



EDUCACIÓN
SECRETARÍA DE EDUCACIÓN PÚBLICA



2026
año de
Margarita
Maza



**UNIVERSIDAD
TECNOLÓGICA
DE LA SELVA**
CIBICENTRO DE CHIAPAS
8000 - 0100

DOCUMENTO DE SEGURIDAD DE LA UNIVERSIDAD TECNOLÓGICA DE LA SELVA.

www.utselva.edu.mx

Entronque Toniná Km 0.5 carretera Ocosingo-Altamirano
Ocosingo, Chiapas; México. C.P. 29950

Teléfonos: (52) (919) 67 3 09 70, 72, 67 3 12 90, 93



**UT
SELVA**

UNIVERSIDAD
TECNOLÓGICA
DE LA SELVA



ISO 9001:2015
ISO 14001:2015
ISO 27001:2018



DOCUMENTO DE SEGURIDAD DE LA UNIVERSIDAD TECNOLÓGICA DE LA SELVA.

1.-Introducción	4
2.- Objetivo del Documento De Seguridad.....	5
2.1.- Objetivo general.	5
2.2.- Objetivo específico.....	5
3.- Alcance del Documento de Seguridad.....	5
3.1.- Roles y responsabilidades en materia de seguridad de datos personales.....	5
3.2.- Comité de transparencia.....	6
Atribuciones y Funciones:	6
3.3. Alta dirección (Rectoría).....	6
Atribuciones y Funciones:	6
4.- Sistema de gestión de seguridad de los Datos Personales en Posesión de la Universidad Tecnológica de la Selva.....	8
4.1.- Fase de planificación (planear).....	8
4.2.- Fase de implementación (hacer).....	9
4.3.- Fase de verificación y monitoreo (verificar).....	10
4.4.- Fase de mejora continua (actuar).....	11
5.- Inventario de Datos Personales y Sistemas de Tratamientos.....	11
5.1.- Abogado General (incluye Unidad de Transparencia, Unidad de Igualdad de Género y Coordinación de Archivo).....	12
5.2. Secretaría Académica (incluye Direcciones de División: Agroalimentaria, Administración, TI, Turismo/ Gastronomía y Construcción).....	12
5.3.- Departamento de Servicios Escolares (adscrito a la Secretaría Académica).....	13
5.4. Departamento de Servicios Bibliotecarios (adscrito a la Secretaría Académica).....	14
5.5. Departamento de Servicios Estudiantiles (adscrito a la Secretaría Académica).....	14
5.6. Dirección de Vinculación.....	14
5.7. Dirección de Planeación y Evaluación.....	15
5.9. Subdirección de Servicios Administrativos y Departamento de Recursos Materiales y Servicios Generales.....	16
5.10. Subdirección de Tecnologías de la Información, Comunicación y Redes.....	16
5.11. Departamento de Contabilidad.....	17





5.12. Departamentos de Sistema de Gestión de la Calidad.....	17
5.13. Departamentos de Prensa y Difusión.....	18
5.14. Departamentos de Actividades Deportivas y Culturales.....	18
6.- Funciones y obligaciones de las personas que tratan datos personales.....	20
7.- Evaluación y diagnóstico de medidas de seguridad (análisis de riesgos de los Sistemas de Datos Personales).....	23
7.1.- Criterios para la evaluación del riesgo inherente.....	23
7.2.- Matriz institucional de evaluación de riesgos por unidad administrativa.....	24
7.3.- Análisis de brecha.....	25
7.3.1.- Diagnóstico comparativo de medidas de seguridad.....	25
7.4.- Entregables estratégicos derivados del análisis de brecha.....	26
7.4.1.- Plan de trabajo institucional.....	26
7.4.2.- Mecanismos de monitoreo y revisión de medidas de seguridad.....	26
7.4.3.- Programa interno de capacitación y sensibilización.....	27
8.- Protocolo para la gestión, registro y notificación de incidencias de seguridad.....	28
8.1.- Objetivo y alcance.....	28
8.2.- Eventos de vulneración considerados.....	28
8.2.1.- Medidas de seguridad físicas y técnicas.....	28
8.3.- Procedimiento y flujo de notificación sin dilación.....	29
8.4.- Formato operativo: bitácora de registro de incidencias de seguridad.....	30
8.5. Acciones prioritarias de mitigación técnica (análisis de brecha).....	30
9.- Mecanismos de revisión, monitoreo y actualización del Documento de Seguridad.....	31
9.1. Criterios y causal de actualización obligatoria.....	31
9.2. Periodicidad de revisión ordinaria.....	32
10. Formalización, dictamen y aprobación normativa.....	32





DOCUMENTO DE SEGURIDAD DE LA UNIVERSIDAD TECNOLÓGICA DE LA SELVA.

1.-Introducción

El presente Documento de Seguridad se constituye como el instrumento rector que describe de manera integral y sistemática las medidas de seguridad administrativas, físicas y técnicas implementadas por la Universidad Tecnológica de la Selva para la protección de los datos personales que obran en su posesión.

Como institución pública de educación superior y Sujeto Obligado en términos de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas (LPDPPSOCHIS), la Universidad Tecnológica de la Selva asume el compromiso legal, ético y social de velar por el cumplimiento del deber de seguridad. Este deber exige salvaguardar la confidencialidad, integridad y disponibilidad de la información personal que la comunidad universitaria (estudiantes, docentes, personal administrativo, proveedores y ciudadanía en general) proporciona para llevar a cabo trámites, gestiones, procesos académicos, administrativos y la prestación de servicios institucionales.

A través de este documento, se articula un Sistema de Gestión de Seguridad de los Datos Personales que abarca todo el ciclo de vida de la información –desde su obtención, uso y almacenamiento, hasta su eventual supresión o eliminación–. Asimismo, reúne los elementos exigidos por la normatividad vigente, tales como:

- El inventario de datos personales y de los sistemas de tratamiento institucionales.
- La identificación de las funciones y obligaciones del personal involucrado en el tratamiento de la información.
- El análisis de riesgos y el análisis de brecha para diagnosticar y mitigar las vulnerabilidades existentes.
- El plan de trabajo y los mecanismos de monitoreo y revisión continua.
- El programa interno de capacitación orientado a fortalecer la cultura de la protección de datos entre los servidores públicos universitarios.

Con la implementación de este Documento de Seguridad, la Universidad Tecnológica de la Selva busca promover un tratamiento lícito, transparente y responsable de los datos personales, previniendo situaciones que pongan en riesgo la información, tales como su daño, pérdida, alteración, destrucción, o el acceso, uso o transferencia no autorizada, consolidando así la cultura de la transparencia, la seguridad de la información y las buenas prácticas institucionales.





2.- Objetivo del Documento De Seguridad.

2.1.- Objetivo general.

Establecer, describir y normar las medidas de seguridad administrativas, físicas y técnicas implementadas por la Universidad Tecnológica de la Selva para garantizar la confidencialidad, integridad y disponibilidad de las datos personales que posee, obtiene y trata en el ejercicio de sus atribuciones legales, asegurando el cumplimiento de la *Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas* y previniendo su daño, pérdida, alteración, destrucción o el uso, acceso a tratamiento no autorizado.

2.2.- Objetivo específico.

- **Garantizar la protección de los datos personales:** Definir los controles y protocolos de seguridad adecuados a los riesgos y tipos de tratamiento aplicados a los datos personales de estudiantes, docentes, personal administrativo, proveedores y público en general.
- **Integrar el Sistema de Gestión de Seguridad:** Organizar de manera estructurada el inventario de tratamientos, el análisis de riesgos, el análisis de brecha y el plan de trabajo para el fortalecimiento continuo de las medidas de seguridad.
- **Delimitar responsabilidades:** Formalizar las funciones y obligaciones del personal que realiza tratamientos de datos personales en cada una de las unidades administrativas de la Universidad.
- **Atender vulnerabilidades e incidencias:** Disponer de los procedimientos necesarios para la prevención, detección, contención y respuesta ante posibles vulneraciones a la seguridad de la información.

3.- Alcance del Documento de Seguridad.

3.1.- Roles y responsabilidades en materia de seguridad de datos personales.

En cumplimiento a lo dispuesto por la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas y las directrices institucionales en materia de seguridad de la información, la Universidad Tecnológica de la Selva establece una estructura jerárquica de funciones y responsabilidades para garantizar la confidencialidad, integridad y disponibilidad de los datos personales bajo su resguardo.





3.2- Comité de transparencia,

El Comité de Transparencia es el órgano colegiado de máxima autoridad instituido para supervisar, dictaminar y vigilar el cumplimiento de las disposiciones en materia de transparencia, acceso a la información y protección de datos personales en la Universidad Tecnológica de la Selva.

Atribuciones y Funciones:

1. **Supervisión y Vigilancia:** Vigilar el cumplimiento normativo de los principios, deberes y obligaciones establecidos en la legislación de datos personales por parte de todas las Unidades Administrativas de la Institución.
2. **Aprobación del Documento de Seguridad:** Revisar, dictaminar y aprobar de manera formal el *Documento de Seguridad de la Universidad Tecnológica de la Selva*, así como sus actualizaciones y modificaciones sustanciales.
3. **Rendición de Cuentas e Informe Anual:** Elaborar, aprobar y presentar el Informe Anual de Cumplimiento en materia de Protección de Datos Personales durante las primeras dos semanas de marzo de cada año, dando cuenta de los avances del Plan de Trabajo, análisis de riesgos y estado general del Sistema de Gestión de Seguridad.
4. **Coordinación Institucional:** Promover la adopción e implementación de las medidas de seguridad administrativas, físicas y técnicas aprobadas, asegurando la constante actualización del inventario de tratamientos y la gestión de vulneraciones o incidencias de seguridad.

3.3. Alta dirección (Rectoría)

La Rectoría, en su calidad de máxima autoridad ejecutiva de la Universidad Tecnológica de la Selva, actúa como la instancia estratégica y facilitadora del Sistema de Gestión de Seguridad de Datos Personales.

Atribuciones y Funciones:

1. **Facilitador de Recursos Institucionales:** Asignar y proveer los recursos humanos, presupuestales, tecnológicos y materiales necesarios para la correcta ejecución e implementación de las medidas de seguridad físicas, técnicas y administrativas contenidas en el Plan de Trabajo Institucional.
2. **Respaldo Institucional y Gobernanza:** Respaldo institucionalmente las políticas, lineamientos, protocolos y programas de capacitación promovidos por el Comité de Transparencia y la Unidad de Transparencia/Oficial de Protección de Datos Personales.
3. **Impulso de la Mejora Continua:** Garantizar la sostenibilidad del Sistema de Gestión de Seguridad de Datos Personales (SGSDP) bajo el enfoque de mejora continua, dentro del Plan de Desarrollo Institucional.

El presente Documento de Seguridad es de observancia general y obligatoria para todas las autoridades, directivos, personal docente, administrativo, operativo, prestadores de servicio social, prácticas profesionales y encargados externos que, en razón de sus funciones o mediante



encargo, intervengan en cualquier fase del tratamiento de datos personales dentro de la Universidad Tecnológica de la Selva.

Su aplicación abarca:

1. **Sistemas de Tratamiento de Datos Personales:** Todos los archivos, bases de datos, sistemas de información informáticos y soportes físicos (archivos impresos, expedientes, carpetas u otros mediares) que contengan datos personales o datos personales sensibles administrados por las Unidades Académicas, Secretarías, Direcciones, Departamentos y demás áreas operativas de la Institución.
2. **Ciclo de Vida de los Datos:** Todos los procesos operativos y administrativos que involucren la obtención, recolección, registro, organización, conservación, uso, consulta, transferencia, comunicación, almacenamiento o supresión de datos personales.
3. **Procesos Institucionales:** Entre los tratamientos comprendidos de manera enunciativa mas no limitativa, se destacan:
 - **Procesos Escolares y Académicos:** Captación, admisión, inscripción, emisión de credenciales, historial académico, tramitación de becas, servicio social, estadías profesionales, titulación y bolsa de trabajo.
 - **Recursos Humanos:** Expedientes del personal docente y administrativo, nómina, contrataciones, evaluación del desempeño y trámites prestacionales.
 - **Vinculación y Servicios a la Comunidad:** Convenios con empresas e instituciones, cursos de educación continua y vinculación con egresados.
 - **Recursos Financieros y Materiales:** Padrón de proveedores, contrataciones de bienes/servicios, facturación y control de accesos a las instalaciones.

Las unidades administrativas que tratan datos personales en la Universidad Tecnológica de la Selva son las siguientes:

1. **Abogacía general**
 - a. Unidad de Transparencia
 - b. Unidad de Igualdad de Género
 - c. Coordinación de archivo
2. **Secretaría académica**
 - a. Dirección de la división agroalimentaria
 - b. Dirección de la división de administración





- c. Dirección de la división de tecnologías de la información
- d. Dirección de la división de turismo y gastronomía
- e. Dirección de la división de construcción
- 2.1. Departamento de servicios escolares
- 2.2. Departamento de servicios bibliotecarios
- 2.3. departamento de servicios estudiantiles
3. Dirección de vinculación
4. Dirección de planeación y evaluación
5. Subdirección de informática administrativa y recursos humanos
6. Subdirección de servicios administrativos
7. Departamento de recursos materiales y servicios generales
8. Subdirección de tecnologías de la información, comunicación y redes
9. Departamento de contabilidad
10. Departamento de sistema de gestión de la calidad
11. Departamento de prensa y difusión
12. Departamento de cultura y deporte

En este sentido, la Unidad de Transparencia integra el presente documento de seguridad con base en la información generada por las citadas unidades administrativas acorde al ámbito de sus funciones y, de conformidad con las disposiciones aplicables.

4.- Sistema de gestión de seguridad de los Datos Personales en Posesión de la Universidad Tecnológica de la Selva.



La Universidad Tecnológica de la Selva adopta e implementa un Sistema de Gestión de Seguridad de los Datos Personales (5G5DP) basado en la mejora continua mediante el ciclo PHVA (Planear, Hacer, Verificar, Actuar), permitiendo adaptar las medidas de seguridad administrativas, físicas y técnicas al nivel de riesgo y contexto institucional.

4.1.- Fase de planificación (planear).

En esta fase la Universidad establece los fundamentos operativos y organizacionales para determinar las necesidades de protección de los datos personales:

1. Elaboración del Inventario de Datos Personales:



Se identifican, registran y catalogan todas las bases de datos y sistemas de tratamiento (físicos y digitales) de las Unidades Académicas, Áreas Administrativas y de Vinculación de la Universidad. Se especifica la tipología de datos, finalidades del tratamiento, encargados y flujos o transferencias de información.

2. Identificación de Funciones y Responsabilidades:

Se asignan los roles de seguridad de la información. La coordinación del SGSDP recae en el Oficial de Protección de Datos Personales / Unidad de Transparencia, en coordinación con la Dirección de Tecnologías de la Información y los responsables de cada área o departamento (titulares académicos y administrativos).

3. Análisis de Riesgos:

Se evalúan las amenazas y vulnerabilidades que enfrentan los sistemas de tratamiento institucionales, determinando el impacto potencial sobre los derechos de los titulares (estudiantes, docentes, personal y proveedores) ante eventos de acceso indebido, pérdida, alteración o filtración.

4. Análisis de Brecha:

Se realiza un diagnóstico comparativo entre las medidas de seguridad vigentes en la Universidad y los requisitos exigidos por la LPDPPSOCHIS y la Guía institucional, a fin de identificar vacíos en materia normativa, técnica o física.

5. Plan de Trabajo de Seguridad:

Se diseña la hoja de ruta estratégica con metas, recursos, responsables y plazos de ejecución para subsanar los hallazgos del análisis de brecha e implementar las medidas preventivas y correctivas necesarias.

4.2.- Fase de implementación (hacer).

Se ejecutan las medidas operativas y se implementan las políticas definidas en la fase de planificación:

1. Ejecución del Plan de Trabajo:

Se llevan a cabo los proyectos de infraestructura, configuración técnica y formalización documental programados.

2. Diseño e Implementación de Medidas de Seguridad:

- **Medidas Administrativas:** Emisión de políticas internas de acceso a la información, acuerdos de confidencialidad para el personal docente y administrativo, y





procedimientos para la atención de ejercicios de Derechos ARCO y reporte de incidencias.

- **Medidas Físicas:** Control de acceso a los soportes impresos (archiveros con llave, almacenes de archivo escolar) y a los centros de cómputo/servidores de la Institución mediante bitácoras y restricción de personal no autorizado.
- **Medidas Técnicas:** Implementación de contraseñas seguras, perfiles de usuario por rol, respaldos de información periódicos, antivirus institucionales, cifrado de datos sensibles e instalación de firewalls en la red universitaria.

3. Programa de Capacitación y Sensibilización:

Capacitación continua al personal de la Universidad que trate datos personales para promover la cultura de protección, privacidad por diseño y uso ético de la información.

4. Gestión de Vulneraciones a la Seguridad:

Activación del procedimiento institucional de respuesta rápida ante fugas, pérdidas o incidentes de seguridad en los sistemas de información para contención, remediación y notificación formal a la autoridad garante (ITAIPCH).

4.3.- Fase de verificación y monitoreo (verificar).

La Universidad somete a revisión constante la efectividad de las medidas adoptadas para comprobar el correcto funcionamiento del SGSDP:

1. Monitoreo Continuo:

Seguimiento permanente al cumplimiento de las políticas de seguridad y la efectividad de los controles técnicos y de acceso en las plataformas institucionales (sistemas escolares, nómina, plataformas académicas).

2. Revisiones y Auditorías de Seguridad:

Evaluación periódica (mínimo una vez al año o cuando ocurran cambios sustanciales en los sistemas de información) del estado del inventario de datos personales y de los análisis de riesgo.

3. Atención de Incidencias:

Registro y seguimiento de todas las bitácoras de incidentes de seguridad física y técnica ocurridas en las instalaciones y servidores universitarios.



4.4.- Fase de mejora continua (actuar).

Con base en los resultados del monitoreo, auditorías y cambios en la organización o en la tecnología, se ajustan los controles institucionales:

1. **Acciones Preventivas y Correctivas:**

Implementación de ajustes inmediatos ante vulneraciones detectadas o riesgos emergentes generados por la adopción de nuevos software o procesos educativos.

2. **Actualización del Documento de Seguridad:**

Modificación y actualización del Documento de Seguridad ante:

- Cambios en las normas de protección de datos personales.
- Transformaciones en la estructura orgánica de la Universidad.
- Creación de nuevos trámites, servicios o plataformas tecnológicas que traten datos personales.
- Modificaciones sustanciales en el análisis de riesgo institucional.



5.- Inventario de Datos Personales y Sistemas de Tratamientos.

En cumplimiento a lo establecido en el Artículo 27, fracción III, y Artículo 29 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas (LPDPPSOCHIS), así como en las directrices de la Guía institucional, la Universidad Tecnológica de la Selva ha



formalizado la estructuración y catalogación de los tratamientos de datos personales efectuados por sus 14 Unidades Administrativas y áreas adscritas. A continuación, se detalla el inventario formalizado correspondiente a cada una de las unidades responsables:

5.1.- Abogado General (incluye Unidad de Transparencia, Unidad de Igualdad de Género y Coordinación de Archivo).

Componente	Descripción del inventario institucional
Nombre del tratamiento / trámite	Atención a Solicitudes de Acceso a la Información, Solicitudes de Derechos ARCOP. Quejas y Denuncias por Violencia de Género o Hostigamiento. Gestión y Resguardo del Archivo de Concentración Institucional.
Tipo y catálogo de datos recopilados	Identificativos: Nombre, CURP, RFC, firma, domicilio, correo electrónico, teléfono, identificación oficial. Sensibles: Datos de salud, testimonios o relatos sobre probables conductas de acoso/hostigamiento, perspectiva de género o discriminación.
Medio de obtención y almacenamiento	Mixto: Solicitudes y quejas recibidas en físico (formatos impresos, expedientes) y mediante medios electrónicos (plataformas de transparencia y correo institucional).
Finalidades del tratamiento	Tramitar el ejercicio de derechos ARCOP, sustanciar procedimientos administrativos y jurídicos internos, e integrar el registro de archivo documental
Servidores públicos con acceso	Abogada General, Titular de la Unidad de Transparencia, Enlace de Igualdad de Género y Coordinador de Archivo.
Transferencias o remisiones	Transferencias: Órgano Garante de Transparencia para el Pueblo de Chiapas y Órganos Jurisdiccionales. Fundamento Legal: Ley de Protección de Datos Personales y Ley de Transparencia del Estado de Chiapas.
Plazo de conservación	Conforme al Catálogo de Disposición Documental: 1 a 3 años en Archivo de Trámite; 5 años en Archivo de Concentración.
Transferencias o remisiones	"No aplican remisiones a encargados externos".

5.2. Secretaría Académica (incluye Direcciones de División: Agroalimentaria, Administración, TI, Turismo/Gastronomía y Construcción).

Componente	Descripción del inventario institucional
Nombre del tratamiento / trámite	Comisiones para docentes y administrativos, informes internos y externos, permisos para docentes y administrativos.



	Asesorías, carga horaria, estadías, comisiones para docentes y administrativos, grupos de WhatsApp, horario de docentes y grupos, informes internos y externos, listas de asistencia, permiso de alumno, permiso de docentes y administrativos, tutorías.
Tipo y catálogo de datos recopilados	Identificativos: Nombre, matrícula, RFC, CURP, firma. Laborales: Cédula profesional, grado académico, perfil profesional. Contacto: número telefónico, correo electrónico, dirección.
Medio de obtención y almacenamiento	Mixto: Fórmulas digitales en plataforma académica/escolar, formatos y expedientes físicos en direcciones de división.
Finalidades del tratamiento	Control e impartición de asignaturas, seguimiento del desempeño escolar y gestión de cuerpos docentes, etc.
Servidores públicos con acceso	Secretario Académico, Directores de División Académica, Coordinadores de Programa Educativo y Tutores.
Transferencias o remisiones	Transferencias: Secretaría de Educación Pública (SEP) y Universidades Tecnológicas (CGUTyP). Fundamento: Cumplimiento de normatividad educativa estatal y federal.
Plazo de conservación	Conforme al Catálogo de Disposición Documental: 2 años en Archivo de Trámite; posterior baja o concentración según valoración.
Transferencias o remisiones	"No aplican remisiones a encargados externos".

5.3.- Departamento de Servicios Escolares (adscrito a la Secretaría Académica).

Componente	Descripción del inventario institucional
Nombre del tratamiento / trámite	Registro y Control Escolar (Inscripción y Reinscripción). Titulación y afiliación al IMSS.
Tipo y catálogo de datos recopilados	Identificativos: Nombre, matrícula, RFC, CURP, firma. Contacto: número telefónico, correo electrónico, dirección.
Medio de obtención y almacenamiento	Mixto: Físico (expediente impreso de nuevo ingreso) y Digital (Sistema Integral de Control Escolar).
Finalidades del tratamiento	Validar la matrícula, llevar el historial académico, certificar estudios e integrar el Padrón General de Estudiantes.
Servidores públicos con acceso	Jefe del Departamento de Servicios Escolares y Analistas de Servicios Escolares.
Transferencias o remisiones	Transferencias: Dirección General de Profesiones (DGP-SEP) Fundamento: Ley General de Educación.
Plazo de conservación	Conservación permanente en expediente digital y archivo físico por el valor histórico-académico de la matrícula.





Transferencias o remisiones	"No aplican remisiones a encargados externos".
-----------------------------	--

5.4. Departamento de Servicios Bibliotecarios (adscrito a la Secretaría Académica).

Componente	Descripción del inventario institucional
Nombre del tratamiento / trámite	Acceso sistematizado (SISTGEBI) registro de usuarios de Biblioteca y préstamo de acervo Bibliográfico.
Tipo y catálogo de datos recopilados	Identificativos: nombre, NSS, Firma.
Medio de obtención y almacenamiento	Digital Base de datos del Sistema de Gestión Bibliotecaria.
Finalidades del tratamiento	Control de préstamos de libros en sala/domicilio y emisión de cartas de no adeudo bibliotecario.
Servidores públicos con acceso	Jefe del Departamento de Servicios Bibliotecarios y Encargados de Módulo de Atención
Transferencias o remisiones	No se realizan transferencias de datos a terceros
Plazo de conservación	Conforme al Catálogo de Disposición Documental: Duración mientras el usuario mantenga estatus activo en la Institución.
Transferencias o remisiones	"No aplican remisiones a encargados externos".

5.5. Departamento de Servicios Estudiantiles (adscrito a la Secretaría Académica).

Componente	Descripción del inventario institucional
Nombre del tratamiento / trámite	Servicios de pedagogía, psicología y enfermería.
Tipo y catálogo de datos recopilados	Identificativos: Nombre, edad, matrícula, género. Contacto: número telefónico.
Medio de obtención y almacenamiento	Mixto: Fórmulas e historiales clínicos físicos resguardados en enfermería y plataforma digital de alumnos.
Finalidades del tratamiento	Atención médica de primeros auxilios, atención psicológica y atención pedagógica.
Servidores públicos con acceso	Jefe del Departamento de Servicios Estudiantiles, Personal de Enfermería, psicólogos.
Transferencias o remisiones	Transferencias: Instituto Mexicano del Seguro Social (IMSS).
Plazo de conservación	5 años posteriores al egreso o baja definitiva del estudiante.
Transferencias o remisiones	"No aplican remisiones a encargados externos".

5.6. Dirección de Vinculación.

Componente	Descripción del inventario institucional
Nombre del tratamiento / trámite	Becas, consejo de vinculación, convenios, estancias y estadías, movilidad nacional e internacional.
Tipo y catálogo de datos recopilados	Identificativos: Nombre, CURP, firma. Contacto: número telefónico, correo electrónico, dirección.





Medio de obtención y almacenamiento	Mixto: Expedientes físicos de asignación de estadías y sistema de seguimiento de egresados
Finalidades del tratamiento	Vincular al alumnado con unidades productivas, dar seguimiento a la empleabilidad y coordinar el Servicio Social.
Servidores públicos con acceso	Director de Vinculación, Jefes de Departamento.
Transferencias o remisiones	Transferencias: Empresas e instituciones públicas/privadas receptoras de estadías y Servicio Social. Fundamento: Convenios Marco de Colaboración y Lineamientos de Estadías.
Plazo de conservación	Conforme al Catálogo de Disposición Documental: 3 años en Archivo de Trámite; 5 años en Archivo de Concentración.
Transferencias o remisiones	"No aplican remisiones a encargados externos".

5.7. Dirección de Planeación y Evaluación.

Componente	Descripción del inventario institucional
Nombre del tratamiento / trámite	Cedulas presupuestales
Tipo y catálogo de datos recopilados	Identificativos: Nombre, RFC, firma.
Medio de obtención y almacenamiento	Físico solicitud de cedula y formatos de comisión.
Finalidades del tratamiento	Cumplir con la rendición de cuentas, reporte de indicadores de calidad y planificación.
Servidores públicos con acceso	Director de Planeación y Evaluación y Analistas de Estadística Institucional.
Transferencias o remisiones	Transferencias: Secretaría de Educación Pública (SEP) y Secretaría de Hacienda del Estado de Chiapas. Fundamento: Ley de Planeación y normatividad estadística.
Plazo de conservación	Conservación permanente de reportes estadísticos consolidados.
Transferencias o remisiones	"No aplican remisiones a encargados externos".

5.8. Subdirección de Informática Administrativa y Recursos Humanos.

Componente	Descripción del inventario institucional
Nombre del tratamiento / trámite	Nómina del personal, registro y control de asistencia del personal, sistemas de videovigilancia (CCTV).
Tipo y catálogo de datos recopilados	Identificativos: Nombre, RFC, CURP firma. Contacto: Correo electrónico. Datos biométricos: reconocimiento facial, y huellas digitales.
Medio de obtención y almacenamiento	Mixto: Expedientes físicos resguardados en archiveros de seguridad y Sistema Informático de Nómina, imagen del sistema de video vigilancia.





Finalidades del tratamiento	Gestión de la relación laboral, pago de salarios, cumplimiento de obligaciones fiscales y seguridad social.
Servidores públicos con acceso	Subdirector de Recursos Humanos, Encargado de Nómina y Auxiliares Administrativos del área.
Transferencias o remisiones	Transferencias: Servicio de Administración Tributaria (SAT), IMSS, INFONAVIT, ISSTECH y Bancos Pagadores (BANXICO/Instituciones bancarias procesadoras). Fundamento: Ley Federal del Trabajo, Ley del Seguro Social y Código Fiscal.
Plazo de conservación	Expediente laboral: Vigencia de la relación laboral + 10 años en Archivo de Concentración conforme a leyes fiscales y laborales.
Transferencias o remisiones	"No aplican remisiones a encargados externos".

5.9. Subdirección de Servicios Administrativos y Departamento de Recursos Materiales y Servicios Generales.

Componente	Descripción del inventario institucional
Nombre del tratamiento / trámite	Licitaciones, pago a proveedores, contratación de bienes y/o servicios.
Tipo y catálogo de datos recopilados	Identificativos: Nombre, RFC, CURP, firma. Contacto: Correo electrónico, número telefónico. Datos bancarios: número de cuenta y CLABE interbancaria.
Medio de obtención y almacenamiento	Mixto: Expedientes físicos de licitaciones/contratos.
Finalidades del tratamiento	Dar de alta en el catálogo de proveedores, formalizar contratos de adquisición/arrendamiento.
Servidores públicos con acceso	Subdirector de Servicios Administrativos, Jefe de Recursos Materiales.
Transferencias o remisiones	Transferencias: Auditoría Superior del Estado (ASE), Secretaría de la Honestidad y Función Pública. Fundamento: Ley de Adquisiciones y Arrendamientos del Estado de Chiapas.
Plazo de conservación	Conforme al Catálogo de Disposición Documental: 5 a 10 años en cumplimiento a las auditorías fiscales.
Transferencias o remisiones	"No aplican remisiones a encargados externos".

5.10. Subdirección de Tecnologías de la Información, Comunicación y Redes.

Componente	Descripción del inventario institucional
Nombre del tratamiento / trámite	Página web institucional, GECKO GPE (gestor de procesos educativos)
Tipo y catálogo de datos recopilados	Identificativos: Nombre, RFC, CURP, firma. Contacto: Correo electrónico, número telefónico.
Medio de obtención y almacenamiento	Digital: Servidores institucionales, bases de datos y sistemas de gestión de identidades.



Finalidades del tratamiento	Proveer credenciales tecnológicas, garantizar el uso correcto de la infraestructura de red.
Servidores públicos con acceso	Subdirector de TI, Administrador de Redes y Administrador de Bases de Datos.
Transferencias o remisiones	No se efectúan transferencias, salvo requerimiento judicial debidamente fundado.
Plazo de conservación	Logs de sistema: 1 año; Cuentas de usuario: Durante la vigencia de la relación académica o laboral.
Transferencias o remisiones	"No aplican remisiones a encargados externos".

5.11. Departamento de Contabilidad.

Componente	Descripción del inventario institucional
Nombre del tratamiento / trámite	Pago de viáticos
Tipo y catálogo de datos recopilados	Identificativos: Nombre, RFC, firma. Contacto: Correo electrónico, número telefónico. Dirección. Datos bancarios: número de cuenta, CLABE interbancaria.
Medio de obtención y almacenamiento	Físico: tramites de viáticos.
Finalidades del tratamiento	Realizar comprobación necesaria referente al pago de viáticos.
Servidores públicos con acceso	Jefe del Departamento de Contabilidad, Contadores y Auxiliares.
Transferencias o remisiones	Transferencias: Servicio de Administración Tributaria (SAT) y Secretaría de Hacienda del Estado. Fundamento: Código Fiscal de la Federación.
Plazo de conservación	5 a 10 años conforme a las obligaciones estipuladas por el Código Fiscal de la Federación.
Transferencias o remisiones	"No aplican remisiones a encargados externos".

5.12. Departamentos de Sistema de Gestión de la Calidad.

Componente	Descripción del inventario institucional
Nombre del tratamiento / trámite	Listas de asistencia y procedimientos del sistema de gestión integral.
Tipo y catálogo de datos recopilados	Identificativos: Nombre, sexo. Contacto: Correo electrónico, número telefónico. dirección.
Medio de obtención y almacenamiento	Físico: mediante validación de formatearía.
Finalidades del tratamiento	Coordinación de auditorías ISO, recabar datos estadísticos de los procedimientos y actividades del sistema de gestión integral.
Servidores públicos con acceso	Jefe del Departamento
Transferencias o remisiones	No se efectúan transferencias, salvo requerimiento judicial debidamente fundado.
Plazo de conservación	Conforme al Catálogo de Disposición Documental: 1 a 3 años según la vigencia de la actividad o ciclo de acreditación.
Transferencias o remisiones	"No aplican remisiones a encargados externos".

5.13. Departamentos de Prensa y Difusión.

Componente	Descripción del inventario institucional
Nombre del tratamiento / trámite	Difusión institucional.
Tipo y catálogo de datos recopilados	Identificativos: Nombre, firma.
Medio de obtención y almacenamiento	Físico: mediante validación de formatearía.
Finalidades del tratamiento	Promoción institucional.
Servidores públicos con acceso	Jefe del Departamento
Transferencias o remisiones	No se efectúan transferencias, salvo requerimiento judicial debidamente fundado.
Plazo de conservación	Conforme al Catálogo de Disposición Documental: 1 a 3 años según la vigencia de la actividad o ciclo de acreditación.
Transferencias o remisiones	"No aplican remisiones a encargados externos".

5.14. Departamentos de Actividades Deportivas y Culturales.

Componente	Descripción del inventario institucional
Nombre del tratamiento / trámite	Listas de asistencia.
Tipo y catálogo de datos recopilados	Identificativos: Nombre, matrícula, firma.
Medio de obtención y almacenamiento	Físico: mediante validación de formatearía.
Finalidades del tratamiento	Promover el desarrollo integral del estudiantado, coordinar la participación en competencias deportivas y culturales locales, regionales y nacionales, y salvaguardar la salud física durante el desarrollo de las actividades.
Servidores públicos con acceso	Jefe del Departamento de cultura y deporte, entrenadores, docentes.
Transferencias o remisiones	No se efectúan transferencias, salvo requerimiento judicial debidamente fundada.
Plazo de conservación	Conforme al Catálogo de Disposición Documental: Durante la permanencia del alumno en el taller o selección y hasta 2 años posteriores a su egreso o baja en Archivo de Trámite.
Transferencias o remisiones	"No aplican remisiones a encargados externos".

En la Universidad Tecnológica de la Selva se efectúa el tratamiento de datos personales a través de 14 unidades y departamentos administrativos, articulando un total de 41 procesos o tratamientos específicos. En estos procesos intervienen servidores públicos autorizados en el manejo de la información conforme a sus atribuciones normativas.



Consolidado de Tratamientos por Área Administrativa

Unidad Administrativa / Departamento	Número de Procesos / Tratamientos	Porcentaje respecto al total(%)
Abogado General (incluye Transparencia, Género y Archivo)	4	9.76%
Secretaría Académica (incluye Direcciones de División)	14	34.15%
Departamento de Servicios Escolares	2	4.88%
Departamento de Servicios Bibliotecarios	1	2.44%
Departamento de Servicios Estudiantiles	1	2.44%
Dirección de Vinculación	5	12.20%
Dirección de Planeación y Evaluación	1	2.44%
Subdirección de Informática Administrativa y Recursos Humanos	3	7.32%
Subdirección de Servicios Administrativos y Recursos Materiales	3	7.32%
Subdirección de TI, Comunicación y Redes	2	4.88%
Departamento de Contabilidad	1	2.44%
Departamento de Sistema de Gestión de la Calidad	2	4.88%
Departamento de Prensa y Difusión	1	2.44%
Departamento de Cultura y Deporte	1	2.44%
TOTAL	41	100.00%





Distribución por tipología de datos personales tratados

Respecto a la tipología de los datos tratados en los 41 procesos institucionales:

- **Datos de Identificación y Contacto:** Presentes en el 100% (41 procesos) de los tratamientos.
- **Datos Patrimoniales y Financieros:** Utilizados en 6 procesos (14.63%), correspondientes a nómina, viáticos, contratación de proveedores y becas.
- **Datos Sensibles:** Utilizados en 4 procesos (9.76%), pertenecientes a las áreas de atención a quejas de género, servicios médicos/psicológicos y fichas médicas deportivas.

Tipología de Datos	Número de Procesos	Porcentaje (%)	Descripción / Áreas
Datos de Identificación y Contacto	41	100.00 %	Presentes en la totalidad de los tratamientos institucionales.
Datos Patrimoniales y Financieros	6	14.63 %	Nómina, viáticos, contratación de proveedores y becas.
Datos Sensibles	4	9.76 %	Atención a quejas de género, servicios médicos/psicológicos y fichas médicas deportivas.

6.- Funciones y obligaciones de las personas que tratan datos personales.

Como resultado de la identificación de los procesos en los que intervienen datos personales, relacionado en el Inventario de Datos Personales, por las áreas que integran las unidades administrativas correspondientes al interior de la Universidad, resulta importante definir estas actividades con las funciones y facultades establecidas en la normatividad interna, que otorga a las personas servidoras públicas responsables de dicho tratamiento; lo anterior, a fin de dar cumplimiento al principio de legalidad que debe atender todo servidor público.

Por lo anterior, a continuación, se ilustran las funciones en esta Universidad de quienes llevan a cabo tratamientos de datos personales:

Órgano administrativo	Nombre y cargo de la persona servidora pública que tratan los datos personales.	Proceso o tratamiento
Abogado General	Erika Estrada Gutiérrez/ Abogada General	• Atención a solicitudes de acceso a la información. • Solicitudes de derechos ARCOP.



		• Quejas y denuncias por violencia de género o hostigamiento. • Gestión y resguardo del archivo de concentración institucional.
Secretaría académica	Jesús Domínguez Gutiérrez/ Secretario Académico	• Comisiones para docentes y administrativos. • Informes internos y externos. • Permisos para docentes y administrativos.
División agroalimentaria	José Elías Penagos Solórzano/ Encargado de la División de Agroalimentaria	• Asesorías. • Carga horaria. • Estadías. • Comisiones para docentes y administrativos. • Grupos de WhatsApp. • Horario de docentes y grupos. • Informes internos y externos. • Lista de asistencia. • Permiso de alumno. • Permiso de docentes y administrativos. • Tutorías.
División de administración	Jandi Elizabeth Albores Gonzales/ Directora de la División de Administración	• Asesorías. • Carga horaria. • Estadías. • Comisiones para docentes y administrativos. • Grupos de WhatsApp. • Horario de docentes y grupos. • Informes internos y externos. • Lista de asistencia. • Permiso de alumno. • Permiso de docentes y administrativos. • Tutorías.
División de tecnologías de la información	Emmanuel Gordillo Espinoza/ Director de la División de Tecnologías de la Información	• Asesorías. • Carga horaria. • Estadías. • Comisiones para docentes y administrativos. • Grupos de WhatsApp. • Horario de docentes y grupos. • Informes internos y externos. • Lista de asistencia. • Permiso de alumno. • Permiso de docentes y administrativos. • Tutorías.
División de turismo y gastronomía	Harvins A. Burguete Trejo/ Encargado de la División de Turismo y Gastronomía	• Asesorías. • Carga horaria. • Estadías. • Comisiones para docentes y administrativos.





		• Grupos de WhatsApp. • Horario de docentes y grupos. • Informes internos y externos. • Lista de asistencia. • Permiso de alumno. • Permiso de docentes y administrativos. • Tutorías.
División de construcción	Omar Eleuterio Pérez Aguilar / Encargado de la División de Construcción.	• Asesorías. • Carga horaria. • Estadías. • Comisiones para docentes y administrativos. • Grupos de WhatsApp. • Horario de docentes y grupos. • Informes internos y externos. • Lista de asistencia. • Permiso de alumno. • Permiso de docentes y administrativos. • Tutorías.
Departamento de servicios escolares	Arturo Paniagua Sesma / Jefe del Departamento de Servicios Escolares	• Registro y control escolar (inscripción y reinscripción). • Titulación y afiliación al IMSS.
Departamento de servicios bibliotecarios	Carlos Gerardo Morales Olivera / Jefe del Departamento de Servicios Bibliotecarios	• Acceso sistematizado (SISTGEBI) registro de usuarios y préstamo de acervo bibliográfico.
Departamento de servicios estudiantiles	Arisbel Kanter Torres / Jefa de Departamento de Servicios Estudiantiles	• Servicios de pedagogía, psicología y enfermería.
Dirección de vinculación	Horacio Albores Ortiz / Director de Vinculación	• Becas. • Consejo de vinculación. • Convenios. • Estancias y estadíos. • Movilidad nacional e internacional.
Dirección de planeación y evaluación.	Juan Moisés Gómez Pérez / Encargado de la Dirección de Planeación y Evaluación	• Cédulas presupuestales.
Subdirección de informática administrativa y recursos humanos	Daniel Alejandro Hernández Gómez / Subdirector de informática administrativa y recursos humanos	• Nómina del personal. • Registro y control de asistencia del personal. • Sistemas de videovigilancia (CCTV)
Subdirección de servicios administrativos	Lath Manuel Ovando Mota / Subdirector de Servicios Administrativos	• Licitación.
Jefatura de recursos materiales y servicios generales	Roxana Leodeni Luna Domínguez / Jefe de Departamento de Recursos Materiales	• Pago a proveedores. • Contratación de bienes y/o servicios.
Subdirección de tecnologías de la información, comunicación y redes	Miguel Ángel Trujillo Feliciano / Encargado de la Subdirección de Tecnologías de la Información, Comunicación y Redes	• Página web institucional. • GECKO GPE (gestor de procesos educativos).
Departamento de contabilidad	Rosa Elena Pulido Aguilar /	• Pago de viáticos.





	Jefe del Departamento de Contabilidad	
Departamento de gestión de la calidad	Luzma Alejandra López Ramirez/ Jefe del Departamento del Sistema de Gestión de la Calidad	- Listas de asistencia. - Procedimientos del sistema de gestión integral.
Departamento de prensa y difusión	Marco Antonio Palacios Ávila/ Jefe del Departamento de Prensa y Difusión	1. Difusión institucional.
Departamento de actividades deportivas y culturales	Juan Carlos Méndez Vidal/ Jefe del Departamento de Actividades Culturales y Deportivas	2. Lista de asistencia.

SECCIÓN CLASIFICADA COMO RESERVADA - APARTADO 7: EVALUACIÓN Y DIAGNÓSTICO DE MEDIDAS DE SEGURIDAD (ANÁLISIS DE RIESGOS de los sistemas de datos personales)

Se testa el apartado número 7 en su totalidad (incluyendo Criterios de Evaluación de Riesgo Inherente, Matriz Institucional de Evaluación de Riesgos por Unidad Administrativa, Análisis de Brecha, Diagnóstico Comparativo de Medidas de Seguridad, Plan de Trabajo Institucional y Mecanismos de Monitoreo), toda vez que contiene información sensible que identifica las vulnerabilidades, debilidades, amenazas, valoraciones numéricas de riesgo y estrategias de corrección del sujeto obligado. Su divulgación pública pondría en riesgo la seguridad de las plataformas informáticas y bases de datos institucionales, facilitando accesos no autorizados, ataques cibernéticos o sustracción de datos personales. Lo anterior de conformidad con lo dispuesto en los artículos 103, fracciones II y III, y 112, fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas; artículos 3, fracción XXV, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas; y los artículos vigésimo sexto y trigésimo octavo de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas.

SECCIÓN CLASIFICADA COMO RESERVADA - APARTADO 7: EVALUACIÓN Y DIAGNÓSTICO DE MEDIDAS DE SEGURIDAD (ANÁLISIS DE RIESGOS de los sistemas de datos personales)

Se testa el apartado número 7 en su totalidad (incluyendo Criterios de Evaluación de Riesgo Inherente, Matriz Institucional de Evaluación de Riesgos por Unidad Administrativa, Análisis de Brecha, Diagnóstico Comparativo de Medidas de Seguridad, Plan de Trabajo Institucional y Mecanismos de Monitoreo), toda vez que contiene información sensible que identifica las vulnerabilidades, debilidades, amenazas, valoraciones numéricas de riesgo y estrategias de corrección del sujeto obligado. Su divulgación pública pondría en riesgo la seguridad de las plataformas informáticas y bases de datos institucionales, facilitando accesos no autorizados, ataques cibernéticos o sustracción de datos personales. Lo anterior de conformidad con lo dispuesto en los artículos 103, fracciones II y III, y 112, fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas; artículos 3, fracción XXV, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas; y los artículos vigésimo sexto y trigésimo octavo de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas.



SECCIÓN CLASIFICADA COMO RESERVADA - APARTADO 7: EVALUACIÓN Y DIAGNÓSTICO DE MEDIDAS DE SEGURIDAD (ANÁLISIS DE RIESGOS de los sistemas de datos personales)

Se testa el apartado número 7 en su totalidad (incluyendo Criterios de Evaluación de Riesgo Inherente, Matriz Institucional de Evaluación de Riesgos por Unidad Administrativa, Análisis de Brecha, Diagnóstico Comparativo de Medidas de Seguridad, Plan de Trabajo Institucional y Mecanismos de Monitoreo), toda vez que contiene información sensible que identifica las vulnerabilidades, debilidades, amenazas, valoraciones numéricas de riesgo y estrategias de corrección del sujeto obligado. Su divulgación pública pondría en riesgo la seguridad de las plataformas informáticas y bases de datos institucionales, facilitando accesos no autorizados, ataques cibernéticos o sustracción de datos personales. Lo anterior de conformidad con lo dispuesto en los artículos 103, fracciones II y III, y 112, fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas; artículos 3, fracción XXV, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas; y los artículos vigésimo sexto y trigésimo octavo de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas.





SECCIÓN CLASIFICADA COMO RESERVADA - APARTADO 7: EVALUACIÓN Y DIAGNÓSTICO DE MEDIDAS DE SEGURIDAD (ANÁLISIS DE RIESGOS de los sistemas de datos personales)

Se testa el apartado número 7 en su totalidad (incluyendo Criterios de Evaluación de Riesgo Inherente, Matriz Institucional de Evaluación de Riesgos por Unidad Administrativa, Análisis de Brecha, Diagnóstico Comparativo de Medidas de Seguridad, Plan de Trabajo Institucional y Mecanismos de Monitoreo), toda vez que contiene información sensible que identifica las vulnerabilidades, debilidades, amenazas, valoraciones numéricas de riesgo y estrategias de corrección del sujeto obligado. Su divulgación pública pondría en riesgo la seguridad de las plataformas informáticas y bases de datos institucionales, facilitando accesos no autorizados, ataques cibernéticos o sustracción de datos personales. Lo anterior de conformidad con lo dispuesto en los artículos 103, fracciones II y III, y 112, fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas; artículos 3, fracción XXV, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas; y los artículos vigésimo sexto y trigésimo octavo de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas.



SECCIÓN CLASIFICADA COMO RESERVADA - APARTADO 7: EVALUACIÓN Y DIAGNÓSTICO DE MEDIDAS DE SEGURIDAD (ANÁLISIS DE RIESGOS de los sistemas de datos personales)

Se testa el apartado número 7 en su totalidad (incluyendo Criterios de Evaluación de Riesgo Inherente, Matriz Institucional de Evaluación de Riesgos por Unidad Administrativa, Análisis de Brecha, Diagnóstico Comparativo de Medidas de Seguridad, Plan de Trabajo Institucional y Mecanismos de Monitoreo), toda vez que contiene información sensible que identifica las vulnerabilidades, debilidades, amenazas, valoraciones numéricas de riesgo y estrategias de corrección del sujeto obligado. Su divulgación pública pondría en riesgo la seguridad de las plataformas informáticas y bases de datos institucionales, facilitando accesos no autorizados, ataques cibernéticos o sustracción de datos personales. Lo anterior de conformidad con lo dispuesto en los artículos 103, fracciones II y III, y 112, fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas; artículos 3, fracción XXV, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas; y los artículos vigésimo sexto y trigésimo octavo de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas.

7.4.3.- Programa interno de capacitación y sensibilización.

Programa permanente enfocado a la profesionalización de las servidoras y servidores públicos de la UTSelva que participan en la recolección, manejo, almacenamiento o transferencia de datos personales.

Objetivo General: Capacitar al 100% del personal administrativo, académico y de soporte en los principios, deberes y medidas de seguridad en materia de datos personales.

Calendario y Contenido Temático Anual:

MÓDULO 1: Principios y Deberes de transparencia conforme a la ley.

- Audiencia: Personal de la UTSelva encargado del manejo de datos personales y encargados de transparencia en las unidades administrativas.
- Duración: 3 Horas (modalidad mixta).
- Periodo: Marzo - Abril.

MÓDULO 2: Avisos de privacidad conforme al tratamiento de datos personales en sus áreas.

- Audiencia: Personal encargado del manejo y trato de datos personales de las unidades administrativas.
- Duración: 3 Horas (modalidad mixta).
- Periodo: Junio - Julio.



MÓDULO 3: Transparencia (llenado y carga de información en la plataforma nacional)

- Audiencia: Personal encargado del manejo y trato de datos personales de las unidades administrativas.
- Duración: 3 Horas (modalidad mixta)
- Periodo: Septiembre - Octubre.

8.- Protocolo para la gestión, registro y notificación de incidencias de seguridad.

8.1.- Objetivo y alcance.

Establecer las acciones obligatorias para la detección, contención, registro, análisis y notificación ante eventuales vulneraciones a la seguridad de los datos personales en custodia de la Universidad Tecnológica de la Selva, conforme a lo establecido en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas.

SECCIÓN CLASIFICADA COMO RESERVADA - APARTADO 8: PROTOCOLO PARA LA GESTIÓN, REGISTRO Y NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD.

Se testa el apartado número 8 en su totalidad (incluyendo Objetivo y alcance, eventos de vulneración considerados, medidas de seguridad físicas y técnicas, política de gestión de accesos e identidades, procedimiento y flujo de notificación sin dilación, formato operativo: bitácora de registro de incidencias de seguridad), toda vez que contiene información sensible que identifica las vulnerabilidades, debilidades, amenazas, valoraciones numéricas de riesgo y estrategias de corrección del sujeto obligado. Su divulgación pública pondría en riesgo la seguridad de las plataformas informáticas y bases de datos institucionales, facilitando accesos no autorizados, ataques cibernéticos o sustracción de datos personales. Lo anterior de conformidad con lo dispuesto en los artículos 103, fracciones II y III, y 112, fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas; artículos 3, fracción XXV, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas; y los artículos vigésimo sexto y trigésimo octavo de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas.





SECCIÓN CLASIFICADA COMO RESERVADA - APARTADO 8: PROTOCOLO PARA LA GESTIÓN, REGISTRO Y NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD.

Se testa el apartado número 8 en su totalidad (incluyendo Objetivo y alcance, eventos de vulneración considerados, medidas de seguridad físicas y técnicas, política de gestión de accesos e identidades, procedimiento y flujo de notificación sin dilación, formato operativo: bitácora de registro de incidencias de seguridad), toda vez que contiene información sensible que identifica las vulnerabilidades, debilidades, amenazas, valoraciones numéricas de riesgo y estrategias de corrección del sujeto obligado. Su divulgación pública pondría en riesgo la seguridad de las plataformas informáticas y bases de datos institucionales, facilitando accesos no autorizados, ataques cibernéticos o sustracción de datos personales. Lo anterior de conformidad con lo dispuesto en los artículos 103, fracciones II y III, y 112, fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas; artículos 3, fracción XXV, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas; y los artículos vigésimo sexto y trigésimo octavo de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas.





SECCIÓN CLASIFICADA COMO RESERVADA - APARTADO 8: PROTOCOLO PARA LA GESTIÓN, REGISTRO Y NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD.

Se testa el apartado número 8 en su totalidad (incluyendo Objetivo y alcance, eventos de vulneración considerados, medidas de seguridad físicas y técnicas, política de gestión de accesos e identidades, procedimiento y flujo de notificación sin dilación, formato operativo: bitácora de registro de incidencias de seguridad), toda vez que contiene información sensible que identifica las vulnerabilidades, debilidades, amenazas, valoraciones numéricas de riesgo y estrategias de corrección del sujeto obligado. Su divulgación pública pondría en riesgo la seguridad de las plataformas informáticas y bases de datos institucionales, facilitando accesos no autorizados, ataques cibernéticos o sustracción de datos personales. Lo anterior de conformidad con lo dispuesto en los artículos 103, fracciones II y III, y 112, fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas; artículos 3, fracción XXV, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas; y los artículos vigésimo sexto y trigésimo octavo de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas.



SECCIÓN CLASIFICADA COMO RESERVADA - APARTADO 8: PROTOCOLO PARA LA GESTIÓN, REGISTRO Y NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD.

Se testa el apartado número 8 en su totalidad (incluyendo Objetivo y alcance, eventos de vulneración considerados, medidas de seguridad físicas y técnicas, política de gestión de accesos e identidades, procedimiento y flujo de notificación sin dilación, formato operativo: bitácora de registro de incidencias de seguridad), toda vez que contiene información sensible que identifica las vulnerabilidades, debilidades, amenazas, valoraciones numéricas de riesgo y estrategias de corrección del sujeto obligado. Su divulgación pública pondría en riesgo la seguridad de las plataformas informáticas y bases de datos institucionales, facilitando accesos no autorizados, ataques cibernéticos o sustracción de datos personales. Lo anterior de conformidad con lo dispuesto en los artículos 103, fracciones II y III, y 112, fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas; artículos 3, fracción XXV, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas; y los artículos vigésimo sexto y trigésimo octavo de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas.

9.- Mecanismos de revisión, monitoreo y actualización del Documento de Seguridad.

9.1. Criterios y causal de actualización obligatoria.

Con fundamento en lo dispuesto por el Artículo 30 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas (LPDPPSOCHIS) y las directrices emitidas por la Autoridad Garante (Transparencia para el Pueblo de Chiapas), el presente Documento de Seguridad será revisado de forma continua y actualizado de manera obligatoria cuando se presente cualquiera de los siguientes supuestos:

1. **Modificaciones Sustanciales al Tratamiento:** Cuando se adopten nuevas tecnologías, software, plataformas o servicios (incluyendo servicios en la nube) que modifiquen el ciclo de vida o incrementen el nivel de riesgo en los tratamientos de datos personales.
2. **Reestructuración Orgánica:** Cuando ocurran cambios en la estructura organizacional de la Universidad Tecnológica de la Selva que modifiquen la asignación de funciones, atribuciones, unidades administrativas o personal que trata datos personales.
3. **Resultado de Auditorías y Mejora Continua:** Derivado del proceso regular de monitoreo, revisión anual del Sistema de Gestión de Seguridad de los Datos Personales (SGSDP) y del análisis de brecha institucional.



4. Ocurrencia de Vulneraciones a la Seguridad: Posterior a la contención de un incidente o vulneración de seguridad confirmada, como resultado de las acciones correctivas y preventivas implementadas para mitigar su impacto y evitar su reincidencia.

9.2. Periodicidad de revisión ordinaria.

Sin perjuicio de las actualizaciones extraordinarias derivadas de las causales anteriores, el Comité de Transparencia en coordinación con la Unidad de Transparencia/Oficial de Protección de Datos Personales de la Universidad Tecnológica de la Selva llevará a cabo una revisión anual ordinaria del presente Documento de Seguridad durante el último trimestre de cada ejercicio fiscal (mes de noviembre), a efecto de someter su ratificación o actualización formal ante el Comité de Transparencia para su entrada en vigor al inicio del siguiente ciclo institucional.

10. Formalización, dictamen y aprobación normativa.

En cumplimiento a lo establecido en los Artículos 27, 29, 77 y 78 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, el presente Documento de Seguridad de la Universidad Tecnológica de la Selva ha sido integrado, revisado, dictaminado y aprobado de conformidad con la estructura y validación.

DOCUMENTO DE SEGURIDAD	
SISTEMA DE DATOS PERSONALES DE LA UNIVERSIDAD TECNOLÓGICA DE LA SELVA	
Fecha de elaboración del Documento de Seguridad: 29/09/2026	Fecha de última actualización del documento de Seguridad: 29/09/2026
Elaboró: Ender Octavio Arguello Moreno Auxiliar de Transparencia	Aprobó: Erika Estrada Gutiérrez Presidente del Comité de Transparencia, Responsable de la Unidad de Transparencia y Abogada General.