Evaluación de riegos a los sistemas informáticos que apoyan el desarrollo de las actividades sustantivas, financieras o administrativas.

La evaluación de riesgos informáticos comprende la identificación de activos y amenazas a los que se encuentran expuestos y poder así evaluar su probabilidad de ocurrencia y el impacto que se generaría, todo esto con el objetivo de poder determinar los controles adecuados para calcular, aceptar, disminuir, transferir o evitar la ocurrencia de riesgo.

1. **Activos de información.**

En este punto se detallarán todos los activos que tienen valor en cuestión de Tecnologías de la Información y Comunicación TIC´s con las que cuenta el Instituto Tlaxcalteca de la Infraestructura Física Educativa, para el desarrollo de las diversas actividades que realizan los empleados.

- Hardware
  - Equipos de cómputo portátiles.
  - Equipos de cómputo de escritorio.
  - Servidor.
  - Impresoras.
- Software
  - Korima SGG.
  - Sistema Automatizado de Administración y Contabilidad Gubernamental.
  - Banca en línea.
  - Licencias de AutoCAD.
  - Licencias de Microsoft Office.
  - Licencias de Microsoft.
  - Licencia de antivirus.
  - Licencias de escáneres Kodak.

2. Vulnerabilidades de los activos.

Son debilidades en configuración de sistemas operativos, fallas de diseño del equipo o en sus componentes.

Activo.	Descripción de las vulnerabilidades.
Hardware	• No mantener actualizado el BIOS. • Fallos lógicos en microprocesador. • Vulnerabilidades en sistema operativo. • Fallas de fabrica en componentes. • Componentes con características bajas. • No mantener actualizado su sistema operativo. • No mantener actualizado su firmware.

Activo.	Descripción de las vulnerabilidades.
Software	• Exposición de información confidencial a un actor no autorizado. • Carga de archivo sin restricción de formato. • Consumo de recursos inadecuados. • Plugin desactualizados. • Sitios de internet fraudulentos, (clones de sitios, banca en línea). • Redirección de URL a un sitio que no es de confianza. • No poder establecer y mantener una conexión con su servidor. • Elevación de privilegios. • Suplantación de identidad. (No originales).

3. Amenazas de los activos

Son todas aquellas acciones que aprovechan las vulnerabilidades para atacar un sistema, robo de información o uso inadecuado de los sistemas ya sean internos o externos.

Activo.	Descripción de amenazas.
Hardware	• Daño por virus, malware, troyanos, ransonware, keyloggers. • Daño por golpe intencional o no intencional. • No tener antivirus optimo y actualizado.

Activo.	Descripción de amenazas.
Software	• Sabotaje o robo de información que genera. • Eliminación de información. • Eliminación de módulos. • Alteración a bases de datos. • Eliminación de información de base de datos. • Asignación de privilegios a usuarios no autorizados. • Borrar carpeta o archivos de instalación del programa. • Ataque por virus, malware, troyanos, ransonware, keyloggers. • Guardar por default credenciales de acceso. • No utilizar licencias originales. • No ingresar las credenciales para el buen funcionamiento del software.