COMPLEJO EDUCATIVO "SAN BARTOLOMÉ APÓSTOL" **Ilopango/San Salvador** **CODIGO 70026** **Guía de Informática**	
Ing. Blanca Martínez de Ulloa	**Grado: 6° A-B"** **Turno Matutino** **Guía 2 fase 3**

Indicaciones: Transcriba la siguiente información y desarrolle las actividades propuestas.

Si cuenta con acceso a internet, desde su casa, envíe imágenes de la solución de las actividades que se le indican al correo electrónico informatica.cesba@gmail.com (todo el minúscula sin tilde), o subir evidencias por inbox a la página de Facebook Informática Complejo Educativo "San Bartolomé Apóstol" SEMANA DE ENVÍO DE EVIDENCIAS Del 29 junio al 04 de julio

DESARROLLO

SEGURIDAD FÍSICA Y LÓGICA.

SEGURIDAD FÍSICA

Aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información.

AMENAZAS

- Incendios,
- Inundaciones
- Terremotos
- Suministro ininterrumpido de corriente
  - ✓ Estática
  - ✓ Cableados defectuosos
  - ✓ Suministro ininterrumpido de corriente.
  - ✓ Cableado defectuoso.
- Seguridad del equipamiento.

CONTROLES

- Sistemas de alarma.
- Control de persona.
- Barreras infrarrojas-ultrasónicas.
- Control de hardware.
- Controles biométricos.
  - ✓ Huellas digitales
  - ✓ Control de voz
  - ✓ Patrones oculares

- ✓ Verificación de firmas.

SEGURIDAD LÓGICA

Aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo.

Identificación: El usuario se da a conocer al sistema.

Autentificación: Verificación del sistema ante la Identificación.

FORMAS DE AUTENTIFICACIÓN-VERIFICACIÓN.

- ✓ Algo que la persona conoce-Password
- ✓ Algo que la persona es-Huella digital.
- ✓ Algo que la persona hace-Firmar.
- ✓ Algo que la persona posee-Token Card.

AMENAZAS

Elemento que compromete al sistema.

TIPOS DE ATAQUE

A la hora de estudiar los distintos tipos de ataques informáticos, podríamos diferenciar en primer lugar entre los ataques activos, que producen cambios en la información y en la situación de los recursos del sistema, y los ataques pasivos, que se limitan a registrar el uso de los recursos y/o a acceder a la información guardada o transmitida por el sistema.

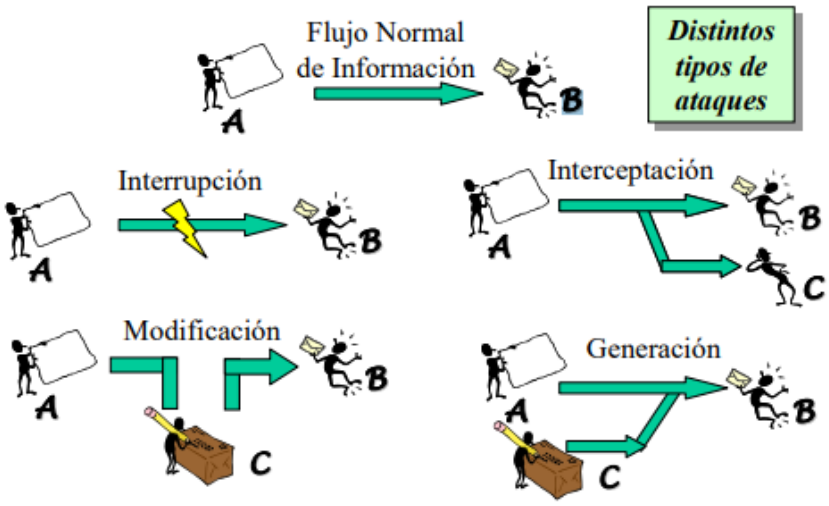


Figura 1: Distintos tipos de ataques en una red de ordenadores

A CONTINUACIÓN, SE ENUMERA ALGUNOS ATAQUES INFORMÁTICOS.

PHISING:

Se trata de un ataque se **suplantación de identidad**. En un correo electrónico el pirata finge ser una entidad legítima como un banco y pide que se acceda a su aplicación web para realizar una determinada gestión como por ejemplo reactivar la cuenta. En el momento que se accede al servicio **el pirata posee todas las claves** de acceso y contraseñas.

DDOS

Un ataque de **Denegación de servicios distribuidos** (DDos) Consiste en bloquear un servicio online generando un inmenso tráfico hacia su sitio. El fin es comprometer a la organización y colapsar los servicios en línea impidiendo el acceso y la publicación de información.

DRIVE-BY DOWNLOAD

El ataque Drive-by-download consiste en la descarga de un programa en el ordenador sin el consentimiento del usuario. El ataque se activa cuando **la víctima hace clic sobre un enlace** y se produce la infestación del ordenador, el malware se denomina troyano.

ATAQUES DE AMENAZA PERSISTENTE (APT)

Un ataque de amenaza persistente consiste en un ataque en el que una persona sin autorización logra el acceso a una red y permanece dentro durante un tiempo. El objeto es **acceder a las credenciales de los usuarios** y recopilar todo tipo de información valiosa para el pirata.

RAMSONWARE

Un ataque de ransomware introduce en el ordenador de la víctima un **software malicioso** que bloquea el acceso, cerrando el sistema o cifrando los archivos importantes en el sistema hasta que se paga una suma de dinero en concepto de rescate.
El ramsonware se ha hecho cada vez más popular entre los piratas informáticos siendo incluso la regla general **exigir los rescates en monedas virtuales como el bitcoin.**

¿QUÉ ES UN VIRUS?

En informática, **un virus de computadora es un programa malicioso desarrollado por programadores que infecta un sistema para realizar alguna acción determinada.** Puede dañar el sistema de archivos, robar o secuestrar información o hacer copias de si mismo e intentar esparcirse a otras computadoras utilizando diversos medios.

El término usado para englobar todos estos códigos es malware, formado por la unión de las palabras malicious y software, es decir, software maléfico. Actualmente, existen muchos *tipos de virus* (malware), con comportamientos característicos que permiten clasificarlos en diferentes categorías.

SINTOMAS

a) Reducción del espacio libre en la memoria disco duro. Un virus, cuando entra en un ordenador, debe situarse obligatoriamente en la memoria RAM, y por ello ocupa una porción de ella. Por tanto, el tamaño útil operativo de la memoria se reduce en la misma cuantía que tiene el código del virus.

1. Aparición de mensajes de error no comunes.
2. Fallos en la ejecución de programas.
3. Frecuentes caídas del sistema
4. Tiempos de carga mayores.
5. Las operaciones rutinarias se realizan con más lentitud.
6. Aparición de programas residentes en memoria desconocidos.

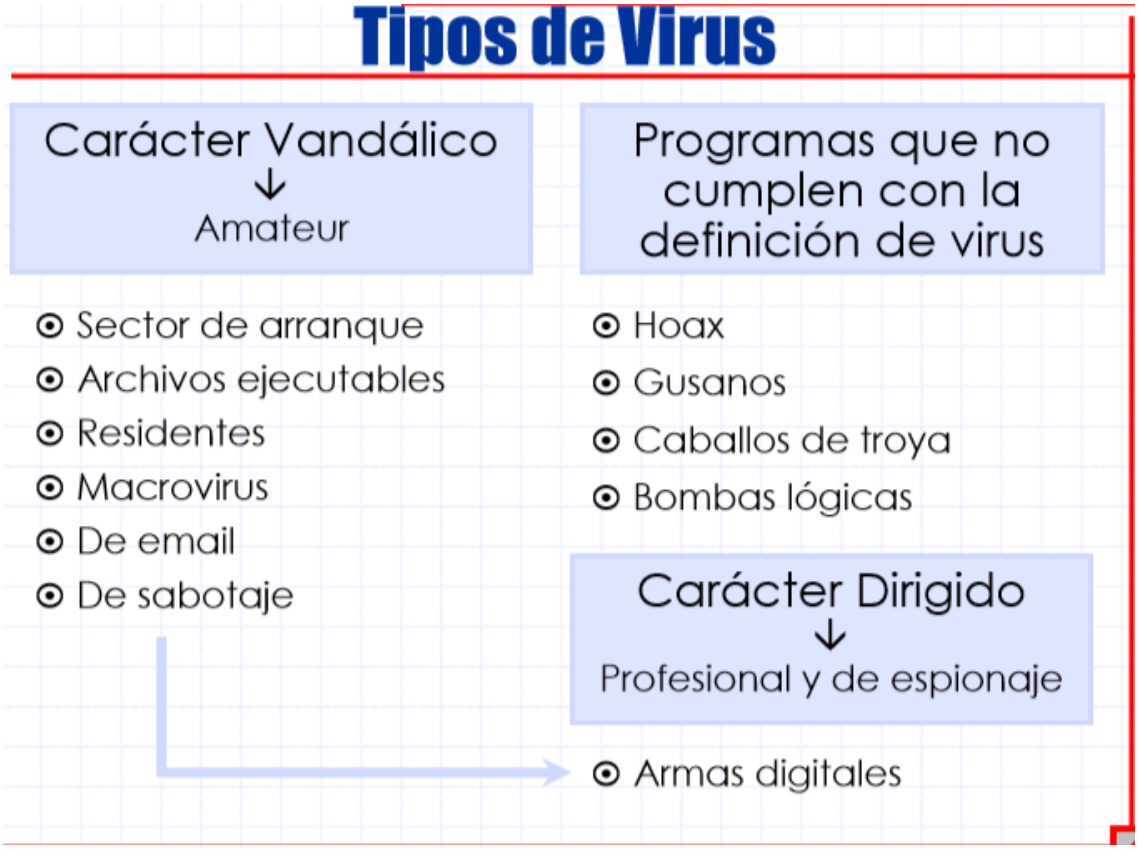
b) Actividad y comportamientos inusuales de la pantalla. Muchos de los virus eligen el sistema de vídeo para notificar al usuario su presencia en el ordenador. Cualquier desajuste de la pantalla, o de los caracteres de esta nos puede notificar la presencia de un virus.

c) El disco duro aparece con sectores en mal estado Algunos virus usan sectores del disco para camuflarse, lo que hace que aparezcan como dañados o inoperativos.

d) Cambios en las características de los ficheros ejecutables Casi todos los virus de fichero, aumentan el tamaño de un fichero ejecutable cuando lo infectan. También puede pasar, si el virus no ha sido programado por un experto, que cambien la fecha del fichero a la fecha de infección.

e) Aparición de anomalías en el teclado. Existen algunos virus que definen ciertas teclas que al ser pulsadas, realizan acciones perniciosas en el ordenador.

También suele ser común el cambio de la configuración de las teclas, por la del país donde se programó el virus.



II PARTE

ACTIVIDAD

1. ¿Cuál son tipos de seguridad informática?
2. ¿Qué tipo seguridad utiliza el password como forma de autentificación y verificación?
3. ¿Qué función tienen los ataques informáticos pasivos?
4. ¿Qué función tienen los ataques informáticos activos?
5. Ataque informático que consiste en la suplantación de identidad.
6. Ataque se activa cuando el usuario (víctima) hace clic sobre un enlace.
7. ¿De la unión de que palabras provienen el termino malware?
8. Enumere dos síntomas de un virus informático.
9. Enumere tres controles de seguridad física.
10. Enumere 4 amenazas físicas de los sistemas informáticos.