POLÍTICAS ESENCIALES DE SEGURIDAD INFORMÁTICA
INSTITUTO TECNOLÓGICO SUPERIOR DE OCCIDENTE DEL ESTADO DE HIDALGO (ITSOEH)

Presentación

La Dirección General del ITSOEH, reconociendo que los sistemas informáticos y la información que estos resguardan son activos estratégicos para el cumplimiento de la misión educativa, la investigación y la eficiencia administrativa, establece políticas.
Estas políticas definen las medidas de seguridad, los roles y las responsabilidades de toda la comunidad institucional (personal directivo, docentes, administrativo y alumnos) para promover una cultura de seguridad organizacional. El objetivo es garantizar la confiabilidad, integridad y disponibilidad de los recursos informáticos, previniendo amenazas y administrando los riesgos relacionados con la infraestructura, equipos y servicios.

Objetivos

El objetivo principal de estas políticas es:

1. Establecer un marco de trabajo para proteger y administrar los riesgos relacionados con la infraestructura, equipos, información y servicios informáticos del ITSOEH.
2. Promover el buen uso y cuidado de los recursos informáticos y prevenir amenazas y riesgos.
3. Asegurar que las personas usuarias se conduzcan conforme a los principios de legalidad, consentimiento, calidad de datos, confidencialidad, seguridad, disponibilidad, temporalidad y uso de los recursos informáticos.

Justificación

Es indispensable que el ITSOEH cuente con un marco jurídico, flexible y ágil que permita la participación de la comunidad en el cumplimiento de las funciones. La seguridad informática es una necesidad operativa para cualquier organización que maneje activos informáticos.
La aplicación de estas políticas es esencial para proteger los componentes de los sistemas, prevenir amenazas y riesgos y garantizar que la información sensible, reservada y/o confidencial esté resguardada, ya que su divulgación podría causar un perjuicio institucional.

Lineamientos Esenciales de Seguridad

1. Seguridad Informática en la Institución

- **Activos Informáticos:** Se considera Activo Informático a todo recurso informático o relacionado, como equipos de cómputo, servidores, software, impresoras, infraestructura, etc., que son necesarios para el desempeño de las funciones del instituto.
- **Principios de Seguridad:** Se debe garantizar la Confidencialidad (divulgar información solo a personas autorizadas) y la Disponibilidad (asegurar el acceso oportuno a la información y sistemas)
- **Roles y Responsabilidades:** Las políticas definen las medidas, roles y responsabilidades para la gestión de incidentes y el buen uso.

2. Buen Uso de los Activos Informáticos

- **Responsabilidad de Resguardo:** Las personas usuarias son responsables del activo informático o equipo móvil que se les asigne, incluyendo el contenido de la información que este contenga.
- **Movilización:** La movilización de activos informáticos dentro o fuera de las instalaciones es responsabilidad de la persona usuaria resguardante.
- **Restricción de Personal:** Únicamente el personal adscrito al ITSOEH debe ser responsable de los activos informáticos.

3. Clasificación y Resguardo de la Información

- **Protección de la Información:** Toda persona servidora pública es responsable del resguardo de la información para asegurar su integridad y confidencialidad.
- **Uso Aprobado:** El uso de la información debe ser acorde a la función de la persona usuaria.
- **Información Confidencial:** Las personas usuarias deben evitar que la información clasificada como restringida o confidencial sea accedida por personas no autorizadas.

4. Intercambio de Información y Servicios de Terceros

- **Registro de Intercambio:** Al intercambiar información reservada y/o confidencial, se debe dejar registro de la entrega de dicha información.
- **Cláusulas de Confidencialidad:** Todo convenio con terceros para compartir información reservada y/o confidencial debe apegarse a las disposiciones de protección de datos personales e incluir cláusulas de confidencialidad.
- **Monitoreo de Servicios de Terceros:** Todo servicio y/o equipo informático otorgado por terceros debe ser monitoreado y revisado para asegurar el cumplimiento de los términos contractuales.

5. Protección contra Código Malicioso (Malware)

- **Antivirus Obligatorio:** Los equipos de cómputo deben contar con **software antivirus institucional**, además de estar protegidos por el **Firewall.**
- **Reporte Inmediato:** Toda persona que identifique una anomalía o sospecha de **malware** en su equipo debe reportarla de inmediato al área de Soporte Técnico.
- **No Alteración:** Las personas usuarias **no deben alterar o eliminar las configuraciones de seguridad** de programas como antivirus, correo electrónico o navegadores.
-

6. Servicios Informáticos y Uso de Cuentas

- **Uso de Servicios:** Todo el personal del ITSOEH, son responsables del buen uso de los servicios informáticos. La información confidencial solo debe ser almacenada o transmitida dentro de la red interna o hacia redes externas autorizadas.
- **Cuentas Personales y de Área:**
  - Las cuentas de usuario personales, son intransferibles y se permiten para uso exclusivo durante la vigencia de la relación con la institución. Las personas usuarias deben autentificarse con cuentas que permitan identificarlas.
  - Para cada cuenta asignada por área, el jefe inmediato deberá designar a una persona responsable de su uso, quien deberá manejar la información con responsabilidad y mantener la debida confidencialidad
- **Contraseñas Seguras:** Las cuentas deben estar protegidas con contraseñas seguras. Las contraseñas deben ser actualizadas por lo menos dos veces al año.

- **Cancelación de Acceso:** El acceso a servicios y cuentas se **cancelará de manera definitiva** a toda persona que deje de laborar o tener relación con el instituto.

7. Uso de Internet y Correo Electrónico Institucional

- **Uso de Internet:** El servicio de Internet se considera herramienta de trabajo y debe utilizarse exclusivamente para apoyo a las actividades académicas y/o administrativas.
- **Seguridad en Descargas:** Se debe omitir descargar archivos de dudosa procedencia que puedan contener **virus o malware**, ya que pueden poner en riesgo la información del equipo de cómputo y del instituto.
- **Correo Institucional:** Es de uso exclusivo del personal. La cuenta de correo debe utilizarse solo para realizar actividades relacionadas con sus funciones.
- **Responsabilidad del Buzón:** Es responsabilidad del usuario respaldar y depurar constantemente el contenido de su correo electrónico para evitar problemas de saturación.

8. Uso del Software

- **Software Autorizado:** Solo se permite la instalación de software con licenciamiento vigente, ya sea educativo, libre o comercial.
- **Instalación Exclusiva:** El área de soporte técnico del ITSOEH es la única facultada para realizar o asesorar la instalación de software en los laboratorios asignados al área.
- **Falta Grave:** Se considera una falta grave que las personas usuarias instalen cualquier tipo de programa o **software** que **no esté autorizado** en equipos institucionales.

A T E N T A M E N T E
Excelencia en Educación Tecnológica®

ING. IVAN RODRIGUEZ HERNANDEZ
ENCARGADO DE SOPORTE TÉCNICO

VALIDO

MTRO. ÁNGEL HERNÁNDEZ CABRERA
DIRECTOR DE PLANEACIÓN Y VINCULACIÓN

Carretera Mixquiahuala-Tula km. 2.5, Paseo del Agrarismo No. 2000, Mixquiahuala de Juárez, Hgo., C. P. 42700 Tel.: 738 735 4000 | www.itsoeh.edu.mx