACTED]
- 25.** [REDACTED]
- 26.** [REDACTED]

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPECHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”



27.

XIV. LOS CONTROLES DE IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS.

28.

29.

XV. LOS PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS PERSONALES.

30.

31.

XVI. EL PLAN DE CONTINGENCIA.

32.

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

33.

XVII. LAS TÉCNICAS UTILIZADAS PARA LA SUPRESIÓN Y BORRADO SEGURO DE LOS DATOS PERSONALES.

34. Los expedientes y archivos que contengan datos personales de aspirantes y estudiantes sólo podrán eliminarse cuando hayan cumplido su finalidad y los periodos de conservación académica y archivística aplicables. Los documentos físicos cuya eliminación proceda deberán destruirse de forma que no puedan reconstruirse; los archivos electrónicos deberán borrarse de manera segura.
35. No deberán reutilizarse como papel de borrador fichas de canalización, registros de asesoría, documentos de biblioteca ni otros soportes que contengan datos personales.

XVIII. EL PLAN DE TRABAJO.

36.

37.

XIX. LOS MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD.

38. La Jefatura verificará los accesos a MindBox y a los expedientes, el estado de los archiveros, los registros de transferencia, las bitácoras de acceso y vulneraciones y la disponibilidad de los respaldos electrónicos.
39. Los incidentes o nuevas amenazas deberán utilizarse para actualizar las medidas de seguridad y los controles del Departamento.

XX. EL PROGRAMA GENERAL DE CAPACITACIÓN.

40. El personal del Departamento de Desarrollo Académico deberá recibir capacitación sobre confidencialidad, manejo de información académica y sensible, uso seguro de

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

MindBox, resguardo de fichas de canalización y registros de biblioteca, avisos de privacidad, derechos ARCOP, transferencias y atención de vulneraciones.

41. La capacitación deberá reforzarse cuando se incorporen nuevas personas, cambien los procesos o sistemas o se detecten nuevos riesgos.

ANEXO 1: Bitácora de acceso a los Datos Personales

Órgano Administrativo (o área generadora/resguardante):

Instituto Tecnológico Superior de Cintalapa
Departamento de Desarrollo Académico.

Responsable del Archivo:

Clara María Serrano Altuzar
Jefa del Departamento de Desarrollo Académico

Número Progresivo	Nombre completo (de quien accede a los datos personales)	Cargo	Área de adscripción	Propósito del acceso	Número de control del alumno y/o egresado	Tipo de soporte utilizado (Expediente o registro electrónico)	Fecha en formato (al que corresponde la bitácora) día, mes y año

ANEXO 2: Bitácora de vulneraciones a la seguridad de los Datos Personales

Órgano Administrativo (o área generadora/resguardante):

Instituto Tecnológico Superior de Cintalapa
Departamento de Desarrollo Académico.

Responsable del Archivo:

Clara María Serrano Altuzar
Jefa del Departamento de Desarrollo Académico

Número progresivo	Fecha y Hora de Vulneración	Documento o información vulnerada	Motivo de la vulneración	Acciones correctivas y definitivas implementadas	Persona que resolvió la vulneración	Fecha y hora de notificación de la vulneración a los titulares de los datos personales comprometidos	Fecha en formato (al que corresponde la bitácora) día, mes y año

DIRECCIÓN ACADÉMICA

II. El nombre de los sistemas de tratamiento de datos personales.

La Dirección Académica realiza el tratamiento de datos personales mediante los siguientes sistemas y medios de tratamiento: MindBox para el seguimiento, supervisión y validación de datos electrónicos de alumnos de nuevo ingreso y activos, así como para la gestión del historial académico; bases de datos electrónicas utilizadas para la atención del Comité Académico, resoluciones de procedimientos académicos, examen de nuevo ingreso, integración de estadística institucional y reportes oficiales; expedientes físicos y electrónicos para el control y seguimiento de información académica; formatos del Comité Académico, minutas, kardex y fichas de canalización; y plataformas oficiales del Tecnológico Nacional de México utilizadas para la transferencia y seguimiento de información académica, incluyendo RegresaTec.

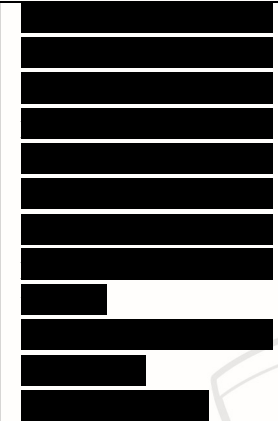
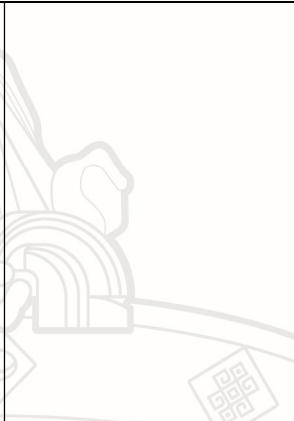
III. El nombre, cargo y adscripción del administrador del sistema de tratamiento.

Los responsables del tratamiento de los datos personales de la Dirección Académica, son los que describen a continuación:

Responsable	Cargo	Órgano Administrativo	Tratamiento
	Directora Académica. Responsable de la Supervisión, Revisión y Validación de	Dirección Académica	

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LEIAPCHS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

	información para la atención del comité académico y resoluciones de procedimientos académicos; los datos personales quedarán bajo resguardo de la Subdirección Académica.		
	Asistente Responsable de la atención en primera instancia con los estudiantes y personal, de archivo físico y digital de la Dirección Académica.	Dirección Académica – Asistente	

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

IV. Las funciones y obligaciones del responsable y todas las personas servidoras públicas que traten datos personales.

Las funciones y obligaciones del responsable y de todas las personas servidoras públicas que traten datos personales en la Dirección Académica son las siguientes:

Funciones:

- Dar a los datos personales un tratamiento responsable, conforme a las medidas de seguridad establecidas para tal efecto;
- Salvaguardar los datos personales a los que se tenga acceso con motivo del ejercicio de sus funciones;
- Comprobar que el inventario de datos personales y de los sistemas de tratamiento a los que tengan acceso estén ordenados, y su resguardo corresponda a su periodo de atención y gestión;
- Conservar actualizado el listado de personas usuarias que den tratamiento a datos personales;
- Ante un incidente de vulneración de seguridad de los datos personales o de sus sistemas de tratamiento, notificar de inmediato a la persona titular y documentar los hechos, mediante el Anexo 2.

Obligaciones:

- Guardar confidencialidad respecto de los datos personales a los que se tenga acceso, incluso después de concluida la relación laboral;
- Limitar el tratamiento de los datos personales a las finalidades previstas en el aviso de privacidad correspondiente;
- Abstenerse de transferir, difundir o divulgar datos personales sin el consentimiento de la persona titular o sin fundamento legal que lo autorice o bien sea una función a fin a sus actividades laborales;
- Utilizar únicamente los equipos, sistemas y medios institucionales autorizados para el tratamiento de los datos personales;
- Custodiar los expedientes físicos y electrónicos en espacios con acceso restringido, controlado y autorizado.

V. Los datos personales tratados en los sistemas de tratamientos y/o base de datos personales son los siguientes:

Datos:

- ❖ CURP
- ❖ Número de Control
- ❖ Nombres y Apellidos
- ❖ Firma
- ❖ Nivel Educativo
- ❖ Dirección
- ❖ Código postal
- ❖ Localidad
- ❖ Municipio y entidad federativa.
- ❖ Estado Civil
- ❖ Nacionalidad
- ❖ Edad
- ❖ Género
- ❖ Lugar y Fecha de Nacimiento
- ❖ Tipo de Sangre
- ❖ Discapacidad
- ❖ Escuela de procedencia
- ❖ Fecha de egreso de la preparatoria
- ❖ Promedio de egreso
- ❖ Licenciatura que estudiara
- ❖ Número de Seguridad Social
- ❖ Número de Teléfono Fijo o Celular
- ❖ Correo electrónico
- ❖ Tutor
- ❖ Teléfono de Tutor

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

Documentos:

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

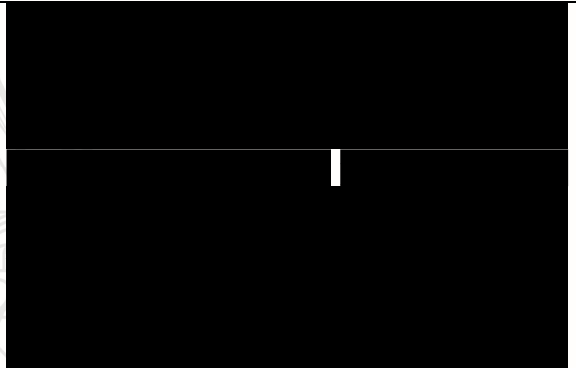
VI. La descripción del sistema de tratamiento, señalando el tipo de soporte y las características del lugar donde se resguardan.

Descripción del Sistema de Tratamiento	Tipo de Soporte	Características del lugar de resguardo
1. Seguimiento, supervisión y validación de datos electrónicos mediante base de datos de alumnos de nuevo ingreso y activos; MindBox. Sistema que resguarda y gestiona el historial académico de los 6 programas educativos vigentes de la institución. - Validación de datos digitales serán utilizados para la atención del comité académico y resoluciones de procedimientos académicos - Descarga y creación de bases de datos para examen de nuevo ingreso que	Electronico. MindBox.	[REDACTED]

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIPI) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

contienen datos generales de aspirantes vigentes para realizar Transferencia de datos al Tecnológico Nacional de México, en calidad de líder federal de la red de Tecnológicos. Integración de la estadística institucional y reportes oficiales para Dirección General.		
---	--	--

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

2. Se integran y actualizan los expedientes de acuerdo al período vigente, para el control y seguimiento de los datos personales y sensibles tratados para la educación integral de los estudiantes: Tutorías, fichas de canalización, asesorías académicas, los cuales serán utilizados para la atención del comité académico y resoluciones de procedimientos académicos;	Físico.	
--	----------------	--

VII. Los controles y mecanismos de seguridad para las transferencias que, en su caso, se efectúen.

A continuación, se detalla las áreas tanto internas como externas que reciben información de la Dirección Académica:

Áreas Internas:

- Dirección de Planeación y Vinculación

Uso de información:

- Integrar la estadística institucional (matrícula, ingreso, egreso, titulación, deserción, reprobación y eficiencia terminal) para dar seguimiento a los KPI'S, reportes oficiales, y reportes presentados ante los miembros de la Junta Directiva Institucional y Comité Académico
- Elaborar y dar seguimiento a los programas institucionales, indicadores y metas, así como a los procesos de evaluación y acreditación;
- Atender solicitudes de información del TecNM, SEP y las autoridades, así como auditorías y requerimientos de transparencia.

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

- Coordinar los procesos inscripción y de acreditación de programas educativos y las opciones de titulación en vinculación con el Departamento de Control Escolar.
- Coordinar los procesos de acreditación de Servicio Social y Residencia profesional de los programas educativos, en vinculación con la Subdirección de Vinculación.

➤ **Subdirección Académica**

Uso de información:

- Dar seguimiento a la trayectoria académica de los alumnos (aprobación, reprobación, rezago y deserción y posible reincorporación con programa RegresaTec apegados a los lineamientos vigentes de TecNM Federal);
- Operar los programas de tutoría, asesoría académica y atención a alumnos en riesgo de abandono escolar;
- Analizar y dictaminar casos de alumnos con estatus de equivalencia, revalidación, baja, reingreso o situaciones académicas especiales;
- Coordinar los procesos de acreditación de programas educativos y las opciones de titulación en vinculación con las Jefaturas de División.



➤ **Dirección General**

Uso de información:

- Tomar decisiones institucionales;
- Elaborar los informes de rendición de cuentas ante las autoridades y órganos de gobierno;
- Atender los requerimientos del TecNM, la SEP Federal, estatal y otras instancias fiscalizadoras o de control;
- Firmar y validar documentos oficiales, como constancias, convocatorias;
- Resolver casos especiales que requieran su intervención.

Áreas externas:

➤ **Tecnológico Nacional de México**

Uso de información:

- Integrar la estadística institucional y los reportes oficiales de matrícula, ingreso, egreso, deserción, reprobación y titulación.
- Alimentar y validar los sistemas de información del TecNM Federal.
- Supervisar los procesos de examen de nuevo ingreso y evaluación docente de acuerdo a la normatividad académica y administrativa. Vigente.
- Atender auditorías, evaluaciones, acreditaciones y requerimientos de rendición de cuentas federales.
- Dar seguimiento a los programas y apoyos federales que operan a través del TecNM.

Carretera Panamericana km. 995, CP. 30400, Cintalapa de Figueroa, Chiapas.
Tel. 9686844779 Ext. 2126
transparencia@cintalapa.tecnm.mx
www.cintalapa.tecnm.mx

➤ Secretaría de Educación Pública del Estado

Uso de información:

- Integrar la estadística educativa estatal con los datos otorgados por parte de la Institución Educativa;
- Registrar y validar la información que requiera en formatos oficiales.
- Atender revisiones, auditorías y requerimientos de control del programa a nivel federal.

Mecanismos de seguridad:

Para implementar las medidas de seguridad aplicables a la transferencia de datos personales el receptor de los datos personales asumirá el carácter de responsable conforme a la legislación en la materia al recibir dicha información mediante el traslado de soportes físicos, electrónicos o a través del correo electrónico institucional, por lo que deberá tratar los datos personales atendiendo y apegándose al aviso de privacidad de la Dirección Académica, mismo que se encuentra publicado en:

<https://cintalapa.tecnm.mx/aviso-privacidad>

En cada una de estas modalidades se deberá sujetarse a lo siguiente:

A. Traslado de soportes físicos: Los datos personales se trasladan en documentos impresos que pueden leerse directamente, sin necesidad de un dispositivo que procese su contenido para consultarlo, modificarlo o almacenarlo.

Por ejemplo: cuando la Dirección Académica remite por correo electrónico institucional oficial oficios, formatos, constancias o copias de documentos del expediente del alumno al comité académico o para resoluciones de algún proceso académico.

B. Traslado físico de soportes electrónicos: Los datos personales se entregan al destinatario mediante archivos electrónicos almacenados en medios que requieren un dispositivo con circuitos electrónicos para consultar, modificar o almacenar su contenido.

Por ejemplo: cuando la Dirección Académica entrega mediante una memoria USB con los archivos digitalizados de expedientes.

C. Traslado sobre redes electrónicas: Los datos personales se transmiten en archivos electrónicos a través de una red electrónica.

Por ejemplo: cuando la Dirección Académica realiza carga de las bases de datos de alumnos de reingreso, para utilizarlos para la atención del comité académico y resoluciones de procedimientos académicos; a la Plataforma de RegresaTec en las plataformas oficiales del Tecnológico Nacional de México.

VIII. El resguardo de los soportes físicos de los datos personales.

Los expedientes físicos se encuentran resguardados y en custodia de los responsables del sistema de tratamiento de los datos personales en el área asignada para tal efecto.



“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

XI. El análisis de brecha.

28. [Redacted]
- [Redacted]
 - [Redacted]
 - [Redacted]
 - [Redacted]
 - [Redacted]
29. [Redacted]

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- 30. [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- 31. [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- 32. [Redacted]
- [Redacted]
- [Redacted]

“Se testian las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

XII. La gestión de vulneraciones.

En caso de ocurrir alguna vulneración deberá registrarse en la bitácora de contingencias (Anexo 2), y se llevará a cabo conforme al siguiente procedimiento:

- 22. Detección y aviso interno:** El personal de la Dirección Académica que detecte o sospeche de una vulneración lo comunicará de inmediato a la Directora Académica, preservando el estado de los documentos, equipos o sistemas involucrados.
- 23. Contención:** Se ejecutarán acciones inmediatas para evitar mayor afectación, tales como resguardar el archivo, suspender accesos, cambiar contraseñas o desconectar el equipo comprometido.
- 24. Registro inicial:** Se asentará en la bitácora la fecha y hora de la vulneración, el documento o información vulnerada y el motivo de la vulneración.
- 25. Evaluación:** La Directora determinará el alcance del incidente, las personas titulares afectadas y si se comprometen sus derechos patrimoniales o morales.

- 26. Acciones correctivas y definitivas:** Se implementarán las medidas para reestablecer la información y eliminar la causa, y se registrarán en la bitácora junto con el nombre de la persona que resolvió la vulneración.
- 27. Notificación:** Se informará a las personas titulares, dentro del plazo no mayor a 3 días (72 horas), la notificación incluirá la naturaleza del incidente, los datos personales comprometidos, las recomendaciones para la persona titular, las acciones correctivas realizadas y los medios para obtener mayor información. Se registrará en la bitácora la fecha y hora de cada notificación.
- 28. Cierre y prevención.** La Directora revisará las medidas de seguridad vigentes y ajustará las que resulten necesarias para evitar que el incidente se repita.

XIII. Las medidas de seguridad físicas aplicadas a las instalaciones.

42. [REDACTED]
43. [REDACTED]
44. [REDACTED]
45. [REDACTED]

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIPI) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

[Redacted text block]

XIV. LOS CONTROLES DE IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS.

46. [Redacted text block]
47. [Redacted text block]

XV. LOS PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS PERSONALES.

48. [Redacted text block]
49. [Redacted text block]

XVI. EL PLAN DE CONTINGENCIA.

50. [Redacted text block]
51. [Redacted text block]

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIIP) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

XVII. LAS TÉCNICAS UTILIZADAS PARA LA SUPRESIÓN Y BORRADO SEGURO DE LOS DATOS PERSONALES.

52. Los expedientes, minutas, constancias y demás documentos académicos que contengan datos personales sólo podrán eliminarse una vez cumplidos los periodos de conservación y disposiciones académicas y archivísticas aplicables. Los documentos físicos cuya eliminación proceda deberán destruirse de manera que no puedan reconstruirse; los archivos electrónicos deberán borrarse de forma segura.
53. No deberán reutilizarse como papel de borrador documentos que contengan información personal o académica.

XVIII. EL PLAN DE TRABAJO.

54. [REDACTED]
55. [REDACTED]

XIX. LOS MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD.

56. La Dirección Académica realizará el monitoreo de los accesos físicos y electrónicos, las bitácoras, los permisos de sistemas, las transferencias de información y la disponibilidad de los respaldos institucionales.
57. Los incidentes, cambios de sistemas o nuevas amenazas deberán analizarse para actualizar las medidas de seguridad y el presente Documento de Seguridad.

XX. EL PROGRAMA GENERAL DE CAPACITACIÓN.

58. El personal que intervenga en los tratamientos de la Dirección Académica deberá recibir capacitación sobre confidencialidad, avisos de privacidad, derechos ARCOP, manejo de información académica y sensible, uso seguro de MindBox, Comité Académico, transferencias, bitácoras y respuesta a vulneraciones.
59. La capacitación deberá reforzarse cuando cambien los procesos, sistemas, personal o riesgos de seguridad.

“Se testan las amenazas y vulnerabilidades existentes, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 115 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIPI) y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.”

ANEXO 1: Bitácora de acceso a los Datos Personales

Órgano Administrativo (o área generadora/resguardante):

Instituto Tecnológico Superior de Cintalapa
Dirección Académica.

Responsable del Archivo:

Rubí Alejandra González Gutiérrez
Directora Académica

Número Progresivo	Nombre completo (de quien accede a los datos personales)	Cargo	Área de adscripción	Propósito del acceso	Número de control del alumno y/o egresado	Tipo de soporte utilizado (Expediente o registro electrónico)	Fecha en formato (al que corresponde la bitácora) día, mes y año

ANEXO 2: Bitácora de vulneraciones a la seguridad de los Datos Personales

Órgano Administrativo (o área generadora/resguardante):

Instituto Tecnológico Superior de Cintalapa
Dirección Académica.

Responsable del Archivo:

Rubí Alejandra González Gutiérrez
Directora Académica

Número progresivo	Fecha y Hora de Vulneración	Documento o información vulnerada	Motivo de la vulneración	Acciones correctivas y definitivas implementadas	Persona que resolvió la vulneración	Fecha y hora de notificación de la vulneración a los titulares de los datos personales comprometidos	Fecha en formato (al que corresponde la bitácora) día, mes y año