1. Introducción

En la actualidad las computadoras no solamente se utilizan como herramientas auxiliares en nuestra vida, sino como un medio eficaz para obtener y distribuir información. La informática está presente hoy en día en todos los campos de la vida moderna facilitándonos grandemente nuestro desempeño, sistematizando tareas que antes realizábamos manualmente.
Este esparcimiento informático no solo nos ha traído ventajas sino que también problemas de gran importancia en la seguridad de los sistemas de información en negocios, hogares, empresas, gobierno, en fin en todos los aspectos relacionado con la sociedad.
En este trabajo discutiré el tema de los virus, desde sus orígenes, sus creadores, la razón de su existencia entre otras cosas. El trabajo constará con descripciones de las categorías donde se agrupan los virus así como las diferencias de lo que es un virus contra lo que falsamente se considera virus.

También describiré los métodos existentes en el mercado para contrarrestar los virus como son los antivirus, la concienciación a los usuarios y las políticas de uso de las tecnologías en cuanto a seguridad y virus informáticos.

2. ¿Que es un Virus?

Desde hace muchos años los virus son la mayor amenaza para las computadoras siendo el causal mayor de pérdidas económicas en las empresas y el sector del gobierno. Un virus informático es una serie de instrucciones codificadas en un lenguaje de programación creadas intencionalmente e introducido en las computadoras sin el consentimiento del usuario. Su características principales son que se puede auto replicar, intentan ocultar su presencia hasta el momento de la explosión y causan efectos dañinos en donde son alojados. Si vemos bien esas características nos podemos dar cuenta que sus características son semejantes a las de un virus biológico, de ahí es que nace el nombre virus.
Estos programas malignos son capaces de alterar el funcionamiento correcto de las computadoras llegando a veces a provocar daños irreparables a los equipos o borrar información del disco duro.
Los virus informáticos ocupan un mínimo de espacio donde residen, hay que tener en cuenta que mientras más pequeño el programa más fácil será de pasar desapercibido. Los virus se ejecutan sin conocimiento del usuario y se dedican a copiarse e infectar todos los archivos, tablas de partición y sectores de arranque del disco duro y memoria.
Todos los virus son dañinos, siempre causan algún tipo de malestar donde son alojados. El daño no tan solo puede ser explícito, sino también implícito cuando lo que se busca es alterar o destruir información o crear un desempeño pobre en el funcionamiento de la computadora afectando el consumo de la memoria o el tiempo del procesador en repetir estas instrucciones malignas.

3. ¿Cómo nacieron los Virus?

La primera aclaración que hay que hacer es que los virus de computadoras, son simplemente programas, y como tales, hechos por programadores. Para crear los virus no hace falta tener capacitación especial ni una genialidad significativa, sino conocimientos de algún lenguaje de programación como por ejemplo: Ensamblador, C++, Delphi, PowerBasic, entre otros y el conocimiento de algunos temas que no son difundidos para el público en general.
A ciencia cierta es muy difícil determinar el momento exacto del nacimiento de los virus informáticos, pero mucha literatura menciona que fue para los años 60 que un grupo de programadores de los laboratorios Bell de AT&T crearon el juego "Core War" a escondidas de sus supervisores. El propósito del juego era crear un organismo cuyo hábitat fuera la memoria de la computadora, a partir de una señal cada programa intentaba forzar al otro a realizar una instrucción invalidad, ganando el primero que lo consiguiera. Cuando terminaban de jugar los programadores borraban todo tipo de rastro para que nadie se diera cuenta de lo que estaba

pasando ya que esta conducta era altamente reprendida por los supervisores.
Uno de los primeros registros de virus que se tienen son del 1987 cuando una firma Pakistaní introducía en los disquete que distribuía ilegalmente la firma de "ð Brain." La razón de esto era para darles un escarmiento a las personas que conseguían los programas ilegalmente. Ellos habían notado que el sector de arranque de un disquete contenía un código ejecutable y si se modificaban un par de instrucciones ahí iban a poder infectar todos los disquetes que se introdujeran ahí. Es en ese momento que se logran los primeros virus del sector de arranque.
En ese mismo año, un programador de nombre Ralf Burger creó las instrucciones que hicieron posible que un archivo se siguiera copiando solo a otros archivos y lo llamo Virdem el cual podía infectar cualquier archivo con extensión .COM.
Antes de la explosión de las micro computadoras lo que se hablaba de virus era muy poco, pero se puede decir que los virus tienen la misma edad que las computadoras, uno es función del otro. Antes el campo de las computadoras era el secreto de unos pocos. Mientras que por otro lado el gobierno, los científicos y militares que vieron como sus equipos eran infectados por virus se quedaban callados para no hacer pública la vulnerabilidad de sus sistemas que costaron millones de dólares al bolsillo de los contribuyentes. Tampoco las empresas privadas como los bancos o grandes corporaciones decían nada para no perder la confianza que sus clientes habían depositado en ellos. Es por esta razón que lo que se sabe de virus entre 1949 y 1989 es muy poco.
En 1983 el Dr. Ken Thomson, uno de los creadores del "Core Wars" rompe el silencio acordado y da a conocer la existencia del programa y los detalles de su estructura. En 1984 la revista Scientific American publica toda esa información y la guía de cómo fueron creados. Ese es el punto de partida de la gran proliferación de virus y su difusión sin control en las computadoras personales.
En 1987, los sistemas de correo electrónicos de la IBM fueron infectados por un virus que enviaba mensajes navideños y se multiplicaba con gran rapidez. Esto ocasionó que los discos duros de los servidores se llenaran rápidamente creando inconsistencias y lentitud en el sistema hasta llegar a tumbar los servidores por espacio de tres días.
Ya en 1989 la cantidad de virus detectados sobrepasaban los 100 y la epidemia comenzaba a causar grandes estragos. Entre las medidas que se tomaron para tratar de detener la proliferación de virus fue enjuiciar en Estados Unidos a Robert Moris Jr. acusado de ser el creador de un virus que afecto al gobierno y sectores de la empresa privada. Él a través de las instrucciones del juego Core Wars creó el virus y lo difundió entre sus amigos los cuales se encargaron de distribuirlo por diferentes medios a redes y equipos de computación. Al juicio se le dio gran publicidad, pero no detuvo a los creadores de virus.
Actualmente los virus son creados en cantidades extraordinarias por distintas personas alrededor del mundo. Muchos son creados por diversión, otros para probar sus habilidades de programación o para entrar en competencia con otras personas. En mi opinión creo que hay que investigar a las firmas desarrolladoras de antivirus ya que estas hacen mucha publicidad cuando detectan un virus y peor aún encuentran la solución rápida para que los usuarios o actualicen sus antivirus o compren el programa de ello.

4. Métodos de Infección

La propagación de los virus informáticos a las computadoras personales, servidores o equipo de computación se logra mediante distintas formas, como por ejemplo: a través de disquetes, cintas magnéticas, CD o cualquier otro medio de entrada de información. El método que más ha proliferado la infección con virus es las redes de comunicación y más tarde la Internet. Es con la Internet y especialmente el correo electrónico que millones de computadoras han sido afectadas creando perdidas económicas incalculables.
Hay personas que piensan que con tan solo estar navegando en la Internet no se van a contagiar porque no están bajando archivos a sus ordenadores pero la verdad es que están bien equivocados. Hay algunas paginas en Internet que utilizan objetos ¨ActiveX¨ que son archivos ejecutables que el navegador de Internet va ejecutar en nuestras computadoras, si en el active X se le codifica algún tipo de virus este va a pasar a nuestra computadoras con tan solo estar observando esa página.
Cuando uno esta recibiendo correos electrónicos debe ser selectivo en los archivos que uno baja en nuestras computadoras. Es mas seguro bajarlos directamente a nuestra computadora para luego revisarlos con un

antivirus antes que ejecutarlos directamente de donde están.
Un virus informático puede estar oculto en cualquier sitio. Cuando un usuario ejecuta algún archivo con extensión .EXE que es portador de un algún virus todas las instrucciones son leídas por la computadora y procesadas por esta hasta que el virus es alojado en algún punto del disco duro o en la memoria del sistema. Luego esta va pasando de archivo en archivo infectando todo a su alcance añadiéndole bytes adicionales a los demás archivos y contaminándolos con el virus. Los archivos que son infectados mayormente por los virus son tales cuyas extensiones son: EXE, COM, BAT, SYS, PIF, DLL, DRV.

5. Clasificación de los virus

La clasificación de los virus es un tanto confusa y se pueden recibir distintas respuestas dependiendo a quien se le pregunte. Podemos clasificarlos por el lugar donde se alojan como por ejemplo: sectores de arranque o archivos ejecutables, por su nivel de alcance en el ámbito mundial, por su comportamiento, por sus técnicas de ataque o simplemente por la forma en que tratan de ocultarse.
A continuación se presenta una clasificación de acuerdo a su comportamiento:

Caballo de Troya
Es un programa maligno que se oculta en otro programa legítimo. Posee subrutinas que permiten que se manifieste en el momento oportuno. No es capaz de infectar otros archivos y solo se ejecuta una vez. Se pueden utilizar para conseguir contraseñas y pueden ser programado de tal forma que una vez logre su objetivo se autodestruya dejando todo como si nunca nada hubiese ocurrido.

Camaleones
Son una variación de los Caballos de Troya, pero actúan como otros programas comerciales ganándose la confianza de uno. Estos virus pueden realizar todas las funciones de un programa legítimo además de ejecutar a la vez el código maligno que siempre cargan.

Poliformes o Mutantes
Encripta todas sus instrucciones para que no pueda ser detectado fácilmente. Solamente deja sin encriptar aquellas instrucciones necesarias para ejecutar el virus. Este virus cada vez que contagia algo cambia de forma para hacer de las suyas libremente. Los antivirus normales hay veces que no detectan este tipo de virus y hay que crear programas específicamente (como son las vacunas) para erradicar dicho virus.

Sigilosos o Stealth
Este virus cuenta con un módulo de defensa sofisticado. Trabaja a la par con el sistema operativo viendo como este hace las cosas y tapando y ocultando todo lo que va editando a su paso. Trabaja en el sector de arranque de la computadora y engaña al sistema operativo haciéndole creer que los archivos infectados que se le verifica el tamaño de bytes no han sufrido ningún aumento en tamaño.

Retro Virus
Son los virus que atacan directamente al antivirus que esta en la computadora. Generalmente lo que hace es que busca las tablas de las definiciones de virus del antivirus y las destruye.

Virus voraces
Alteran el contenido de los archivos indiscriminadamente. Este tipo de virus lo que hace es que cambia el archivo ejecutable por su propio archivo. Se dedican a destruir completamente los datos que estén a su alcance.

Bombas de tiempo
Es un programa que se mantiene oculto hasta que se den ciertas condiciones en especificas como por ejemplo una fecha o cuando se ejecuta una combinación de teclas en particular.

Gusano
Su fin es ir consumiendo la memoria del sistema mediante la creación de copias sucesivas de sí mismo hasta hacer que la memoria se llene y no pueda funcionar más.

Macro virus
Estos son los que más se están esparciendo por la red. Su máximo peligro es que funcionan independientes al sistema operativo y a decir mas no son programas ejecutables. Los macro virus están hechos en script o lenguajes de un programa como Word o Excel.

¿Que no se considera un virus?
Hay muchos programas que sin llegar a ser virus informáticos le pueden ocasionar efectos devastadores a los usuarios de computadoras. No se consideran virus porque no cuentan con las características comunes de los virus como por ejemplo ser dañinos o auto reproductores. Un ejemplo de esto ocurrió hace varios años cuando un correo electrónico al ser enviado y ejecutado por un usuario se auto enviaba a las personas que estaban guardados en la lista de contactos de esa persona creado una gran cantidad de trafico acaparando la banda ancha de la RED IBM hasta que ocasiono la caída de esta.
Es importante tener claro que no todo lo que hace que funcione mal un sistema de información no necesariamente en un virus informático. Hay que mencionar que un sistema de información puede estar funcionando inestablemente por varios factores entre los que se puede destacar: fallas en el sistema eléctrico, deterioro por depreciación, incompatibilidad de programas, errores de programación o "bugs", entre otros.

Falsas Alarmas
Hay veces que uno encuentra algún error en la computadora y uno siempre en lo primero que piensa es que tiene algún virus que esta infectando el sistema. Ahí es cuando uno actualiza el antivirus y lo ejecuta para comprobar si tiene o no algún virus, cuando uno se da cuenta que el antivirus no detecto nada es cuando nos damos cuenta que el error puede ser software o hardware.
Si los errores que vemos en el sistema caen bajo alguna de estas preguntas que voy a mencionar ahora puede ser catalogados como falsas alarmas. Puede ser una falsa alarma sí:
¿Es solo un archivo el que reporta la falsa alarma (o quizás varios, pero copias del mismo)?
¿Solamente un producto antivirus reporta la alarma? (Otros productos dicen que el sistema esta limpio)
¿Se indica una falsa alarma después de correr múltiples productos, pero no después de reiniciar, sin ejecutar ningún programa?

Virus Falsos ("HOAX")
Estos se distinguen porque crean gran cantidad de pánico al tratar de llegar a la mayor cantidad de personas comunicando la falsa existencia de supuestos virus que al fin y al cabo son archivos de nombres raros que utiliza el sistema operativo para su funcionamiento normal, si estos archivos son eliminados como casi siempre dicen las instrucciones de los hoax entonces vamos a crearles inconsistencias al sistema y este dejará de funcionar.
Cuando uno recibe ese tipo de correos uno no debe continuar la cadena del pánico rompiéndola de inmediato.

6. ¿Que es un antivirus?

Un antivirus es un programa de computadora cuyo propósito es combatir y erradicar los virus informáticos. Para que el antivirus sea productivo y efectivo hay que configurarlo cuidadosamente de tal forma que aprovechemos todas las cualidades que ellos poseen. Hay que saber cuales son sus fortalezas y debilidades y tenerlas en cuenta a la hora de enfrentar a los virus.
Uno debe tener claro que según en la vida humana hay virus que no tienen cura, esto también sucede en el mundo digital y hay que andar con mucha precaución. Un antivirus es una solución para minimizar los riesgos y nunca será una solución definitiva, lo principal es mantenerlo actualizado. Para mantener el sistema estable y seguro el antivirus debe estar siempre actualizado, tomando siempre medidas preventivas y correctivas y estar constantemente leyendo sobre los virus y nuevas tecnologías.

El antivirus normalmente escanea cada archivo en la computadora y lo compara con las tablas de virus que guarda en disco. Esto significa que la mayoría de los virus son eliminados del sistema después que atacan a éste. Por esto el antivirus siempre debe estar actualizado, es recomendable que se actualice una vez por semana para que sea capaz de combatir los virus que son creados cada día. También, los antivirus utilizan la técnica heurística que permite detectar virus que aun no están en la base de datos del antivirus. Es sumamente útil para las infecciones que todavía no han sido actualizadas en las tablas porque trata de localizar los virus de acuerdo a ciertos comportamientos ya preestablecidos.
El aspecto más importante de un antivirus es detectar virus en la computadora y tratar de alguna manera sacarlo y eliminarlo de nuestro sistema. Los antivirus, no del todo facilitan las cosas, porque al ellos estar todo el tiempo activos y tratando de encontrar virus al instante esto hace que consuman memoria de la computadoras y tal vez la vuelvan un poco lentas o de menos desempeño.
Un buen antivirus es uno que se ajuste a nuestras necesidades. No debemos dejarnos seducir por tanta propaganda de los antivirus que dicen que detectan y eliminan 56,432 virus o algo por el estilo porque la mayoría de esos virus o son familias derivadas o nunca van a llegar al país donde nosotros estamos. Muchos virus son solamente de alguna región o de algún país en particular.
A la hora de comprar un buen antivirus debemos saber con que frecuencia esa empresa saca actualizaciones de las tablas de virus ya que estos son creados diariamente para infectar los sistemas. El antivirus debe constar de un programa detector de virus que siempre este activo en la memoria y un programa que verifique la integridad de los sectores críticos del disco duro y sus archivos ejecutables. Hay antivirus que cubren esos dos procesos, pero si no se puede obtener uno con esas características hay que buscar dos programas por separado que hagan esa función teniendo muy en cuenta que no se produzca ningún tipo de conflictos entre ellos.
Un antivirus además de protegernos el sistema contra virus, debe permitirle al usuario hacer alguna copia del archivo infectado por si acaso se corrompe en el proceso de limpieza, también la copia es beneficiosa para intentar una segunda limpieza con otro antivirus si la primera falla en lograr su objetivo.

Detección y Prevención
Hoy en día debido a la sofisticación de los virus, es difícil percatarse de la presencia de estos por causas de pérdida de desempeño, pero hay que destacar que la mayoría de estos hacen que el sistema:

- Realice sus operaciones de procesamiento más lentas
- Los programas tardan mas en cargarse en memoria
- Los programas comienzan a acceder por momentos a la unida de discos flexibles y discos duros sin necesidad alguna
- Disminución sin motivos del espacio en disco duro y memoria de la computadora en forma constante y repentina
- Aparición de programas desconocidos en la memoria

Afortunadamente, las infecciones informáticas pueden ser prevenibles por el usuario. Con una buena combinación de sentido común unido a un buen antivirus se puede precaver a gran escala. Además se debe concienciar a los usuarios con políticas de seguridad en el uso del correo electrónico y otros programas que se bajan de Internet.
La política de seguridad del correo electrónico debe incluir algún párrafo informativo para adiestrar al usuario como el siguiente:
Los archivos adjuntos es la forma más común que es afectado un sistema de información. Hay que ejercer un cuidado extremo cuando se esta abriendo un archivo que acabamos de recibir. Nunca se debe abrir un archivo si no se sabe el lugar de procedencia y mucho menos si no tiene que ver con el trabajo. Antes de abrir el archivo se tiene que verificar con el antivirus. Si tiene alguna duda con respecto al archivo que le enviaron debe comunicarse con el personal de sistemas de información.
También la política debe incluir adiestramiento a los usuarios como medida preventiva a las infecciones. Los adiestramientos pueden ser secciones grupales, recordatorios de procesos o parte del adiestramiento, material de referencia.
Los adiestramientos deben ser cortos, al grano e interactivos donde se promulgue la participación por parte de

los usuarios e inquietarlos y concienciarlos con respectos al daño que ocasionan los virus. Los recordatorios deben ser memos enviados por el correo electrónico describiendo las mejores practicas para combatir los virus. Enviando documentos de los virus nuevos sus estragos y la forma de erradicarlo del sistema. Por ultimo el material de referencia puede ser información para actualizar el antivirus o comunicados que sacan las empresas creadoras de antivirus.
En las medianas empresas se requiere por lo menos dos tipos de antivirus, uno para el correo electrónico y otro para los clientes y servidores. Una buena practica es tener dos antivirus distintos ya que trabajan de distintas maneras. Tal vez mientras uno es bueno detectando nuevos virus el otro es bueno enviado actualizaciones recientes. En las empresas de muchas computadoras quizás cientos el antivirus debe estar centralizado para facilitar el trabajo de actualizaciones y de control de los virus que llegan al servidor manteniendo una bitácora de todo lo que ocurre en la red.
Los usuarios deben ser capacitados para guardar en lugares seguros sus archivos esenciales, borrar archivos adjuntos de los correos electrónicos que no representen seguridad, preparar discos de arranques, bloquear macro virus en las propiedades de los programas entre otras cosas.

Antivirus Comerciales
En el mundo de la informática existen varias empresas que se dedican a la fabricación de antivirus. Dichas empresas desde sus comienzos han tratado de crear unos sistemas estables que le brinden seguridad y tranquilidad a los usuarios. Día a día ellas tienen la encomienda de reconocer nuevos virus y crear los antídotos y vacunas para que la infección no se propague como plagas en el mundo de las telecomunicaciones. Entre los antivirus existente en el mercado se pueden mencionar:

- Panda Antivirus
- Norton Antivirus
- McAfee VirusScan
- Dr. Solomon's Tool Kit
- Esafe
- F−Prot
- IBM Antivirus
- PcCillin

Si se tiene la capacidad de invertir una cantidad de dinero se deben tener por lo menos dos antivirus. Uno que yo recomiendo mucho es el Norton Antivirus que al unirlo con el F−Prot y una buena política sobre virus me ha resuelto grandemente los problemas en la universidad.
Entre los virus que más fuerte han azotado a la universidad en los últimos dos años puedo mencionar:

- Sircam
- Code Red
- Nimda
- Magistr
- Melissa
- Klez
- LoveLetter

Seguridad versus Costo−Beneficio
El método que la Universidad utiliza para asegurar y proteger sus archivos, depende de la sensibilidad de los datos. Como ejemplo puedo decir que los datos que más protegidos y seguros que tiene el Recinto son los que tiene que ver con el Registrador, los de Contabilidad y los de Recursos Humanos. Estos servidores están bien protegidos con buenas políticas seguridad y especialmente de virus, mas los backup y copias de archivos se realizan diariamente.
Esto es así, por que sino el costo de proteger todas las computadoras de los usuarios individuales seria muy elevado y no seria justificable. Por eso a los usuarios o contactos que tiene la Oficina de Sistemas de

Información en cada edificio se le envía boletines informativos de cómo mantener un ambiente bastante seguro en sus computadoras, a la misma vez estos contactos tienen que hacerle llegar esa información que recibieron a los usuarios finales. El objetivo en concienciar a los usuarios a proteger sus archivos sensitivos de tal forma que si ocurre cualquier desgracia los archivos puedan ser rescatados en algún caso extremo de virus o de fallas en disco duro.
Puerto Rico no cuenta con una ley que regule los fraudes cibernéticos ni mucho menos que hable de virus informáticos, pero al ser un territorio de los Estados Unidos le aplica la Ley de 1994 sobre el Acta Federal de Abuso Computacional (18 U.S.C. Sec. 1030) que modifico el Acta de Fraude y Abuso Computacional de 1886.
Con la finalidad de eliminar los argumentos hipertécnicos acerca de que es y que no es un virus, la nueva acta proscribe la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, a los sistemas informáticos, a las redes, información, datos o programas. La nueva ley es un adelanto porque esta directamente en contra de los actos de transmisión de virus.

Aspectos Emocionales
La Comunidad Universitaria del Recinto ha sido afectada grandemente a causas de los virus informáticos que a diario atacan las diferentes computadoras del recinto. Esto ha sido así año tras año ya que los usuarios siempre están informando la presencia de virus en sus computadoras. Esto parece que es un problema que se le ha dedicado mucho tiempo pero que todavía le falta mucho más en lo que el personal de sistemas de información logran concienciar a la comunidad.
Cada vez que una persona pierde un trabajo en el cual le había dedicado una gran cantidad de horas en investigación o escritura se le ve en la cara la angustia, la preocupación y el stress para bregar con la situación. Es en ese momento que le preguntan al personal de sistemas de información si pueden recuperar el trabajo y al éste decirle que si tienen un backup o resguardo para hacerlo es que se dan cuenta que por no seguir unos métodos sencillos explicados en los boletines o información que se le hace llegar es que se dan cuanta que han perdido ese documento por el cual estaba esperando el supervisor o un profesor para otorgar una nota al estudiante.
Yo personalmente he visto como los ojos de algunas personas se vuelven un poco llorosos y afligidos cuando reciben el impacto de esa noticia. Es entonces cuando vienen los lamentos de porque no hice esto o porque no hice esto otro para asegurar el documento. Casi siempre las personas tratan de culpar a los de sistemas de información cuando suceden esos estragos pero no se dan cuenta que cada cual tiene una responsabilidad en su área de trabajo.
Hoy en día hay que contar con unos buenos sistemas de backup porque ya casi todo esta en formato digital y no impreso en papel que era un poco mas fácil a la hora de brindarle seguridad.

7. Reflexión

La ciencia con sus adelantos y creadora de facilidades a través de la tecnología; específicamente las computadoras; ha tenido una gran adopción tanto en las instituciones públicas y privadas como en el trabajo diario de cada persona. Se ha llegado al punto de realizar cualquier tipo de trabajo y entretenimiento a través de las comunicaciones que nos facilitan las computadoras. Además se ha sustituido el tipo de comunicación cara a cara por una comunicación totalmente cibernética. A través de la introducción de virus en los sistemas de información vemos como se pierde el valor de la sociedad y se entra a un mundo donde solo se refleja una crisis de valores.
A través del uso de las computadoras las personas llegan a un nivel de profesionalismo y creatividad mucho mayor, pero este supuesto nivel tambalea cuando un pequeño virus entorpece su obra. El uso de las computadoras crea en la persona un nivel de dependencia creando en este un sentido de impotencia ya que por lo general las personas solo conocen el funcionamiento básico de las computadoras y no se dan a la tarea de conocer el mantenimiento de estas máquinas.