Secretaría de Educación
Gobierno de Puebla

Políticas para la Seguridad de lasTecnologías de la Información.

APROBACIONES

Elaborado por:	Revisado Por:	Aprobado por:
JORGE ARROYO LÓPEZ INFORMÁTICA Y EDUCACIÓN A DISTANCIA	MIGUEL ÁNGEL SÁNCHEZ POLO DIRECTOR DE PLANEACIÓN Y EVALUACIÓN	MIGUEL ÁNGEL SÁNCHEZ POLO DIRECTOR DE PLANEACIÓN Y EVALUACIÓN
Firma	Firma	Firma

HISTORIAL DE REVISIONES

Versión	Fecha	Revisión
1.0	Mayo 2023	Versión inicial

INTRODUCCIÓN

La Seguridad de tecnologías de la información, es una función en la que se deben evaluar y administrar los riesgos dentro de la Universidad Tecnológica de Xicotepec de Juárez basándose en políticas que cubran las necesidades la universidad en materia de seguridad informática, por lo cual el Departemanto de Informática y Educación a Distancia presenta este documento donde se encuentra estructurado en 3 políticas generales de seguridad para el personal de la universidad, con sus respectivos estándares que consideran los siguientes puntos:

1.-Seguridad de Personal
2.-Seguridad Física y Ambiental
3.-Seguridad y Administración de Operaciones de Cómputo
4.-Cumplimiento de la seguridad informatica

OBJETIVO

El presente documento tiene como finalidad dar a conocer las políticas para la seguridad informática que deberán aplicar el personal que labora en la universidad en cuanto a servicios de tecnologías de información, para proteger adecuadamente los activos tecnológicos y la información de la Universidad Tecnológica de Xicotepec de Juárez.

ALCANCE

Este documento describe las políticas de seguridad de tecnologías de la información, que deberán acatar de forma obligatoria todos los usuarios que pertenecen a la universidad tecnológica de Xicotepec de Juárez, para el buen uso del equipo de cómputo, aplicaciones de software y servicios de tecnologías de la información que se tienen.

JUSTIFICACIÓN

El Departemanto de Informática y Educación a Distancia esta capacitado de acuerdo a sus funciones a definir y establecer normas y procedimientos para el uso adecuado, manejo y conservación del equipo de cómputo y telecomunicaciones.

DEFINICIONES

Abreviatura	Definición
Politicas	Politicas para la seguridad informática
Usuario (S)	Servidores que se encuentren trabajando en la Universidad Tecnologica de Xicotepec de Juarez

SANCIONES POR INCUMPLIMIENTO

El incumplimiento a las presentes políticas podrá presumirse como causa de responsabilidad administrativa y/o penal, dependiendo de su naturaleza y gravedad, cuya sanción será aplicada por las autoridades competentes.

1.-Amonestación privada o pública.
2.-Suspensión del empleo, cargo o comisión por un período no menor de tres días ni mayor a un año.
3.-Destitución del puesto.
4.-Sanción económica.
5.-Inhabilitación temporal para desempeñar empleos, cargos o comisiones en el servicio público.

BENEFICIOS

Las políticas establecidas dentro de este documento son la base para el uso correcto y la protección de los activos tecnológicos e información de la Universidad Tecnológica de Xicotepec de Juarez.

1. SEGURIDAD DE PERSONAL

POLÍTICA

Todo usuario de bienes y servicios informáticos se compromete a conducirse bajo los principios de confidencialidad de la información y de su uso adecuado de los recursos informáticos de la Universidad Tecnológica de Xicotepec de Juárez.
Los usuarios deberán cumplir con lo señalado en estas Políticas las cuales fueron diseñadas para observancia y aplicación dentro de las instalaciones de la universidad.

OBLIGACIONES DE LOS USUARIOS

Es responsabilidad de los usuarios de bienes y servicios informáticos cumplir con las presentes Políticas para la Seguridad de las tecnologías de la información establecidas para el buen funcionamiento en materia tecnológica.

ACUERDOS DE USO Y CONFIDENCIALIDAD

Todos los usuarios de bienes y servicios informáticos de la universidad deberán conducirse conforme a los principios de confidencialidad y uso adecuado de los recursos informáticos y de información de la universidad, así como comprometerse a cumplir con lo establecido en las presentes Políticas.

ENTRENAMIENTO EN SEGURIDAD EN LAS TECNOLOGÍAS DE LA INFORMACIÓN

Por medio del Departamento de Personal, en específico en curso de inducción, se solicitará hacer del conocimiento del personal de nuevo ingreso que para conocer las obligaciones para los usuarios y las sanciones que pueden existir en caso de incumplimiento a los servicios informáticos, deberán consultar las Políticas para la Seguridad Informática, a través de este documento.

MEDIDAS DISCIPLINARIAS

Cuando el Departemanto de Informática y Educación a Distancia identifique el incumplimiento a estas Políticas podrá presumirse como causa de responsabilidad administrativa y/o penal, dependiendo de su naturaleza y gravedad, cuya sanción será aplicada por las autoridades competentes.

Se consideran violaciones graves el robo, daño, divulgación de información reservada o confidencial de la universidad, o de que se le declare culpable de un delito informático consideramos entre algunos como:

• Falsificación informática mediante la alteración , o borrado de datos informáticos en documentos oficales de la Universidad Tecnologica de Xicotepec de Juarez.

2. SEGURIDAD FÍSICA Y AMBIENTAL

POLÍTICA

PREVENIR E IMPEDIR ACCESOS NO AUTORIZADOS.

Proteger el equipamiento de procesamiento de información crítica de la universidad ubicándolas en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados. Asimismo, contemplar la protección del mismo en su traslado y permanencia fuera de las áreas protegidas, por motivos de mantenimiento u otros.

Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático que alberga la información de la universidad.

El equipamiento tecnológico estará en una área protegida llamada SITE el cual deberá contener aire acondicionado para evitar un sobrecalentamiento del equipo de computo manteniéndolo a una temperatura adecuada para su correcto funcionamiento.

Implementar medidas para proteger la información manejada por el personal en las oficinas en el marco normal de sus labores habituales.

Adoptar controles adecuados de acceso para minimizar el riesgo de amenazas potenciales, como robos, sustracciones, etc. Por lo que solo personal autorizado del departamento de Informática tendrá acceso a las instalaciones y áreas restringidas de la universidad para salvaguardar algún bien o movimiento dentro del área o la universidad.

El personal autorizado tendrá que registrar su acceso de entrada y salida mediante una bitácora.

Además de la protección de la información y la seguridad de los sistemas, tiene como objeto asegurar la continuidad de la información, que deben actuar coordinadamente evaluando y tratando los riesgos para implementar medidas con el fin de minimizar el impacto ante un incidente de seguridad de la información. Si bien los términos seguridad de la información tienen distintos significados, es necesario que converjan con el fin de proteger la Confidencialidad, Integridad y Disponibilidad de la Información.

RESGUARDO Y PROTECCIÓN DE LA INFORMACIÓN

El personal deberá reportar de forma inmediata al Departemanto de Informática y Educación a Distancia, cuando detecten que existan riesgos reales o potenciales para equipos de cómputo o comunicaciones, como pueden ser fugas de agua, conatos de incendio u otros.

El usuario tiene la obligación de proteger los usb y CDROM que se encuentren bajo su administración, aun cuando no se utilicen y contengan información reservada o confidencial.

Es responsabilidad del usuario evitar en todo momento la fuga de la información de la universidad que se encuentre almacenada en los equipos de cómputo personal que tenga asignados.

Es responsabilidad del usuario el mantener un respaldo actualizado de la información almacenada en el equipo de cómputo asignado.

CONTROLES DE ACCESO FÍSICO

Cualquier persona que tenga acceso a las instalaciones de la universidad, deberá registrar al momento de su entrada, el equipo de cómputo, equipo de comunicaciones, medios de almacenamiento y herramientas que no sean propiedad la universidad, el cual podrán retirar el mismo día. En caso contrario deberá tramitar la autorización de salida correspondiente en caseta de policía, las computadoras personales, las computadoras portátiles, módems, y cualquier activo de tecnología de información, podrá salir de las instalaciones la universidad únicamente con la autorización de salida de caseta de policía.

En caseta de vigilancia deberá haber una bitácora para registrar las características de los equipos que no sean propiedad de la Universidad Tecnologica de Xicotepec de Juarez.

SEGURIDAD EN ÁREAS DE TRABAJO

El centro de cómputo (SITE) que se encuentren es los diferentes edificios de la universidad es área restringida, por lo que sólo el personal autorizado por el Departemanto de Informática y Educación a Distancia puede acceder a él.

PROTECCIÓN Y UBICACIÓN DE LOS EQUIPOS

Los usuarios no deben mover o reubicar los equipos de cómputo o de telecomunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización del Departemanto de Informática y Educación a Distancia.

El equipo de cómputo asignado, deberá ser para uso exclusivo de las funciones asignadas.

Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.

Mientras se opera el equipo de cómputo, no se deberán consumir alimentos o ingerir líquidos.

Se debe evitar colocar objetos encima del equipo o cubrir los orificios de ventilación del monitor o del CPU.

Se debe mantener el equipo informático en un entorno limpio y sin humedad.

El usuario debe asegurarse que los cables de conexión no sean pisados o pinchados al colocar otros objetos encima o contra ellos.

Queda prohibido que el usuario abra o desarme los equipos de cómputo.

MANTENIMIENTO DE EQUIPO

Únicamente el personal autorizado por el Departemanto de Informática y Educación a Distancia podrá llevar a cabo los servicios y reparaciones al equipo informático, por lo que los usuarios deberán solicitar la identificación del personal designado antes de permitir el acceso a sus equipos.

Los usuarios deberán asegurarse de respaldar la información que consideren relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que se encuentre en el equipo, previendo así la pérdida involuntaria de información, derivada del proceso de reparación.

PÉRDIDA DE EQUIPO

El usuario que tenga bajo su resguardo algún equipo de cómputo, será responsable de su uso y custodia; en consecuencia, responderá por dicho bien de acuerdo a la normatividad vigente en los casos de robo, extravío o pérdida del mismo.

El usuario deberá dar aviso inmediato a las áreas de Asuntos Jurídicos y al Departemanto de Informática y Educación a Distancia así mismo levantará un acta del robo o extravío del equipo de cómputo.

USO DE DISPOSITIVOS ESPECIALES

Queda prohibido la instalación de módems, switches, routers externos en las computadoras de escritorio, sin la autorización del Departemanto de Informática y Educación a Distancia.

Si algún área por requerimientos muy específicos del tipo de aplicación o servicio de información tiene la necesidad de contar con uno de ellos, deberá ser justificado y autorizado por el director de Planeación y evaluación de la universidad y por la rectoría.

DAÑO DEL EQUIPO

El equipo de cómputo o cualquier recurso de tecnología de información que sufra alguna descompostura por maltrato, descuido o negligencia por parte del usuario quien resguarda el equipo, deberá cubrir el valor de la reparación o reposición del equipo o accesorio afectado. Para tal caso el Departemanto de Informática y Educación a Distancia determinará la causa de dicha compostura.

3. ADMINISTRACIÓN DE OPERACIONES DE CÓMPUTO

POLÍTICA

Los usuarios deberán utilizar las herramientas que les brinde la universidad para proteger y salvaguardar la información que reside, almacena y utiliza la universidad tecnológica de Xicotepec de Juarez.

Los usuarios que hagan uso de equipo de cómputo, deben conocer y aplicar las medidas para la prevención de código malicioso como pueden ser virus, caballos de Troya o gusanos de red, utilizando las herramientas que la universidad le proporcione tales como antivirus.

USO DE MEDIOS DE ALMACENAMIENTO

Los usuarios deberan usar únicamente el correo institucional, discos duros externos, usb, cd´s, dvd´s oh algún otro tipo de almacenamiento que la universidad les proporcione, por ejemplo almacenamiento en la nube esto para salvaguardar y proteger la información.

Los usuarios deberán respaldar periódicamente la información relevante y crítica que se encuentre en sus equipos de cómputo.

Las actividades que realicen los usuarios en la infraestructura de Tecnologías de Información de la Universidad son registradas y susceptibles de auditoría.

INSTALACIÓN DE SOFTWARE

No se realizará instalación de software institucional a equipos de cómputo personal.

Se considera una falta grave el que los usuarios instalen cualquier tipo de programa (software) en sus computadoras, estaciones de trabajo, servidores, o cualquier equipo conectado a la red de la universidad que no esté autorizado por el Departemanto de Informática y Educación a Distancia.

El equipo de computo institucional solo se le podrá instalar software con licencia, software gratuito o software libre.

ADMINISTRACIÓN DE LA CONFIGURACIÓN

La instalación, administración y configuración del equipo de computo, asi como la infraestructura del equipo de telecomunicaciones queda extrictamente a cargo por el Departemanto de Informática y Educación a Distancia.

SEGURIDAD PARA LA RED

Será considerado como un ataque a la Seguridad en la red y una falta grave, cualquier actividad no autorizada por el Departemanto de Informática y Educación a Distancia, en la cual los usuarios realicen la exploración de los recursos informáticos en la red del Instituto, así como de las aplicaciones que sobre dicha red operan, con fines de detectar y explotar una posible vulnerabilidad.

USO DEL CORREO ELECTRÓNICO

El servicio de correo electrónico institucional, es un servicio gratuito, y no garantizable, se debe hacer uso de él, acatando todas las disposiciones de seguridad diseñadas para su utilización y evitar el uso o introducción de software malicioso a la red institucional.

Los usuarios no deben usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas de otros. Si fuera necesario leer el correo de alguien más (mientras esta persona se encuentre fuera o de vacaciones) el usuario ausente debe re direccionar el correo a otra cuenta de correo interno, quedando prohibido hacerlo a una dirección de correo electrónico externa al Instituto, a menos que cuente con la autorización de la dirección de adscripción.

Los usuarios deberán saber que la información de los correos electrónicos y archivos adjuntos son propiedad de la Universidad Tecnológica de Xicotepec de Juárez, los usuarios podrán enviar información reservada y/o confidencial vía correo electrónico siempre y cuando, de ser posible de manera codificada y destinada exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y atribuciones.

El usuario debe de utilizar el correo electrónico de la Universidad única y exclusivamente a los recursos que tenga asignados y las facultades que les hayan sido atribuidas para el desempeño de su empleo, cargo o comisión, quedando prohibido cualquier otro uso.

La asignación de una cuenta de correo electrónico, deberá solicitarse por escrito al Departemanto de Informática y Educación a Distancia, señalando los motivos por los que se desea el servicio, así como sus datos personales y el área adscrita que lo solicita. Esta solicitud deberá contar con el visto bueno del jefe inmediato del área que corresponda.

Queda prohibido suprimir o sustituir la identidad de un usuario de correo electrónico, así como interceptar, revelar o ayudar a terceros a interceptar o revelar las comunicaciones electrónicas.

El usuario deberá cuidar en todo momento la utilización de un lenguaje apropiado, evitando palabras ofensivas o altisonantes.

Todo uso indebido del servicio de correo electrónico, será motivo de suspensión temporal de su cuenta de correo o según sea necesario la eliminación total de la cuenta dentro del sistema.

CONTROLES CONTRA CÓDIGO MALICIOSO

Para prevenir infecciones por virus informático, los usuarios del Instituto no deben hacer uso de cualquier clase de software que no haya sido proporcionado y validado por el Departemanto de Informática y Educación a Distancia.

Todos los archivos de computadora que sean proporcionados por personal externo o interno considerando al menos programas de software, bases de datos, documentos y hojas de cálculo que tengan que ser descomprimidos, el usuario debe verificar que estén libres de virus utilizando el software antivirus autorizado antes de ejecutarse.

Ningún usuario debe intencionalmente escribir, generar, compilar, copiar, propagar, ejecutar o tratar de introducir código de computadora diseñado para auto replicarse, dañar, o en otros casos impedir el funcionamiento de cualquier memoria de computadora, archivos de sistema, o software. Mucho menos probarlos en cualquiera de los ambientes o plataformas de la universidad. El incumplimiento de este estándar será considerado una falta.

Ningún usuario, empleado o personal externo, podrá bajar o descargar software de sistemas, sin la debida autorización del Departemanto de Informática y Educación a Distancia.

INTERNET

El acceso a Internet provisto a los usuarios es exclusivamente para las actividades relacionadas con las necesidades del puesto y función que desempeña.

La asignación del servicio de Internet, deberá solicitarse por escrito al Departemanto de Informática y Educación a Distancia, señalando los motivos por los que se desea el servicio. Esta solicitud deberá contar con el visto bueno del jefe inmediato del área correspondiente.

Los usuarios del servicio de navegación en Internet, al aceptar el servicio están aceptando que:

- Serán monitoreadas las actividades que realizan en Internet.
- Existe la prohibición al acceso de páginas no autorizadas.
- Existe la prohibición de transmisión de archivos reservados o confidenciales no autorizados.
- Existe la prohibición de descarga de software sin la autorización del Departemanto de Informática y Educación a Distancia.
- La utilización de Internet es para el desempeño de su función y puesto en la universidad y no para propósitos personales.

4. CUMPLIMIENTO DE LA SEGURIDAD INFORMATICA

POLITICA

El Departemanto de Informática y Educación a Distancia tiene como uno de sus objetivos institucionales la de proponer y revisar el cumplimiento de normas y políticas de seguridad, que garanticen acciones preventivas y correctivas para el correcto uso de los equipos e instalaciones de cómputo, así como el correcto uso de la información perteneciente a la universidad.

DERECHOS DE PROPIEDAD INTELECTUAL

Esta prohibido por ley de derechos de autor, realizar copias no autorizadas de software que se adquirido oh desarrollado por la universidad, los usuarios se comprometen a no revelar a terceros el secreto profesional e industrial, la información comercial referente a productos, marcas y patentes de los que tenga o lleguen a tener conocimiento.Misma que se considera como confidencial en términos de lo dispuesto por los artículos 1, 2 fracción V, 3 fracción II, 18 y 29 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados; 36, 37 y 42 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Puebla; 48 y 49 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Puebla y 18, 19 y 20 del Reglamento de la Ley de Transparencia y Acceso a la Información Pública del Estado de Puebla; lo anterior bajo pena de responder de los daños y perjuicios que pudieran ocasionar con independencia de las sanciones civiles o penales en las que pudieran incurrir.

REVISIONES DEL CUMPLIMIENTO

El Departamento de Informatica y Educacion a Distancia se encargara de verificar que los usuarios cumplan y acaten las políticas presentes.

VIOLACIONES DE LAS TECNOLOGIAS DE LA INFORMACION

Está prohibido el uso de herramientas de hardware o software para violar los controles internos de Seguridad en Informática, así como realizar pruebas a los los diferentes entornos de los elementos de Tecnología de Información. Ninguna persona puede probar o intentar comprometer los controles internos.

Ningún usuario debe probar o intentar fallas de la Seguridad de las tecnologias de la información identificadas o conocidas, a menos que estas pruebas sean controladas y aprobadas por el Departemanto de Informática y Educación a Distancia.

No se debe intencionalmente escribir, generar, compilar, copiar, coleccionar, propagar, ejecutar o intentar introducir cualquier tipo de código (programa) conocidos como virus, gusanos o caballos de Troya, diseñado para auto replicarse, dañar o afectar el desempeño o acceso a las computadoras, redes o información de la universidad.