



Educación
Secretaría de Educación Pública



TECNOLÓGICO
NACIONAL DE MÉXICO



Instituto Tecnológico de El Salto
Dirección

Instituto Tecnológico de El Salto

INSTITUTO TECNOLÓGICO DE EL SALTO
TECNOLÓGICO NACIONAL DE MÉXICO

DOCUMENTO OFICIAL

Título: Lineamientos Básicos de Protección de la Información

Código: ITES-PI-01

Versión: 1.0

Fecha de emisión: 2026

Área responsable: Dirección / Subdirección de Planeación y Vinculación / Depto. de Planeación, Programación y Presupuestación / Centro de Cómputo

Tipo de documento: Lineamientos Institucionales

Lineamientos Básicos de Protección de la Información

1. Objetivo

Establecer los lineamientos básicos para la protección de la información del **Instituto Tecnológico de El Salto (ITES)**, con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de la información académica, administrativa y tecnológica, en beneficio de la comunidad estudiantil, docente y administrativa.

2. Alcance

Los presentes lineamientos son de **observancia obligatoria** para:

- Estudiantes
- Personal docente
- Personal administrativo y directivo
- Prestadores de servicio social y prácticas profesionales



2026
año de
**Margarita
Maza**



Calle Tecnológico #101, Colonia La Forestal, C.P. 34942, El Salto, Durango.
Tel. (675) 87 60239 y (675) 87 60783.
e-mail: dir_salto@tecnm.mx www.itelsalto.mx



- Proveedores o terceros con acceso a información institucional

Aplica a toda la información institucional en **formato físico y digital**, así como a los sistemas, plataformas y recursos tecnológicos del Instituto.

3. Marco normativo

El Instituto Tecnológico de El Salto, como institución pública de educación superior adscrita al Tecnológico Nacional de México, se rige por:

- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPSO)
- Lineamientos y disposiciones del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)
- Normatividad aplicable del Tecnológico Nacional de México (TecNM)
- Buenas prácticas en materia de seguridad de la información, tomando como referencia la norma ISO/IEC 27001

4. Clasificación de la información

La información generada, administrada o resguardada por el Instituto se clasifica en:

4.1 Información pública

- Planes y programas de estudio
- Convocatorias
- Reglamentos, normatividad y comunicación institucional

4.2 Información de uso interno

- Procedimientos académicos y administrativos
- Comunicaciones internas entre áreas





4.3 Información confidencial

- Expedientes académicos de estudiantes
- Calificaciones y evaluaciones
- Información laboral del personal

4.4 Información sensible

- Datos personales sensibles, tales como información de salud, datos biométricos y financieros

Cada categoría deberá contar con medidas de protección acordes a su nivel de riesgo.

5. Protección de datos personales

- Recabar únicamente los datos personales necesarios para el cumplimiento de fines institucionales.
 - Contar con Aviso de Privacidad vigente y accesible.
 - Garantizar el ejercicio de los derechos ARCO.
 - Evitar la divulgación, transferencia o uso indebido de datos personales sin consentimiento o fundamento legal.
-

6. Control de acceso a la información

- Asignar accesos a sistemas y archivos conforme a las funciones y responsabilidades del usuario.
 - Aplicar el principio de mínimo privilegio.
 - Utilizar contraseñas seguras, personales e intransferibles.
 - Revocar accesos cuando el usuario cause baja o cambie de funciones.
-





7. Seguridad de sistemas y plataformas

- Proteger los sistemas de control escolar, plataformas educativas y administrativas.
- Mantener actualizados los sistemas, aplicaciones y equipos.
- Registrar accesos y modificaciones relevantes mediante bitácoras.
- Realizar respaldos periódicos de la información crítica.

8. Uso responsable de los recursos tecnológicos

- Utilizar el equipo de cómputo, red y sistemas institucionales exclusivamente para fines académicos y administrativos.
- Prohibir la instalación de software no autorizado.
- Regular el uso de dispositivos personales conectados a la red institucional.

9. Seguridad física de la información

- Restringir el acceso a centros de cómputo, servidores y archivos físicos.
- Resguardar adecuadamente documentos impresos con información confidencial.
- Destruir de forma segura la información obsoleta.

10. Concientización y capacitación

- Fomentar la cultura institucional de protección de la información.
- Capacitar periódicamente a estudiantes y personal en materia de seguridad de la información y protección de datos personales.





11. Gestión de incidentes de seguridad

- Reportar de inmediato cualquier incidente que comprometa la información institucional.
- Atender, documentar y dar seguimiento a los incidentes conforme a los procedimientos internos.
- Implementar acciones correctivas y preventivas.

12. Responsabilidades

- Designar a un Responsable de Protección de Datos Personales.
- Supervisar el cumplimiento de los presentes lineamientos.
- Aplicar las medidas administrativas correspondientes en caso de incumplimiento.

13. Vigencia

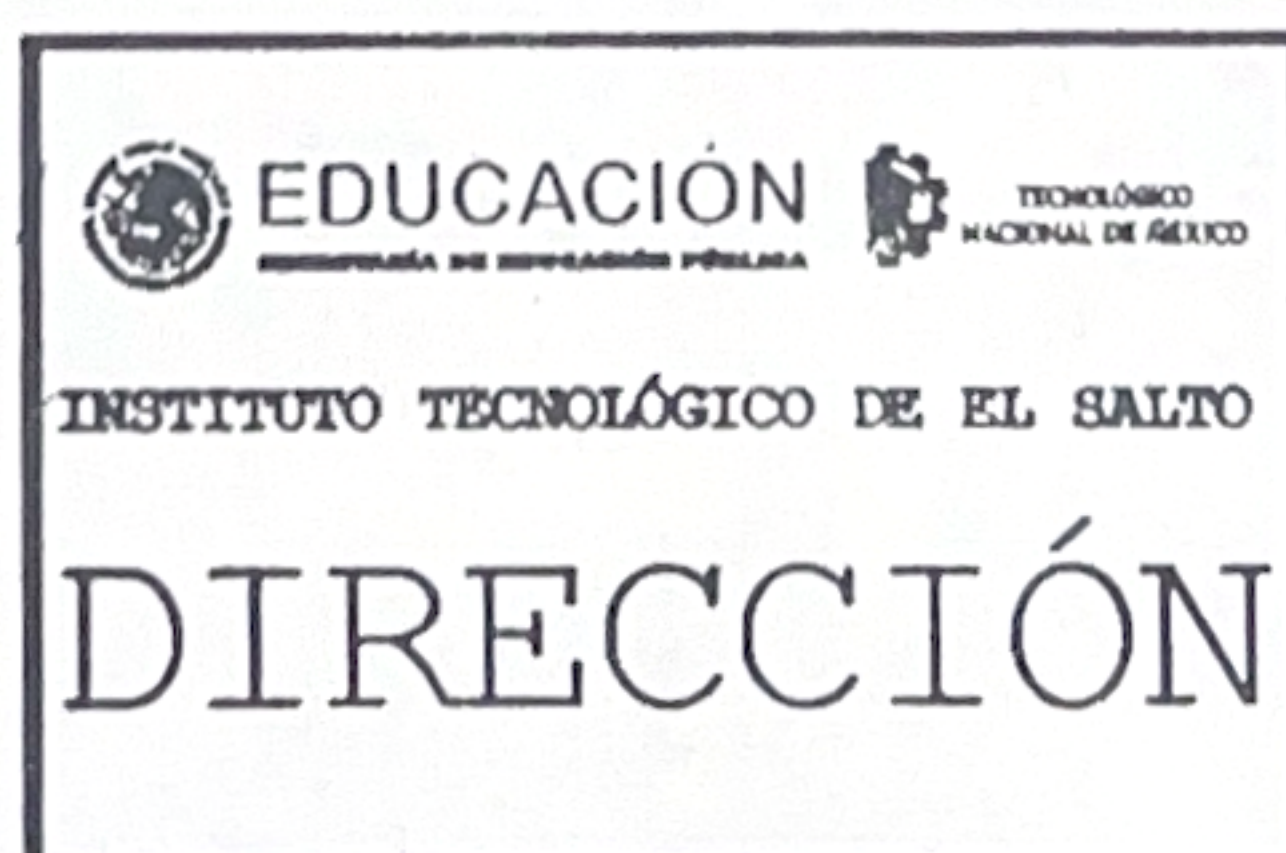
Los presentes lineamientos entrarán en vigor a partir de su **aprobación oficial** por la autoridad competente del Instituto Tecnológico de El Salto y permanecerán vigentes hasta su actualización o sustitución.

Instituto Tecnológico de El Salto
Documento oficial de observancia obligatoria.

ATENTAMENTE

Excelencia en Educación Tecnológica®
"La mejor opción para servir a México"

DAVID MALDONADO AYALA
DIRECTOR



2026
año de
**Margarita
Maza**

