Secretaría de Educación Pública
Gobierno del Estado de Hidalgo

Subsecretaría de Educación Media Superior y Superior
Dirección General de Formación y Superación Docente
Departamento de Educación Normal
Escuela Normal "Sierra Hidalguense"

Estado Libre y Soberano de Hidalgo

LICENCIATURA EN EDUCACIÓN PREESCOLAR

Curso:

Las Tic en la Educación

Trabajo:

"Cuadro de Amenazas Y Soluciones"

Alumnas:

Vianey Abigail Hernández Guzmán

Miriam Guadalupe Cortes Hernández

Yazmin Lizbeth Sánchez Domínguez

Flor Zulidey Pardo Cortes

Ciclo Escolar:

2017 – 2018

Semestre:

Primero

Fecha: 18 septiembre del 2017

TIPOS DE AMENAZAS EN UN EQUIPO DE COMPÚTO

AMENAZA	¿QUE ES?	SOLUCIÓN
VIRUS INFORMÁTICO	Es un programa que se copia automáticamente y que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario.	Es bueno mantenerse protegido con un buen ANTIVIRUS los cuales son los encargados de encontrar estos archivos infectados y eliminarlos de tu computador (solo se encarga de eliminar el archivo infectado pero si es que esta ya había causado daños dentro de su computador, el antivirus en ningún caso podrá o reparar dichos archivos). Ejemplo: ➢ ***Avast!*** ➢ ***Nod32*** ➢ ***Kaspersky*** ➢ ***Bitdefender***
GUSANOS (WORMS)	Es un virus informático que tiene la propiedad de duplicarse a sí mismo. Los gusanos utilizan las partes automáticas de un sistema operativo que generalmente son invisibles al usuario.Un gusano no precisa alterar los archivos de programas, sino que reside en la memoria y se duplica a sí mismo.	Estos se pueden combatir con un ANTIVIRUS actualizado como los ya mencionados anteriormente. A pesar de que un gusano puede causar una molestia enorme, un antivirus actualizado es capas de mantenerte casi en la totalidad de ellos a salvo.
TROYANO	Se le denomina a un programa malicioso capaz de alojarse en computadoras y permitir el acceso a usuarios externos, a través de una red local o de Internet, con el fin de recabar información o controlar remotamente a la máquina	Generalmente los **troyanos** son demasiado difíciles de eliminar debido a que tienen una función de auto-replicarse al momento de ser borrados lo que trae como consecuencia un gran dolor de cabeza, pero como ese no es el caso de todos un buen antivirus ACTUALIZADO podría ser una buena solución para eliminar estas pesadillas.

HACKER	Un **hacker** en la informática es conocido como un usuario ajeno que entra en tu computadora con intenciones de robar información y de causar daño.	La mejor forma de evitarlos es no entrar a paginas de Internet de dudosa procedencia ni tampoco revelar ninguna clase de datos por medios de los cuales usted no confié en su totalidad
ADWARE	Se trata de un programa malicioso que se instala en el computador sin que el usuario lo note, y cuya función es descargar y mostrar anuncios publicitarios en la pantalla de la víctima	El Adware no produce una modificación explícita que dañe el sistema operativo, pero sí disminuye el rendimiento del equipo y de la navegación por la Red ya que utiliza recursos del procesador, la memoria y el ancho de banda. La manera para evitar contagio es proteger su computadora con diversos antivirus que se encargan de cuidar a profundo el procesador de la máquina.
BOTNETS	Es una red de equipos infectados (robot o zombi) por códigos maliciosos, los cuales son controlados por un delincuente informático el cual, de manera remota, envía órdenes a los equipos zombis haciendo uso de sus recursos. Las acciones de un equipo zombi son realizadas en su totalidad de forma transparente al usuario**.**	Uno de los síntomas más importantes de un sistema infectado por un malware de este tipo es el consumo excesivo de recursos, el cual hace lento el funcionamiento del sistema y de las conexiones, e incluso puede llegar a impedir su utilización. Existen diversos antivirus que pueden proteger su computadora.

Rootkit	Son herramientas como programas, archivos, procesos, puertos o cualquier componente lógico diseñadas para mantener en forma encubierta el control de un computador. No es un software maligno en sí mismo, sino que permite ocultar las acciones malignas que se desarrollan en un equipo. Otras amenazas se incorporan y fusionan con técnicas de rootkit para disminuir su probabilidad de ser detectadas.	En la algunos casos los antivirus no son capaces de encontrar los Roofkit sea porque el antivirus no está actualizado o bien el antivirus no lo reconoce como una amenaza, pero para solucionar de la manera más eficaz es con un anti-spyware que son los encargados de eliminar estos problemas de una manera eficaz
Malware	Es el acrónimo, en inglés, de las palabras 'malicious' y 'software', por lo que se conoce como software malicioso. En este grupo se encuentran los virus clásicos (aquellas formas de infección que existen desde hace años) y otras nuevas amenazas que han surgido con el tiempo. Se puede considerar como malware todo programa con algún fin dañino (hay algunos que incluso combinan diferentes características de cada amenaza).	Una mejor forma de poder evitarlos es no entrar a páginas de Internet de ni tampoco revelar ninguna clase de datos por medios de los cuales usted no confié en su totalidad, pero también la mejor forma de combatirlos (quizás la más fácil pero no de confianza) es con otro hacker más capacitado que el anterior (hay que considerar que esta persona debe ser de confianza, de lo contrario el daño podría ser aun peor
Spam	Es el correo electrónico no deseado o correo basura, que se envía sin ser solicitado, de manera masiva, por parte de un tercero. Aunque en un principio se utilizaba para envío de publicidad, se ha visto un creciente uso con el fin de propagar códigos maliciosos. Según estudios, entre el 80 y el 85% del correo electrónico que se le envía a una persona es correo basura	El spam llegaba a la bandeja de entrada inicialmente en mensajes en formato de texto. Sin embargo, con la creación de filtros anti-spam, el spam evolucionó a correos con imágenes o contenido Html para evadir la protección.

SPYWARE	Son aplicaciones que recopilan información del usuario sin su consentimiento. Su objetivo más común es obtener datos sobre los hábitos de navegación o comportamiento en la web del usuario atacado y enviarlos a entes externos. Entre la información recabada se puede encontrar qué sitios web visita, cada cuánto lo hace, cuánto tiempo permanece el usuario en el sitio, qué aplicaciones se ejecutan, qué compras se realizan o qué archivos se descargan.	No es una amenaza que dañe al ordenador, sino que afecta el rendimiento de este y, en este caso, atenta contra la privacidad de los usuarios. Sin embargo, en algunos casos se producen pequeñas alteraciones en la configuración del sistema, especialmente en las configuraciones de Internet o en la página de inicio. Una manera más común es no proporcionar información a este tipo de aplicaciones,
PHISHING	Consiste en el robo de información personal y financiera del usuario, a través de la falsificación de un ente de confianza. El usuario recibe un correo electrónico simulando la identidad de una organización de confianza, por lo que este, al confiar en el remitente, envía sus datos directamente al atacante. Su identificación es compleja pues prácticamente todos los componentes del mensaje enviado al usuario son idénticos a un mensaje legítimo del mismo tipo.	Una manera más común es no proporcionar información a este tipo de robos que pertinentemente aparecen al estar conectados al internet. Esta manera es más eficaz para proteger tus datos personales y bancarios.
VIRUS	Es un programa informático creado para producir algún daño en el computador. Posee dos características particulares: pretende actuar de forma transparente al usuario y tiene la capacidad de reproducirse a sí mismo.	Debido a que los virus son molestos y al mismo tiempo son capaces de destruir e infectar gran parte de tus archivos debes tener protegida tu maquina por algunos antivirus que te ayudaran a mantenerte en cuidado al insertar algunas memorias, etc. Como ejemplo: Avast, Esed nod32, etc.