DOCUMENTO DE SEGURIDAD
Políticas de Seguridad de la Información del Instituto Tecnológico Superior de Tierra Blanca

Disposiciones Generales.

La presente política tiene por objeto, acordar y divulgar los estándares, procedimientos, medidas de seguridad de carácter administrativos, físicos y técnicos, y los niveles de seguridad que se aplican para la seguridad de los Datos Personales en el Instituto Tecnológico Superior de Tierra Blanca, en los sucesivo Instituto así como los mecanismos y medidas de control que deberá emplear cada servidor público del Instituto que sean los responsable de la Administración de los Datos Personales, de conformidad con las presentes Políticas y las normas establecidas para el efecto.

La presente Política es general y obligatoria para las Unidades y Áreas Administrativas del Instituto y los servidores públicos adscritos a la misma, para establecer los procedimientos institucionales y responsabilidades de los servidores públicos, a efecto de garantizar el derecho de acceso a la información pública que posee el Instituto de conformidad con la Ley General de Transparencia y Acceso a la Información Pública, Ley 250 de Transparencia y Acceso a la Información Pública para el Estado de Veracruz de Ignacio de la Llave, Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, y Ley 251 de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Veracruz de Ignacio de la Llave y demás disposiciones legales y normativas aplicables.

La presente Política y sus anexos, son un instrumento necesario para establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

El Instituto, reconoce el derecho del usuario a la privacidad y seguridad por lo que establece la política general de seguridad de la información para la protección de los mismos.

Si surgiera la necesidad de intervenir la privacidad de alguna personal durante el curso de alguna investigación de carácter judicial y por el uso inapropiado de los activos de la información, el Instituto, deberá cumplir con los procedimientos legales vigentes para hacerlo.

Para los efectos legales de la presente política se entiende por:

Confidencialidad: Es la garantía de que la información personal será protegida para que no sea divulgada sin consentimiento de la persona.

Integridad: Consiste en el mantenimiento de la exactitud y completitud de la información y sus métodos de procesos.

Disponibilidad: Consiste en que la información se encuentre accesible y disponible cuando los requiera una entidad, proceso o persona autorizada.

Ámbito de aplicación y obligatoriedad

El presente documento será de aplicación obligatoria a las y los servidores públicos del Instituto responsables de la Administración de los datos de carácter personal, así como a las personas externas cuyos servicios contratados por el Instituto, estén relacionados con el uso de datos.

Así mismo, a las personas que deberán aplicar las políticas, estándares, procedimientos y controles de accesos administrativos, físicos y técnicos que se detallan en este documento:

a. Las personas responsables, encargadas y usuarias de los Datos Personales en el Instituto;
b. El Comité de Transparencia del Instituto.
c. El jefe del Departamento de Difusión y concertación

Todo el personal del Instituto que tengan acceso a los datos personales, está obligado a conocer y aplicar las medidas de seguridad propias en el que se concentren los datos y es aplicable en todas y cada una de las fases del tratamiento de los datos personales, iniciando desde la obtención de los mismos y finalizando con su cancelación de los mismos.

Medidas de seguridad de los Datos Personales.

La seguridad de la información es el conjunto de medidas de control establecidas por el Instituto, para asegurar y mantener la confidencialidad, integridad y disponibilidad de la información, identificado, valorando y gestionando los riesgos en función del impacto que representan para el Instituto, para impedir o evitar su uso, divulgación, sustracción, destrucción, ocultamiento o inutilización indebidos.

La seguridad de la información se clasifica en:
I. Seguridad física. Es la condición que se alcanza aplicando las medidas de control para proteger el entorno físico en el que se encuentran los activos de información; y
II.Seguridad lógica. Es la condición que se logra mediante el establecimiento de medidas de control para el acceso a la información intangible almacenada en medio digital o

Los niveles de seguridad, se identificarán por cada responsable de la Administración de los e Datos que contienen son de carácter personal.

El objetivo de la seguridad de la información es salvaguardar la información institucional, así como todos los activos de información implicados en su tratamiento frente a riesgos y amenazas, estableciendo medidas de control para mantener la confidencialidad, integridad y disponibilidad de la misma.

Medidas de seguridad: conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permiten garantizar la protección, confidencialidad, disponibilidad e integridad de los datos personales;

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

Medidas de seguridad físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se debe considerar las siguientes actividades:

- Prevenir el acceso no autorizado en las instalaciones físicas, recursos e información;
- Prevenir el daño o interferencia a las instalaciones físicas, recursos e información.
- Proteger las computadoras de escritorio o portátiles y cualquier soporte físico o electrónico, que pueda salir fuera de las instalaciones de la organización; y
- Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz que asegure su disponibilidad, funcionalidad e integridad.

Medidas de seguridad técnicas: Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y recursos involucrados en su tratamiento.
De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

- Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;
- Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
- Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware; y

- Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales

Aunado a lo anterior, para determinar el nivel de riesgo se considera el criterio del riesgo inherente del dato personal, así como el nivel se seguridad requerido para éste, en adición a las vulnerabilidades y amenazas, de acuerdo con las categorías o tipos de datos personales que se detallan a continuación:

CRITERIOS DEL NIVEL DE RIESGO	
Riesgo Inherente Básico	Nivel de Seguridad Básico
Riesgo Inherente Medio	Nivel de Seguridad Medio
Riesgo Inherente Alto	Nivel de Seguridad Alto

Los niveles de seguridad responden a la mayor o menor necesidad de garantizar la integridad de los datos personales. Por lo tanto, las Unidades o Áreas Administrativas y sus responsables aplicarán el nivel básico, medio o alto de medidas de seguridad.

Las medidas de seguridad marcadas con nivel básico serán aplicables a todos los Datos Personales y es obligatoria.

Se considerarán aplicables las medidas de seguridad de **NIVEL BÁSICO** a Datos Personales que contengan algunos datos que enseguida se mencionan:

IDENTIFICACIÓN: Nombre, domicilio, correo electrónico, número de teléfono; RFC, CURP, estado civil, firma, firma electrónica, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes, beneficiarios, fotografía, idioma o lengua, entre otros.

Los Datos Personales que contengan alguno de los datos que se enlistan a continuación, además de cumplir con las medidas de seguridad de nivel básico deberán observar las marcadas con **NIVEL MEDIO.**

DATOS PATRIMONIALES: Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados, referencias personales, entre otros.

DATOS SOBRE PROCEDIMIENTOS ADMINISTRATIVOS SEGUIDOS EN FORMA DE JUICIO Y/O JURISDICCIONALES: Información relativa a una persona que se

encuentre sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal o administrativa.

DATOS ACADÉMICOS: Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros.
DATOS DE TRÁNSITO Y MOVIMIENTOS MIGRATORIOS: Información relativa al tránsito de las personas dentro y fuera del país e información migratoria de las personas, entre otros.
Los Datos Personales que contengan alguno de los dato personal sensibles que se enlistan a continuación, además de cumplir con las medidas de seguridad de nivel básico y medio, deberán tomar las marcadas con **NIVEL ALTO**.
DATOS IDEOLÓGICOS: Creencia religiosa, ideológica, afiliación, política y/o sindical, pertenencia a organizaciones de la sociedad civil y/o asociaciones religiosas, entre otros.
DATOS DE SALUD: Estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos, prótesis, entre otros.
CARACTERÍSTICAS PERSONALES: Tipo de sangre, ADN, huella digital, u otros análogos.
CARACTERÍSTICAS FÍSICAS: Color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros.
VIDA SEXUAL: Preferencia sexual, hábitos sexuales, entre otros.

Cada Unidad o Área Administrativa designará un servidor público responsable de Datos Personales y será el encargado de apoyar a la persona Titular o encargada de la Unidad o Área Administrativa de su adscripción y tendrá las siguientes funciones:

a) Adoptar las medidas de seguridad para el resguardo de Datos Personales bajo su responsabilidad, en soporte físico, de manera que se evite su alteración, pérdida o acceso no autorizado;
b) Autorizar expresamente, en los casos en que no esté previsto por un instrumento jurídico o disposición normativa, a los usuarios, y llevar una relación actualizada de las personas que tengan acceso los Datos Personales que se encuentran en soporte físico, y
c) Aplicar y vigilar el cumplimiento de las medidas de seguridad para la conservación y resguardo de los Datos Personales del Instituto, que para tal efecto determine el Comité, a través de la aprobación de disposiciones normativas específicas de observancia general para las Unidades o Áreas Administrativas que cuenten con los resguardos de datos personales.

Corresponderá a la persona Titular o encargada de la Unidad o Área Administrativa responsable establecer controles o mecanismos que tengan por objeto que todas aquellas personas que intervengan en cualquier fase del tratamiento de los datos personales, guarden

confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar su relación con el mismo.

Como son las siguientes obligaciones generales:
a) Guardar la debida secrecía sobre los datos personales que conozcan en el desarrollo de sus funciones, evitando su difusión y/o transmisión.
b) Informar al responsable de Seguridad sobre cualquier incidencia que tenga conocimiento.
c) No dejar información visible cuando abandone su puesto, ya sea que se ausente de manera temporal o si hay alguna persona ajena a la Unidad Administrativa a la que esté adscrito.
d) Conservar el buen estado físico de los soportes documentales a que tengan acceso, por motivo del ejercicio de sus funciones.
e) Reportar alguna vulneración de los datos personales

Otras de las actividades que realizarán los responsables de seguridad de los Datos Personales serán:

- Crear políticas internas para la gestión y tratamiento de los datos personales, el ciclo de vida de los Datos Personales (obtención, uso y supresión).
- Definir las funciones y obligaciones del personal involucrado.
- Elaborar el inventario de Datos Personales.
- Realizar el análisis de riesgo considerando las amenazas y vulnerabilidades existentes,
- Control de accesos
- Copias de respaldo
- Realizar el análisis de brecha,
- Elaborar un plan de trabajo,
- Implementar las medidas de seguridad faltantes,
- Revisar de manera periódica las medidas de seguridad implementadas.
- Diseñar y aplicar capacitaciones del personal bajo su mando, dependiendo de sus roles y responsabilidades.

PLAN DE CAPACITACIÓN

Para los programas de capacitación, el responsable deberá tomar en cuenta lo siguiente:

- Los requerimientos y actualizaciones del sistema de gestión;
- La legislación vigente en materia de protección de datos personales y las mejores prácticas relacionadas con el tratamiento de estos;
- Las consecuencias del incumplimiento de los requerimientos legales o requisitos organizacionales; y
- Las herramientas tecnológicas relacionadas o utilizadas para el tratamiento de los datos personales y para la implementación de las medidas de seguridad.

Calendario programático para llevar a cabo:

- Capacitaciones integrales del personal que resguarda los datos personales;
- Actualizaciones;
- Fechas y duración de la capacitación;
- Áreas a capacitar;
- Temas;
- Mejoras implementadas;
- Desaciertos y aciertos;
- Oportunidades de mejora;

Sanciones

Los servidores públicos que incumplan en alguna de las disposiciones contenidas en esta Política, incurrirán en la probable comisión u omisión de alguna falta de responsabilidad administrativa, y serán sancionados de acuerdo a sus atribuciones por los Órganos Internos de Control o la autoridad competente.

Av. Veracruz s/n esq. Héroes de Puebla, Col. PEMEX
Tierra Blanca, Ver. C.P. 95180 Tels. 2747434992 Ext. 222
e-mail: uaip@itstb.edu.mx www.itstb.edu.mx