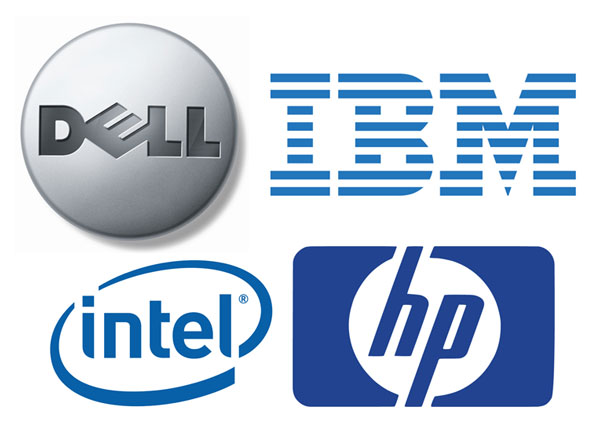
 **MEMORANDUM.**

PARA: TECNICOS DE EMPRESAS

DE: JESICA SHECCID PEREZ CADENA

ASUNTO: CLASIFICACION DE VIRUS.

FECHA: 26 DE SEPTIEMBRE DEL 2015.

Por medio de este memorándum se les informa de la clasificación de los virus:

***Tipos de Virus Informáticos según su destino de infección***

**Infectares de archivos ejecutables**

Afectan archivos de extensión EXE, COM, BAT, SYS, PIF, DLL, DRV

Infectares directos. El programa infectado tiene que estar ejecutándose para que el virus pueda funcionar (seguir infectando y ejecutar sus acciones destructivas)

**Infectares del sector de arranque (boto)**  
Tanto los discos rígidos como los disquetes contienen un Sector de Arranque, el cual contiene información específica relativa al formato del disco y los datos almacenados en él. Además, contiene un pequeño programa llamado Boto Programa que se ejecuta al botear desde ese disco y que se encarga de buscar y ejecutar en el disco los archivos del sistema operativo. Este programa es el que muestra el famoso mensaje de "Non-sistema Disk ir Disk Error" en caso de no encontrar los archivos del sistema operativo. Este es el programa afectado por los virus de sector de arranque. La computadora se infecta con un virus de sector de arranque al intentar botear desde un disquete infectado. En este momento el virus se ejecuta e infecta el sector de arranque del disco rígido, infectando luego cada disquete utilizado en el PC. Es importante destacar que como cada disco posee un sector de arranque, es posible infectar el PC con un disquete que contenga solo datos.....

**Virus Multa Partición**  
Bajo este nombre se engloban los virus que utilizan los dos métodos anteriores. Es decir, pueden simultáneamente infectar archivos, sectores boto de arranque y tablas FAT.

**Infectares residentes en memoria**  
El programa infectado no necesita estar ejecutándose, el virus se aloja en la memoria y permanece residente infectando cada nuevo programa ejecutado y ejecutando su rutina de destrucción

**Macro virus**  
Son los virus más populares de la actualidad. No se transmiten a través de archivos ejecutables, sino a través de los documentos de las aplicaciones que poseen algún tipo de lenguaje de macros. Entre ellas encontramos todas las pertenecientes al paquete Office (Word, Excel, Poder Point, Access) y también el Corel Graw, o AutoCAD.  
Cuando uno de estos archivos infectado es abierto o cerrado, el virus toma el control y se copia a la plantilla base de nuevos documentos, de forma que sean infectados todos los archivos que se abran o creen en el futuro.  
Los lenguajes de macros como el Visual Basic Foro Aplicaciones son muy poderosos y poseen capacidades como para cambiar la configuración del sistema operativo, borrar archivos, enviar e-mails, etc.

**De Actives Agentes y Java Pallets**  
En 1997, aparecen los Java pallets y Actives control. Estos pequeños programas se graban en el disco rígido del usuario cuando está conectado a Internet y se ejecutan cuando la página web sobre la que se navega lo requiere, siendo una forma de ejecutar rutinas sin tener que consumir ancho de banda. Los virus desarrollados con Java pallets y Actives control acceden al disco rígido a través de una conexión kW de manera que el usuario no los detecta. Se pueden programar para que borren o corrompan archivos, controlen la memoria, envíen información a un sitio web, etc.

**De HTML**  
Un mecanismo de infección más eficiente que el de los Java pallets y Actives control apareció a fines de 1998 con los virus que incluyen su código en archivos HTML. Con solo conectarse a Internet, cualquier archivo HTML de una página web puede contener y ejecutar un virus. Este tipo de virus se desarrollan en Visual Basic Script. Atacan a usuarios de Win98, 2000 y de las últimas versiones de Explorer. Esto se debe a que necesitan que el Windows Scripting Host se encuentre activo. Potencialmente pueden borrar o corromper archivos.

**Caballos de Troya**  
Los troyanos son programas que imitan programas útiles o ejecutan algún tipo de acción aparentemente inofensiva, pero que de forma oculta al usuario ejecutan el código dañino.  
Los troyanos no cumplen con la función de autor reproducción, sino que generalmente son diseñados de forma que por su contenido sea el mismo usuario el encargado de realizar la tarea de difusión del virus. (Generalmente son enviados por e-mail)

***Tipos de Virus Informáticos según sus acciones y/o modo de activación***

**Bombas**Se denominan así a los virus que ejecutan su acción dañina como si fuesen una bomba. Esto significa que se activan segundos después de verse el sistema infectado o después de un cierto tiempo (bombas de tiempo) o al comprobarse cierto tipo de condición lógica del equipo. (Bombas lógicas). Ejemplos de bombas de tiempo son los virus que se activan en una determinada fecha u hora determinada. Ejemplos de bombas lógicas son los virus que se activan cuando al disco rígido solo le queda el 10% sin uso, una secuencia de teclas o comandos, etc. Ejemplos de este tipo de programas son virus como Viernes 13 o el virus Miguel Ángel

**Camaleones**Son una variedad de virus similares a los caballos de Troya que actúan como otros programas parecidos, en los que el usuario confía, mientras que en realidad están haciendo algún tipo de daño. Cuando están correctamente programados, los camaleones pueden realizar todas las funciones de los programas legítimos a los que sustituyen (actúan como programas de demostración de productos, los cuales son simulaciones de programas reales).  
Un software camaleón podría, por ejemplo, emular un programa de acceso a sistemas remotos realizando todas las acciones que ellos realizan, pero como tarea adicional (y oculta a los usuarios) va almacenando en algún archivo los diferentes logis y pastor para que posteriormente puedan ser recuperados y utilizados ilegalmente por el creador del virus camaleón.

**Reproductores**Los reproductores (también conocidos como conejos-rabitos) se reproducen en forma constante una vez que son ejecutados hasta agotar totalmente (con su descendencia) el espacio de disco o memoria del sistema.  
La única función de este tipo de virus es crear clones y lanzarlos a ejecutar para que ellos hagan lo mismo. El propósito es agotar los recursos del sistema, especialmente en un entorno multiusuario interconectado, hasta el punto que el sistema principal no puede continuar con el procesamiento normal.

**Gusanos (Works)**Los gusanos utilizan las redes de comunicaciones para expandirse de sistema en sistema. Es decir, una vez que un gusano entra a un sistema examina las tablas de ruta, correo u otra información sobre otros sistemas, a fin de copiarse en todos aquellos sistemas sobre los cuales encontró información. Este método de propagación presenta un crecimiento exponencial con lo que puede infectar en muy corto tiempo a una red completa.

Existen básicamente 3 métodos de propagación en los gusanos:

1 - Correo electrónico - El gusano envía una copia de sí mismo a todos los usuarios que aparecen en las libretas de direcciones que encuentra en el ordenador dónde se ha instalado.

2 - Mecanismos basados en RPC (Remoto Procederé Cal) - El gusano ejecuta una copia de sí mismo en todos los sistemas que aparecen en la tabla de rutas (ropa y repercute).

3 - Mecanismos basados en RLOGIN - El gusano se conecta como usuario en otros sistemas y una vez en ellos, se copia y ejecuta de un sistema a otro.

**Backdoors:**Son también conocidos como herramientas de administración remotas ocultas. Son programas que permiten controlar remotamente el PC infectado. Generalmente son distribuidos como troyanos.  
Cuando un virus de estos es ejecutado, se instala dentro del sistema operativo, al cual monitorea sin ningún tipo de mensaje o consulta al usuario. Incluso no se le ve en la lista de programas activos. Los Backdoors permiten al autor tomar total control del PC infectado y de esta forma enviar, recibir archivos, borrar o modificarlos, mostrarle mensajes al usuario.

**Técnicas de protección del sistema de virus:**

¿Cómo se puede proteger un ordenador de los virus?

**Instale un programa antivirus.** Instalar un programa antivirus y mantenerlo actualizado puede ayudarle a defender el equipo frente a virus. Los programas antivirus analizan el equipo en busca de virus que pretenden introducirse en el correo electrónico, el sistema operativo o los archivos. Cada día pueden aparecer virus nuevos, por lo que es recomendable visitar con frecuencia el sitio web del fabricante en busca de actualizaciones. Algunos programas antivirus se venden con suscripciones anuales que pueden renovarse cuando es necesario, pero hay muchos que son gratuitos. Microsoft ofrece Microsoft Security Essentials, un programa antivirus gratuito que puede descargar desde el sitio web de [**Microsoft Security Essentials**](http://go.microsoft.com/fwlink/?LinkId=168949). También puede visitar el sitio web de [**los proveedores de software de seguridad de Windows**](http://go.microsoft.com/fwlink/?LinkId=135654) para buscar un programa antivirus de otro fabricante.

* **No abra mensajes de correo electrónico de remitentes desconocidos ni adjuntos de correos electrónicos que no reconoce.** Muchos virus se envían adjuntos a mensajes de correo electrónico y se propagan en cuanto se abre el archivo. Es mejor no abrir ningún archivo adjunto a menos que se trate de algo que está esperando. Microsoft Outlook y Windows Mail ayudan a bloquear archivos adjuntos potencialmente peligrosos.
* **Use un bloqueador de elementos emergentes en su explorador.** Las ventanas emergentes son ventanas pequeñas del explorador que se abren encima del sitio web que se está viendo. Si bien la mayoría de estas ventanas son creadas por anunciantes, también pueden contener código inseguro o malintencionado. Un bloqueador de elementos emergentes puede evitar que se abran algunas de estas ventanas o todas.

De forma predeterminada, la característica Bloqueador de elementos emergentes de Internet Explorer está activada. Para obtener más información sobre cómo cambiar la configuración de esta función o cómo desactivarla, consulte [**Bloqueador de elementos emergentes de Internet Explorer: preguntas más frecuentes**](http://windows.microsoft.com/es-mx/windows7/internet-explorer-pop-up-blocker-frequently-asked-questions).

* **Mantenga Windows actualizado.** Periódicamente, Microsoft publica actualizaciones de seguridad especiales que pueden ayudarle a proteger el equipo. Estas actualizaciones pueden evitar los virus y otros ataques informáticos solucionando posibles carencias de seguridad. Asegúrese de que Windows recibe estas actualizaciones activando la actualización automática de Windows. Para conocer de qué manera se hace, consulte [**Activar o desactivar las actualizaciones automáticas**](http://windows.microsoft.com/es-mx/windows7/turn-automatic-updating-on-or-off).
* **Use un firewall.** Firewall de Windows o cualquier otro firewall pueden alertarle de actividades sospechosas si un virus o un gusano intentan conectarse al equipo. También pueden bloquear virus, gusanos y piratas informáticos si intentan descargar programas potencialmente peligrosos en el equipo. Para obtener más información acerca del Firewall de Windows, consulte [**Descripción de la configuración de Firewall de Windows**](http://windows.microsoft.com/es-mx/windows7/understanding-windows-firewall-settings).
* **Use la configuración de privacidad del explorador.** Es importante saber cómo los sitios web pueden usar información privada para evitar la aparición de anuncios personalizados, fraudes y robos de identidad. Si está usando Internet Explorer, puede ajustar la configuración de Privacidad o restaurar la configuración predeterminada en cualquier momento que lo desee. Para obtener detalles, consulte [**Cambiar la configuración de privacidad de Internet Explorer**](http://windows.microsoft.com/es-mx/windows7/change-internet-explorer-privacy-settings).
* **Activar el Control de cuentas de usuario (UAC).** Cuando se vayan a realizar cambios en el equipo que requieran permiso de nivel de administrador, UAC se lo notificará y le dará la oportunidad de aprobar el cambio. UAC puede ayudar a evitar que los virus realicen cambios no deseados. Para obtener más información sobre cómo activar el UAC y ajustar la configuración, consulte [**Activar o desactivar el Control de cuentas de usuario**](http://windows.microsoft.com/es-mx/windows7/turn-user-account-control-on-or-off).
* **Borrar la memoria caché de Internet y el historial del explorador.** La mayoría de los exploradores almacena información sobre los sitios web que usted visita e información que los sitios web le pueden solicitar (como su nombre y dirección). Si bien puede ser útil tener esta información almacenada en el equipo, en algunas ocasiones, es posible que usted desee eliminarla de manera parcial o total, por ejemplo, cuando usa un equipo público y no desea dejar registro de su información personal. Para obtener información sobre cómo borrar el historial de Internet Explorer, consulte [**Eliminar historial de páginas web**](http://windows.microsoft.com/es-mx/windows7/delete-webpage-history) y [**Eliminar las cookies de Internet**](http://windows.microsoft.com/es-mx/windows7/delete-your-internet-cookies).