Guía de trabajo autónomo GTA2

Nombre del docente: Jorge Luis Rodríguez Serrano.

Especialidad Técnica: agroindustria con tecnología pecuaria.

Subárea: Agronegocios

Unidad de estudio: Agromática

Nivel: X

Horario de atención: A distancia Centro educativo: Colegio Técnico Profesional la Suiza

Escenario: 1 ( ) 2 ( ) 3 ( ) 4 ( )

Canal de comunicación: WhatsApp, correo electrónico (Jorge.serrano.rodriguez@mep.go.cr), TEAMS.

Período establecido para el desarrollo de la guía:

Del 15 del mes MARZO al 31 del mes MARZO de 2021

Nombre del Estudiante: _____ Sección: _____

Nombre del Padre o encargado: _____ Firma: _____

II Parte. Planificación Pedagógica

Espacio físico, materiales o recursos didácticos que voy a necesitar: (Importante considerar la situación de cada uno de los estudiantes)	• Cuaderno de Comunicación Empresarial • Lápiz o lapicero, hojas rayadas o blancas, otros Computadora (si tiene)
Indicaciones generales:	• Lea detenidamente toda la guía. • Una vez, concluida la lectura, realice cada una de las actividades que se plantean. • Cuide su caligrafía y ortografía. • Trabaje en forma ordenada. • Medio de comunicación oficial por medio de programa teams Si tiene computadora y desea resolver los ejercicios en este mismo documento lo puede hacer y lo guarda o lo puede imprimir si está a su alcance, o puede resolver las actividades en hojas aparte o en su cuaderno .

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

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

- Resolver problemas de virus en las computadoras

Actividades de aprendizaje para la implementación de la mediación pedagógica en educación combinada	Ambiente de Aprendizaje	Evidencias
CONEXION • identifica el concepto de virus y antivirus mediante toma de apuntes. **Clarificación**	Hogar (x) Centro educativo (x)	Tipo: (x) Desempeño _____

• Diferencia los tipos de virus y antivirus y la Instala y configura protecciones antivirus mediante uso de antivirus del computador **<u>Colaboración</u>** • Aplica los procedimientos para la detección, corrección y protección de programas mediante revista digital • **<u>Construcción/aplicación</u>**. • Examina diferentes programas y dispositivos de almacenamiento utilizando antivirus mediante cuadro comparativo. .		(x) Conocimiento _____ (x) Producto

Actividades de aprendizaje para la implementación de la mediación pedagógica en educación combinada.

Actividades:

¿Qué es un virus informático?

Un virus informático es un software malicioso ejecutable o un código que se auto reproduce al tomar control sobre otros programas en un ordenador infectado. Diseñados para esparcirse desde un equipo host hacia otros ordenadores, el virus informático se agrega a un componente del software o a un documento y se queda allí hasta que el usuario abre el archivo en cuestión. Cuando esto pasa, el virus empezará a ejecutar su código y causará daños en el ordenador host.

Hay muchas maneras de contraer un virus informático, con la descarga de archivos, adjuntos de emails, instalación de software comprometido, o enlaces basura en las redes sociales. Usted puede esparcir el virus si comparte los archivos o los enlaces infectados con otros. Si su ordenador forma parte de una red, con que un solo usuario abra el archivo peligroso en su escritorio, puede ser suficiente para que toda la red se comprometa.

Aunque es cierto que ha habido virus “buenos” con efectos positivos sobre los equipos host, los virus informáticos son malos por definición. Cuando se ejecutan, pueden enviar correo no deseado a sus contactos del email y redes sociales, pueden corromper archivos de su disco duro y ralentizar su ordenador. Los virus pueden robarle las contraseñas y cambiarle los datos de registro para que no pueda acceder a sus cuentas de emails o perfiles de redes sociales, cuentas bancarias online o incluso su ordenador. En el peor de los casos, pueden borrar todos los datos de su disco duro en cuestión de segundos.

¿Qué tipos de virus informáticos existen?

Hay más de un millón de virus en el mundo, y muchos más se crean cada día. Evolucionan muy rápido, así los que una vez fueron considerados extremadamente peligrosos, hoy en día se sofocan de forma rutinaria con el mejor software antivirus. Basados en la severidad y en la forma de la que pueden afectar su equipo, hay alrededor de una docena de tipos de virus. Aquí están los cinco peores tipos de virus de computadora que debería conocer.

Macro Virus

Probablemente sea el tipo más común de virus informático, los macro virus se adjuntan a los archivos creados en programas que soportan macros, secuencias de órdenes que se pueden ejecutar simplemente al apretar una tecla. Estos virus se encuentran con más frecuencia en los documentos de Microsoft Word y hojas de cálculo de Excel.

La forma más común de distribuirlos es a través de archivos adjuntos a los emails. Los macro virus se activan cuando usted abre el archivo infectado. Si lo hace directamente desde su email, el virus enviará una copia exacta del archivo a todas las direcciones de su lista de contactos. Si descarga el archivo en su ordenador y lo abre posteriormente, el macro virus se extenderá hacia otros archivos con extensión .docx y .xls de su red de ordenadores y alterará su contenido.

Virus de Archivo

Mientras que los macro virus normalmente infectan archivos creados en Microsoft Office, los virus de archivo se adjuntan a los archivos ejecutables con extensiones .exe y .com. Cuando abre un archivo infectado para iniciar un programa, inconscientemente iniciará el virus también. El virus puede tomar el control del programa y expandirse hacia otros archivos ejecutables en su disco duro o su red de ordenadores.

El objetivo principal de los virus de archivo es poner en peligro archivos y datos en los equipos y redes del usuario, crear botnets interconectados y deshabilitar el software de seguridad en ordenadores encendidos. Algunos virus de archivo reescribirán todos los archivos ejecutables que se activan durante el encendido, y así tomarán el control de su ordenador de una manera efectiva. También se han dado casos en los que un macro virus ha formateado completamente discos duros infectados.

Secuestradores del Navegador

Tal y como su nombre indica, los secuestradores del navegador toman el control sobre ciertos componentes de su explorador de internet. Normalmente cambian su página de inicio por algún explorador falso y sobrescriben los ajustes para que usted no los pueda cambiar. Cuando usted introduce una dirección y presiona Intro, el virus le llevará a una página web totalmente diferente y

le pedirá que haga click en un anuncio o que se registre para cualquier cosa para acceder a la página que quiere ver.

En la mayoría de los casos, los secuestradores del navegador están destinados a generar ingresos para sus creadores por enseñar anuncios en los que se puede hacer click dentro del navegador. Normalmente están alojados en el software gratuito y en las barras de herramientas de los buscadores que ofrecen componentes de búsqueda avanzada. Afortunadamente, la mayoría de los programas antivirus los detectan fácilmente.

Virus de Secuencia de Comandos (Scripting)

Los virus de scripting atacan páginas web populares, normalmente de un modo muy sibilino. Estos virus sobrescriben el código de la página web para insertar enlaces y vídeos que instalarán software malicioso en el ordenador del usuario. En muchos casos, los propietarios de las páginas web ni siquiera saben que están alojando contenido potencialmente dañino. Todo lo que un hacker experimentado tiene que hacer para infectar la página es escribir el código malicioso y publicarlo como un comentario.

Algunos virus de scripting hacen poco más que ofrecerle anuncios visuales y de texto para generar ingresos para sus creadores. Sin embargo, algunos pueden robar sus cookies y utilizar la información para publicar en su nombre en la página web infectada. Afortunadamente, la mayoría de los programas antivirus le avisarán cuando visite una página web dañina.

Virus del Sector de Arranque

Aunque no sean tan frecuentes ahora como lo fueron en el pasado, los virus del sector de arranque todavía pueden aparecer de una forma u otra. Cuando los ordenadores se arrancaban con disquetes, estos virus eran muy comunes. Infectaban el sistema de particiones del disco duro y se ejecutaban con el arranque del ordenador.

Hoy en día, estos virus se esparcen mayoritariamente a través de los dispositivos físicos, como los USB y discos duros externos. Ya no suponen una gran amenaza, ya que, casi todos los sistemas operativos tienen protección del sector de arranque del disco duro contra el software malicioso. Incuso si infectan su sistema de algún modo, la mayoría de los programas antivirus pueden eliminar los virus del sector de arranque fácilmente.

Ejemplos de virus informáticos

Algunos de los ejemplos de virus informáticos más peligrosos y/o conocidos son:

Melissa fue un macro virus que se expandió a través de archivos adjuntos a emails y causó unas pérdidas de 80 millones de dólares. Su creador David L. Smith pasó 20 meses en la cárcel y se le prohibió acceder a redes de ordenadores sin autorización.

Yankee Doodle fue un virus de archivo no destructivo de origen búlgaro, que iniciaba la reproducción de la canción "Yankee Doodle" en los ordenadores infectados todos los días a las 17 horas.

Shamoon es un virus destructivo que borraba todos los datos de redes de ordenadores en cuestión de segundos. Fue desarrollado como arma en la guerra cibernética contra el sector energético de Arabia Saudí. Se neutralizó en 2014, para volver (como "Shamoon 2") dos años más tarde.

Klez fue un macro virus que deshabilitaba el software antivirus en el ordenador infectado y enviaba correo no deseado (spam) a la bandeja de entrada de la víctima para impedir la recepción de nuevos mensajes.

¿Cómo eliminar virus informáticos?

Existen muchos programas, gratuitos y de pago, que prometen mantener su ordenador a salvo de las amenazas, pero solamente los mejores softwares antivirus cumplen con esa promesa. Estos programas analizarán su sistema en busca de amenazas y le informarán cada vez que detecten una. Dependiendo de la severidad del virus, pondrán el archivo infectado en cuarentena o lo eliminarán completamente para evitar que el virus se multiplique.

Algunos virus son tan destructivos que pueden borrar todos sus datos e inutilizar su disco duro. Cuando atacan, puede que sea demasiado tarde para poner una solución, por lo que es muy importante la prevención.

Con software fiable instalado en su ordenador, ningún virus será capaz de infectar sus documentos y archivos. Para disponer de una protección óptima, asegúrese de utilizar siempre la última versión del software y de descargar las actualizaciones de definiciones de virus diariamente. El mejor software antivirus hará todo esto automáticamente, y le permitirá una navegación segura sin tener que preocuparse de los virus y otras amenazas a su seguridad en la red.

Actividad

1) Realizar un mapa conceptual del tema anterior.

- **Evaluación del desempeño:**

DESARROLLO	AUN NO LOGRADO 1	EN PROCESO 2	LOGRADO 3

• Diferencia eficientemente los tipos de virus y antivirus			
• Aplica los procedimientos para la detección, corrección y protección de programas sin margen de error			