ACTIVIDAD EN CLASE

(LEA MUY BIEN LA GUIA)

1.

Realice un documento en Word que tenga:

a. Tabla de contenido
b. Numeración de pagina (http://youtu.be/DZOvxaeCE4k)
c. Encabezado de pagina (http://youtu.be/kimd6zujLsk)

2. La temática del trabajo es:

• LOS VIRUS

○ HISTORIA ○ CARACTERISTICAS ○

METODOS DE PROPAGACIÓN ○

METODOS DE PROTECCIÓN

- Activos
- Pasivos ○ TIPOS DE VIRUS
- Troyano
- Gusano
- Bombas Lógicas
- Hoax
- Joke ○ ACCIONES DE LOS VIRUS ○

ANTIVIRUS

NOTA: el documento debe estar organizado y editado es decir un solo tipo de letra, un solo tamaño y color negro, los párrafos justificados y quitando los hipervinculos.

LA INFORMACIÓN LA PUEDE COPIAR DE:

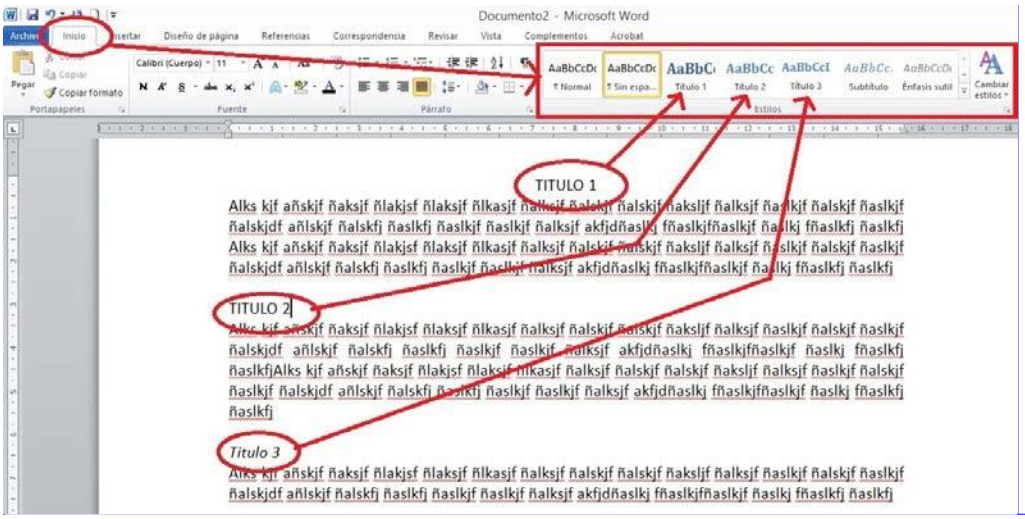
- http://es.wikipedia.org/wiki/Virus_inform%C3%A1tico
- http://es.wikipedia.org/wiki/Antivirus (***ver ejemplo desde la página 4***).

Comentario [DADB2]:
PASOS PARA SUBIR EL DOCUMENTO AL GRUPO "TECNOLOGIA 7-5" EN FACEBOOK

- TERMINADO EL DOCUMENTO LO GUARDA EN MIS DOCUMENTOS CON EL NOMBRE "taller en clase juan díaz y carlos perez" Y LO SUBE A FACEBOOK AL

Comentario [DADB1]:

Comentario [DADB3]:
PARA PONER LOS DIFERENTES ESTILOS A LOS TITULOS O SUBTITULOS (TITULO 1, TITULO 2 Y TITULO 3)

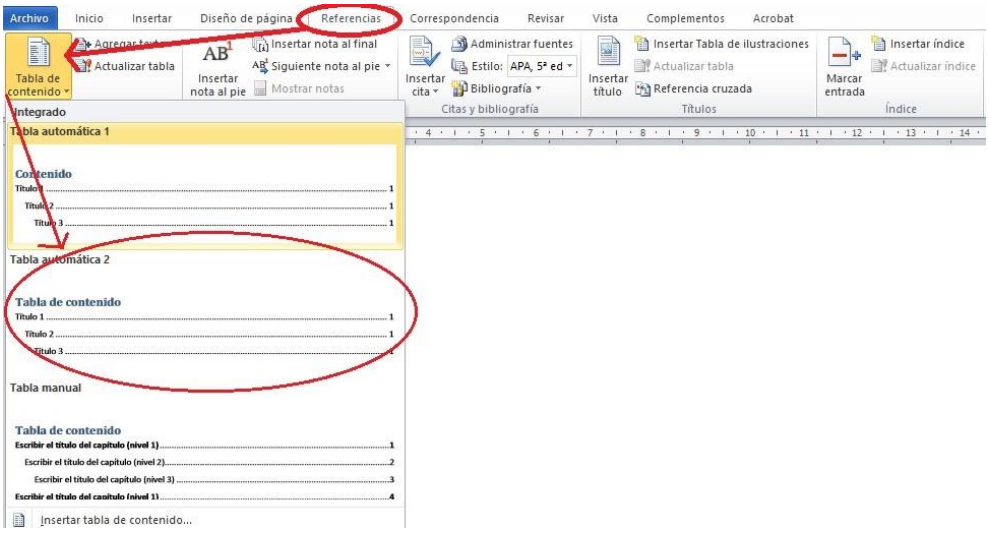


Integrantes del grupo

GRUPO "tecnología 7-1. 7-2, 7-3……."

PARA PONER LOS TITULOS1 – TITULOS 2 Y TITULOS 3 PARA PONER LA TABLA DE CONTENIDO:

Luego de tener los títulos puestos es decir de aplicar los estilos (imagen anterior) **se pone la tabla de contenido**: para ello se da clic en la cinta REFERENCIAS y luego en la opción TABLA DE CONTENIDO y escoge la que quiera. (*ver la siguiente imagen para poner la tabla de contenido*)



LUEGO DE TENER CLARO TODO LO ANTERIOR DEBE QUE DAR EL DOCUMENTO ASI: ***Ver documento organizado desde la pagina 4***, es decir debe quedar igual en cuanto a organización tipo de letra y edicion del documento es decir ud lo va a organizar para que quede igual.

AQUÍ COMIENZA EL DOCUMENTO DE EJEMPO

(ASI DEBE QUEDAR EL SUYO)

TABLA DE CONTENIDO

LOS VIRUS

Un **virus informático** es un malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en una computadora, aunque también existen otros más inofensivos, que solo se caracterizan por ser molestos.

Los virus informáticos tienen, básicamente, la función de propagarse a través de un software, no se replican a sí mismos porque no tienen esa facultad como el gusano informático, son muy nocivos y algunos contienen además una carga dañina (payload) con distintos objetivos, desde una simple broma hasta realizar daños importantes en los sistemas, o bloquear las redes informáticas generando tráfico inútil.

El funcionamiento de un virus informático es conceptualmente simple. Se ejecuta un programa que está infectado, en la mayoría de las ocasiones, por desconocimiento del usuario. El código del virus queda residente (alojado) en la memoria RAM de la computadora, incluso cuando el programa que lo contenía haya terminado de ejecutarse. El virus toma entonces el control de los servicios básicos del sistema operativo, infectando, de manera posterior, archivos ejecutables que sean llamados para su ejecución. Finalmente se añade el código del virus al programa infectado y se graba en el disco, con lo cual el proceso de replicado se completa.

HISTORIA

El primer virus atacó a una máquina IBM Serie 360 (y reconocido como tal). Fue llamado Creeper, creado en 1972. Este programa emitía periódicamente en la pantalla el mensaje: «I'm a creeper... catch me if you can!» (*¡Soy una enredadera... agárrame si puedes!).* Para eliminar este problema se creó el primer programa antivirus denominado *Reaper* (cortadora).

Sin embargo, el término virus no se adoptaría hasta 1984, pero éstos ya existían desde antes. Sus inicios fueron en los laboratorios de *Bell Computers*. Cuatro programadores (H Douglas Mellory, Robert Morris, Victor Vysottsky y Ken Thompson) desarrollaron un juego llamado *Core War*, el cual consistía en ocupar toda la memoria RAM del equipo contrario en el menor tiempo posible.

Comentario [DADB4]:
::::PARA TODOS LOS TITULO1::::
TITULO 1
MAYUSCULA
CENTRADO
NEGRITA

Comentario [DADB5]:
:::::::PARA TODO EL DOCUMENTO:::::::
TEXTO JUSTIFICADO.

TITULO 2 NEGRITA MAYUSCULA ALINEADO A LA IZQUIERDA

CARACTERISTICAS

Comentario [DADB7]: TITULO 2

Comentario [DADB6]:

Después de 1984, los virus han tenido una gran expansión, desde los que atacan los sectores de arranque de disquetes hasta los que se adjuntan en un correo electrónico.

Dado que una característica de los virus es el consumo de recursos, los virus ocasionan problemas tales como: pérdida de productividad, cortes en los sistemas de información o daños a nivel de datos. Una de las características es la posibilidad que tienen de diseminarse por medio de *replicas y copias*. Las redes en la actualidad ayudan a dicha propagación cuando éstas no tienen la seguridad adecuada.

Otros daños que los virus producen a los sistemas informáticos son la pérdida de información, horas de parada productiva, tiempo de reinstalación, etc. Hay que tener en cuenta que cada virus plantea una situación diferente.

METODOS DE PROPAGACIÓN

Comentario [DADB8]: TITULO 2

Existen dos grandes clases de contagio. En la primera, el usuario, en un momento dado, ejecuta o acepta de forma inadvertida la instalación del virus. En la segunda, el programa malicioso actúa replicándose a través de las redes. En este caso se habla de gusanos.

En cualquiera de los dos casos, el sistema operativo infectado comienza a sufrir una serie de comportamientos anómalos o imprevistos. Dichos comportamientos pueden dar una pista del problema y permitir la recuperación del mismo.

Dentro de las contaminaciones más frecuentes por interacción del usuario están las siguientes:

- Mensajes que ejecutan automáticamente programas (como el programa de correo que abre directamente un archivo adjunto).
- Ingeniería social, mensajes como *ejecute este programa y gane un premio*, o, más comúnmente: *Haz 2 clics y gana 2 tonos para móvil gratis.*.
- Entrada de información en discos de otros usuarios infectados.
- Instalación de software modificado o de dudosa procedencia.

En el sistema Windows puede darse el caso de que la computadora pueda infectarse sin ningún tipo de intervención del usuario (versiones Windows 2000, XP y Server 2003) por virus como Blaster, Sasser y sus variantes por el simple hecho de estar la máquina conectada a una red o a Internet. Este tipo de virus aprovechan una vulnerabilidad de desbordamiento de buffer y puertos de red para infiltrarse y contagiar el equipo, causar inestabilidad en el sistema, mostrar mensajes de error, reenviarse a otras máquinas mediante la red local o Internet y hasta reiniciar el sistema, entre otros daños. En las últimas versiones de Windows 2000, XP y Server 2003 se ha corregido este problema en su mayoría.

METODOS DE PROTECCIÓN

Los métodos para disminuir o reducir los riesgos asociados a los virus pueden ser los denominados activos o pasivos.

Activos

- **Antivirus**: son programas que tratan de descubrir las trazas que ha dejado un software malicioso, para detectarlo y eliminarlo, y en algunos casos contener o parar la contaminación. Tratan de tener controlado el sistema mientras funciona

Pasivos

parando las vías conocidas de infección y notificando al usuario de posibles incidencias de seguridad. Por ejemplo, al verse que se crea un archivo llamado *Win32.EXE.vbs* en la carpeta *C:\Windows\%System32%* en segundo plano, ve que es comportamiento sospechoso, salta y avisa al usuario.

- **Filtros de ficheros**: consiste en generar filtros de ficheros dañinos si el computador está conectado a una red. Estos filtros pueden usarse, por ejemplo, en
- Evitar introducir a tu equipo medios de almacenamiento extraíbles que consideres que pudieran estar infectados con algún virus.
- No instalar software "pirata", pues puede tener dudosa procedencia.
- No abrir mensajes provenientes de una dirección electrónica desconocida.
- No aceptar e-mails de desconocidos.

el sistema de correos o usando técnicas de firewall. En general, este sistema proporciona una seguridad donde no se requiere la intervención del usuario, puede ser muy eficaz, y permitir emplear únicamente recursos de forma más selectiva.

Comentario [DADB9]: TITULO 2

Comentario [DADB11]: TITULO 3

Comentario [DADB10]: ::::PARA TODOS LOS TITULO 3:::: TITULO 3 NEGRITA MINUSCULA ALINEADO A LA IZQUIERDA

TIPOS DE VIRUS

Comentario [DADB12]: TITULO 2

- Informarse y utilizar sistemas operativos más seguros.
- No abrir documentos sin asegurarnos del tipo de archivo. Puede ser un ejecutable o incorporar macros en su interior.

Troyano

Comentario [DADB13]: TITULO 3

Existen diversos tipos de virus, varían según su función o la manera en que éste se ejecuta en nuestra computadora alterando la actividad de la misma, entre los más comunes están:

Consiste en robar información o alterar el sistema del hardware o en un caso extremo

Bombas Lógicas

Comentario [DADB14]: TITULO 3

permite que un usuario externo pueda controlar el equipo.

Gusano

Tiene la propiedad de duplicarse a sí mismo. Los gusanos utilizan las partes automáticas de un sistema operativo que generalmente son invisibles al usuario.

Hoax

Comentario [DADB15]: TITULO 3

Son programas que se activan al producirse un acontecimiento determinado. La condición suele ser una fecha (Bombas de Tiempo), una combinación de teclas, o ciertas condiciones técnicas (Bombas Lógicas). Si no se produce la condición permanece oculto al usuario.

Los hoax no son virus ni tienen capacidad de reproducirse por si solos. Son mensajes de

Joke

Comentario [DADB16]: TITULO 3

contenido falso que incitan al usuario a hacer copias y enviarla a sus contactos. Suelen apelar a los sentimientos morales ("Ayuda a un niño enfermo de cáncer") o al espíritu de solidaridad ("Aviso de un nuevo virus peligrosísimo") y, en cualquier caso, tratan de aprovecharse de la falta de experiencia de los internautas novatos.

Al igual que los hoax, no son virus, pero son molestos, un ejemplo: una página pornográfica que se mueve de un lado a otro, y si se le llega a dar a errar es posible que salga una ventana que diga: OMFG!! No se puede cerrar!

ACCIONES DE LOS VIRUS

Comentario [DADB17]: TITULO 2

Algunas de las acciones de algunos virus son:

- Unirse a un programa instalado en el computador permitiendo su propagación.
- Mostrar en la pantalla mensajes o imágenes humorísticas, generalmente molestas.
- Ralentizar o bloquear el computador.

ANTIVIRUS

Comentario [DADB18]: TITULO 2

- Destruir la información almacenada en el disco, en algunos casos vital para el sistema, que impedirá el funcionamiento del equipo.
- Reducir el espacio en el disco.
- Molestar al usuario cerrando ventanas, moviendo el ratón..

En informática los **antivirus** son programas cuyo objetivo es detectar y/o eliminar virus informáticos. Nacieron durante la década de 1980.

CIBERGRAFIA

Comentario [DADB19]: TITULO 1

Con el transcurso del tiempo, la aparición de sistemas operativos más avanzados e Internet, ha hecho que los antivirus hayan evolucionado hacia programas más avanzados que no sólo buscan detectar virus informáticos, sino bloquearlos, desinfectarlos y prevenir una infección de los mismos, y actualmente ya son capaces de reconocer otros tipos de *malware*, como *spyware*, *rootkits*, etc.

- http://es.wikipedia.org/wiki/Virus_inform%C3%A1tico
- http://es.wikipedia.org/wiki/Antivirus

Comentario [DADB20]: PONER LOS INTEGRANTES DEL GRUPO APELLIDOS Y NOMBRES

INTEGRANTES: Nombre(s) del/Los integrante(s) del grupo