	INSTITUCIÓN EDUCATIVA SAN CRISTÓBAL “Liderando procesos de crecimiento humano”
	TALLER DE TECNOLOGÍA **TEMA: Delitos informáticos** **Docente: Beatriz Elena Herrera Legarda.**

Virus Informáticos

Un virus informático es un programa malicioso que, al ejecutarse, se reproduce insertando copias de sí mismo en otros programas o archivos. Su objetivo puede ser dañar, robar información o controlar el equipo sin permiso.

Clasificación de virus informáticos:

- Virus de archivo: Infecta archivos ejecutables y se activa al abrir el archivo infectado.

- Virus de sector de arranque: Infecta el sector de arranque del disco y se carga antes del sistema operativo.

- Gusanos: Programas que se replican a sí mismos a través de redes, consumiendo ancho de banda.

- Troyanos: Se presentan como software legítimo, pero ocultan funcionalidades maliciosas.

- Macrovirus: Infectan documentos con macros, como archivos de Word o Excel.

Delitos Informáticos

Los delitos informáticos son acciones ilícitas que utilizan medios electrónicos o digitales para perjudicar a otras personas, empresas o instituciones.

Tipos de delitos informáticos:

- Hacking: Acceso no autorizado a sistemas o redes para obtener información.

- Phishing: Suplantación de identidad para obtener datos privados mediante engaños.

- Fraude informático: Uso de sistemas informáticos para realizar estafas o fraudes económicos.

- Suplantación de identidad: Uso indebido de datos personales de otro usuario.

- Ciberacoso: Acoso, amenazas o hostigamiento a través de medios digitales.

- Distribución de malware: Creación y difusión de software malicioso.

Seguridad Informática

La seguridad informática comprende las medidas y prácticas para proteger la información digital y los sistemas de posibles ataques o accesos no autorizados.

Aspectos clave para protegerse:

- Uso de contraseñas seguras y gestión de contraseñas.

- Mantener el sistema operativo y software actualizados.

- Instalar y actualizar un programa antivirus y antimalware.

- Configurar y revisar regularmente cortafuegos (firewalls).

- No hacer clic en enlaces o descargar archivos de fuentes desconocidas.

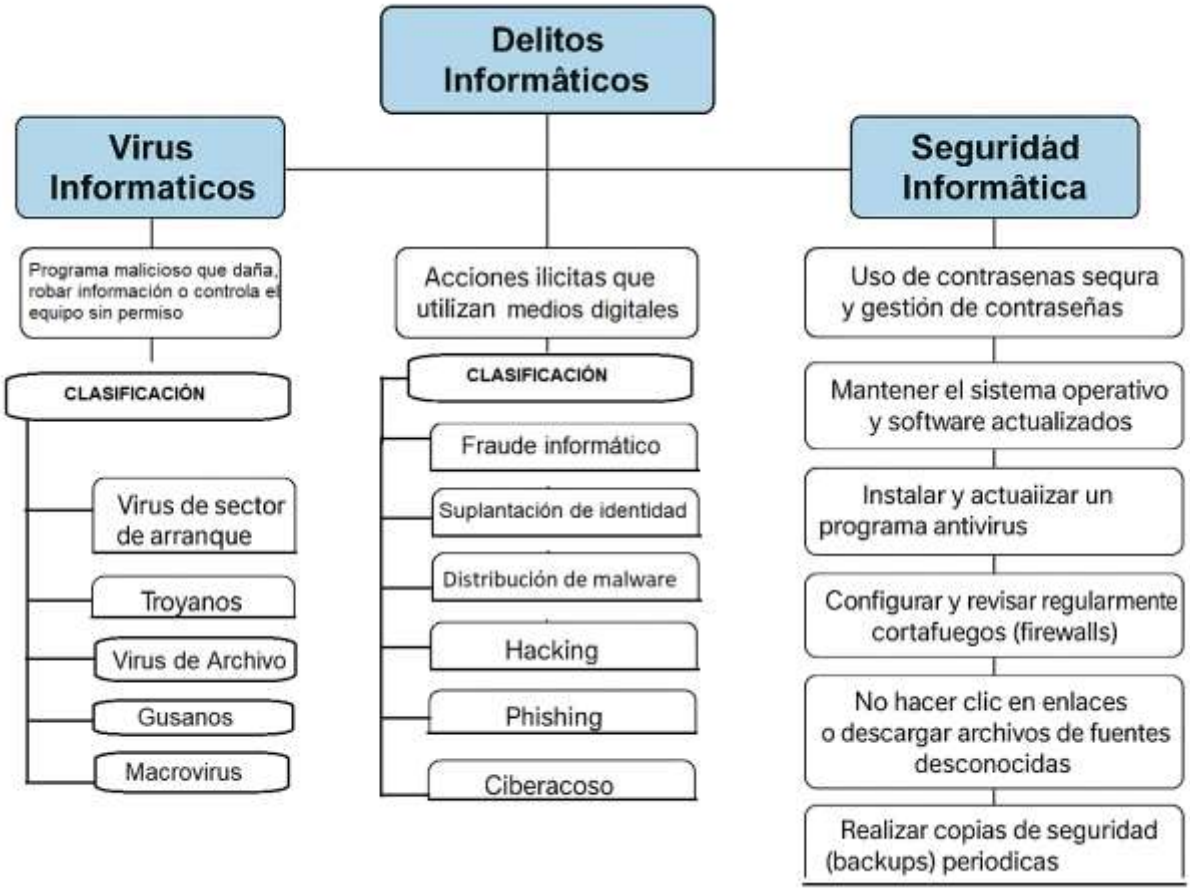
- Realizar copias de seguridad (backups) periódicas.

- Proteger los datos personales y no compartir información sensible.

Actividad

1. Copia el texto en el cuaderno.

2. Realiza el siguiente esquema en el computador.



3. De acuerdo a los siguientes enunciados, escribe al frente el tipo de virus o de delito informático al que pertenece:

a. Un archivo ejecutable descargado de un sitio desconocido que, al abrirlo, infecta otros .exe en la carpeta de usuario.

b. Una USB infectada que al conectarse al computador modifica el sector de arranque y el sistema no arranca correctamente.

c. Un programa que se envía automáticamente por correo electrónico a todos los contactos del usuario, consumiendo ancho de banda.

d. Una aplicación de juego gratuito de apariencia legítima que instala un programa que da acceso remoto al instalarla.

e. Un documento de Word con macros que, al habilitar macros, ejecuta código que infecta otros documentos.

f. Un atacante explota una vulnerabilidad en el servidor de una empresa para obtener datos confidenciales de clientes.

g. Un correo que simula ser del banco pide al usuario ingresar sus credenciales en un enlace falso.

h. Venta de productos inexistentes en una tienda en línea falsa, cobrando por adelantado y sin entregar nada.

i. Creación de un perfil falso en redes sociales usando fotos y datos de otra persona para pedir préstamos.

j. Envió constante de mensajes amenazantes y difamatorios a una víctima a través de redes sociales.

4. Elaborar un afiche donde expliques algunas recomendaciones de seguridad para no ser víctima de un delito informático.