

## Guía de trabajo autónomo #2

Nombre del docente: <b>Lic. Clotilde Fuentes Núñez</b>
Especialidad Técnica: <b>Secretariado Ejecutivo</b>
Subárea: <b>Destrezas digitales para el procedimiento y archivo de la información física y electrónica.</b>
Unidad de estudio: <b>Destrezas digitales para el procedimiento y archivo de la información.</b>
Nivel: <b>Décimo</b>
Horario de atención: <b>Presencial</b> Centro educativo: <b>CTP LA SUIZA</b>
Escenario: 1 ( <input checked="" type="checkbox"/> ) 2 ( <input type="checkbox"/> ) 3 ( <input type="checkbox"/> ) 4 ( <input type="checkbox"/> )
Período establecido para el desarrollo de la guía: <b>Del 15 al 26 de Marzo del 2021</b>

### II Parte. Planificación Pedagógica

<b>Espacio físico, materiales o recursos didácticos que voy a necesitar:</b>	Lapiceros, lápiz, calculadora, cuaderno para materia, herramientas tecnológicas.
<b>Indicaciones generales:</b>	Todo el material se le hace llegar a los estudiantes por medio de la plataforma teams, página web institucional, físico o correo electrónico; las tareas o trabajos son devueltos por medio de teams o en forma física para ser revisados.

### Detalle de la planificación de las actividades que realiza el estudiante.

#### Resultado (s) de aprendizaje/Objetivo (s):

1. Operar las funciones básicas del sistema operativo garantizando la seguridad de la información según protocolos

Actividades de aprendizaje para la implementación de la mediación 1. pedagógica en educación combinada	Ambiente de Aprendizaje	Evidencias
<p>Conexión</p> <p>Se explica el concepto de los fundamentos de la computadora con ayuda de material bibliográfico.</p> <p>Construcción/Aplicación:</p> <p>El estudiante en elabora un desplegable sobre el tema de virus y antivirus, puede utilizar material reutilizable.</p>	<p>Hogar ( <input checked="" type="checkbox"/> )</p> <p>Centro educativo ( <input checked="" type="checkbox"/> )</p>	<p>Tipo:</p> <p>( <input type="checkbox"/> ) Conocimiento</p> <p>_____</p> <p>( <input type="checkbox"/> ) Desempeño</p> <p>_____</p> <p>( <input checked="" type="checkbox"/> ) Producto</p> <p>desplegable</p>

## I UNIDAD: Destrezas digitales para elaborar procesar y organizar información

### TEMA: Virus y Antivirus



#### Concepto

Es un programa de computadora que tiene la capacidad de causar daño infectando “entidades ejecutables” (cualquier archivo o sector de las unidades de almacenamiento que contenga códigos de instrucción que el procesador valla a ejecutar). Su característica más relevante es que puede replicarse a sí mismo y propagarse a otras computadoras.

#### Tipos de Virus

Todos los virus tienen en común una característica, y es que crean efectos dañinos. A continuación se presenta una clasificación de los virus informáticos, basada en el daño que causan y efectos que provocan.

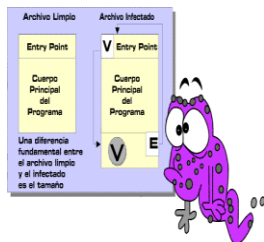
➤ **Caballo de Troya:** Es un programa dañino que se oculta en otro programa legítimo, y que produce sus efectos dañinos al ejecutarse el legítimo. En este caso, no es capaz de infectar otros archivos o soportes, y sólo se ejecuta una vez, aunque es suficiente, en la mayoría de las ocasiones, para causar su efecto destructivo.



➤ **Gusano o Worms:** Es un programa cuya única finalidad es la de ir consumiendo la memoria del sistema, se copia así mismo sucesivamente, hasta que desborda la RAM, siendo ésta su única acción maligna.

➤ **Virus de macros:** Los virus de macros (secuencia de órdenes de teclado y mouse asignadas a una sola tecla, símbolo o comando) afectan a archivos y plantillas que los contienen, haciéndose pasar por una macro y actúan hasta que el archivo se abra o utilice.





- **Virus de sobreescritura:** Sobrescriben en el interior de los archivos atacados, haciendo que se pierda el contenido de los mismos.

- **Virus de Programa:** Comúnmente infectan archivos con extensiones .EXE, .COM, .OVL, .DRV, .BIN, .DLL, y .SYS., los dos primeros son atacados más frecuentemente por que se utilizan más.



- **Virus de Boot:** Son virus que infectan sectores de inicio y booteo (Boot Record) de los diskettes y el sector de arranque maestro (Master Boot Record) de los discos duros; también pueden infectar las tablas de particiones de los discos.

- **Virus Residentes:** Se colocan automáticamente en la memoria de la computadora y desde ella esperan la ejecución de algún programa o la utilización de algún archivo.

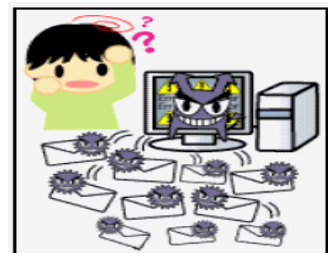


- **Virus de enlace o directorio:** Modifican las direcciones que permiten, a nivel interno, acceder a cada uno de los archivos existentes, y como consecuencia no es posible localizarlos y trabajar con ellos.

- **Virus mutantes o polimórficos:** Son virus que mutan, es decir cambian ciertas partes de su código fuente haciendo uso de procesos de encriptación y de la misma tecnología que utilizan los antivirus. Debido a estas mutaciones, cada generación de virus es diferente a la versión anterior, dificultando así su detección y eliminación.



➤ **Virus falso o Hoax:** Los denominados virus falsos en realidad no son virus, sino cadenas de mensajes distribuidas a través del correo electrónico y las redes. Estos mensajes normalmente informan acerca de peligros de infección de virus, los cuales mayormente son falsos y cuyo único objetivo es sobrecargar el flujo de información a través de las redes y el correo electrónico de todo el mundo.



➤ **Virus Múltiples:** Son virus que infectan archivos ejecutables y sectores de booteo simultáneamente, combinando en ellos la acción de los virus de programa y de los virus de sector de arranque.

## Síntomas de infección de virus en un computador

Después de abrir y ejecutar un programa o un archivo adjunto infectado en la computadora, quizá no se dé cuenta de que ha introducido un virus hasta que note que algo no funciona como debiera.

A continuación se enumeran algunos síntomas que podrían indicar que su sistema está infectado:

- Funciona más lentamente que de costumbre
- Deja de responder o se bloquea con frecuencia
- La computadora se bloquea y el sistema se reinicia cada pocos minutos
- Se reinicia por sí solo y después no funciona normalmente
- Las aplicaciones no funcionan correctamente
- Los discos o las unidades de disco no están accesibles
- No se imprime correctamente
- Aparecen mensajes de error poco habituales
- Se ven menús y cuadros de diálogo distorsionados

Éstos son síntomas comunes de infección, pero también podrían ser indicativos de problemas de hardware o software que no tienen nada que ver con un virus. La cuestión es que, a menos que instale un software antivirus estándar en la computadora y lo vaya actualizando debidamente, no hay ningún medio de determinar con total seguridad si la computadora está infectada con virus o no.

**Sugerencia:** Cuidado con los mensajes en los que se le advierte que ha enviado correo electrónico que contenía un virus. Esto puede indicar que el virus ha incluido su dirección de correo electrónico como remitente de correo electrónico infectado. Eso no significa necesariamente que tenga un virus.



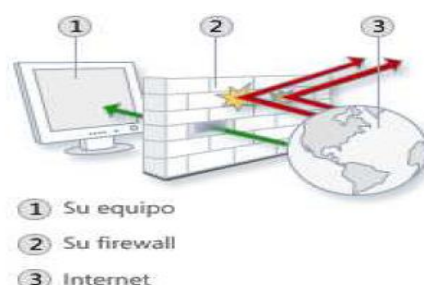
## Medidas Preventivas y Cuidados contra Virus

Muchos recomiendan no utilizar unidades de almacenamiento extraíble que fueron utilizados en otros equipos informáticos que posteriormente serán utilizados en nuestra computadora, sin embargo esta medida es imposible, ya que los usuarios transportan información electrónicamente, ya sea por correo electrónico, redes locales, Internet y unidades físicas de almacenamiento, (Cd, Unidad USB, Disquetes, Zip, otros); a lo cual necesariamente esa información llegará a nuestro computador.

Microsoft Corporation recomienda tres métodos fundamentales:

1. **Contar con un Firewall:** Un firewall es software o hardware que comprueba la información procedente de Internet o de una red y, a continuación, bloquea o permite el paso de ésta al equipo, en función de la configuración del firewall.

En la siguiente ilustración se muestra el funcionamiento de un firewall:



## 2. Actualizar el Sistema Operativo

Las actualizaciones son adiciones al software que pueden evitar o corregir problemas, aumentar la seguridad del equipo contra virus o gusanos, o bien mejorar el rendimiento de éste.

## 3. Instalar un Antivirus

Existen diferentes versiones de antivirus, y cada una de ellas con diferentes propósitos.

## Software Antivirus

Un antivirus es un programa diseñado para prevenir y evitar la activación de virus en nuestra computadora, tiene rutinas de detección, eliminación y reconstrucción de la información afectada.

Los antivirus realizan tres principales funciones que son:

1. **Vacunar:** La vacuna de los antivirus se queda residente en memoria y filtra los programas que son ejecutados.
2. **Detectar:** Revisa todos los archivos que tenemos grabados en el disco duro. Mediante el grupo de códigos virales el antivirus escanea la información para reconocerlos y borrarlos.



3. Eliminar: Es la parte del antivirus que desarma la estructura del virus y las elimina, finalmente repara los archivos dañados.

Un programa antivirus debe estar bien configurado para que trabaje correctamente, y algo muy importante debe estar actualizado. El antivirus no es una solución definitiva, nos ayuda a minimizar el riesgo.

### **Tipos de antivirus**

- ✓ AVG
- ✓ Norton
- ✓ Microsoft Security
- ✓ Avira
- ✓ Kaspersky
- ✓ Panda
- ✓ Avast!
- ✓ NOD 32

### **ACTIVIDAD**

1. Utilizando materiales reutilizables, elabore un desplegable sobre los virus y tipos de virus, así como de los diferentes antivirus.