UNIVERSIDAD TECNOLOGICA ISRAEL

Investigación, Análisis y Recomendaciones para usuarios que manejan Sistemas Operativos Windows, como forma de protección a fallos existentes en los accesos de seguridad.

Estudiante

Cristhian Gonzalo Tinoco López

Tutor

Ing. Pablo Tamayo

Cuenca-Ecuador

2011

CERTIFICADO DE RESPONSABILIDAD

Yo, Ing. Pablo Tamayo , certifico que el señor Cristhian Gonzalo Tinoco Lopez con C.C. No. 1803346400 realizo la presente tesis con el titulo “Investigación, Análisis y Recomendaciones para usuarios que manejan Sistemas Operativos Windows, como forma de protección a fallos existentes en los accesos de seguridad”, y que es autor intelectual del mismo, que es original , autentico y personal.

_____

Ing. Pablo Tamayo

ACTA DE CESION DE DERECHOS

Yo, Cristhian Gonzalo Tinoco Lopez, declaro conocer y aceptar la disposición de la Normativa de la Universidad Tecnológica Israel que en su parte pertinente textualmente dice: “Forma parte del Patrimonio de la Universidad la propiedad intelectual de las investigaciones, trabajos científicos o técnicos y tesis de grado que se realicen a través, o con el apoyo financiero, académico o institucional (operativo) de la Universidad”.

_____

Cristhian Gonzalo Tinoco Lopez

CERTIFICADO DE AUTORIA

Yo, Cristhian Gonzalo Tinoco Lopez con CC: 1803346400, declaro que soy autor intelectual del presente trabajo de tesis, que es original autentico y personal.

Todos los efectos académicos , legales que se desprendan de este trabajo de tesis son de mi exclusiva responsabilidad.

_____

Cristhian Gonzalo Tinoco Lopez

DEDICATORIA

La presente tesis de grado la dedico a mi Madre, la cual con toda su dedicacion, amor y apoyo hacia mi, por todo lo que ha significado poder cumplir esta meta, sin duda me ha dado las fuerzas necesarias y es un pilar fundamental al termino de esta etapa estudiantil.

AGRADECIMIENTO

Agradezco a todas las personas que de una u otra manera estuvieron involucradas en el desarrollo del presente trabajo, a mi familia por darme en todo momento su apoyo y comprensión, y de manera especial quiero agradecer al Ing. Pablo Tamayo por brindarme los conocimientos necesarios que sirvieron de guia para la culminación del presente trabajo de tesis.

RESUMEN

Cuando se habla de seguridad en un ambiente informatico el concepto para la mayoría de los usuarios no queda muy claro, y es por lo mismo que se desconocen los riesgos que implica tener un Sistema Operativo funcionando sin todas las medidas correctivas que nos ayuden asegurar nuestra informacion.

En primera instancia es importante hacer mención, que para el usuario común de un computador hacer uso de Windows de la forma como viene preconfigurado el Sistema Operativo es muy habitual y las vulnerabilidades que tenga el software pasan desapercibidas, sea en un sistema servidor como una versión de usuario final.

El siguiente trabajo de investigación se lo realiza dado la gran aceptacion que tiene por parte de la mayoría de usuarios, el uso del Sistema Operativo Windows como el sistema mas amigable que existe en el mercado hoy en dia, gracias a su interfaz con el usuario , en este estudio se realizara un análisis previo de conceptos y definiciones importantes que permitirán un entendimiento mejor de este sistema para luego determinar los tipos de vulnerabilidades y riesgos que puede estar expuesta la información manejada desde un ambiente de hogar como también el empresarial.

SUMARY

When it comes to security in a computer environment the concept for most users is not very clear, and therefore the unknown risks of having an operating system running without any corrective action that will help us secure our information .

In the first instance is important to mention that for the average user of a computer to use Windows comes pre-configured the way the operating system is very common and have the software vulnerabilities that go unnoticed, either in a server system as a version end user.

The following research work is done because it has the great acceptance by most users use Windows as the operating system more user-friendly system that exists in the market today, thanks to its user interface, in this study was to conduct a preliminary analysis of important concepts and definitions that will enable a better understanding of this system and then determine the types of vulnerabilities and risks that may be exposed to the information managed from a home environment as well as the business.

TABLA DE CONTENIDOS

CAPITULO I

INTRODUCCION

En la actualidad en nuestro medio la mayor parte de personas están acostumbrados al sistema operativo Windows, en sus diferentes versiones por tener una interfaz grafica amigable, y ser de fácil acceso ya que se lo puede obtener en nuestro medio de diferentes formas , quizás por falta de conocimientos o descuido se utiliza la plataforma sin seguir ciertas normas de seguridad, que garanticen su correcto y pleno funcionamiento, la investigación propuesta permitirá realizar un documento guía que ayude al usuario a mejorar el uso de la plataforma.

Para el desarrollo del tema se empleará el método de Investigación este, facilitara la búsqueda de información para el análisis de los fallos existentes en el sistema operativo Windows 7 y Windows Server 2008 logrando así el objetivo propuesto inicialmente.

Se lo realizara mediante un estudio que reflejé las vulnerabilidades existentes en el sistema operativo Windows 7 y Windows Server 2008, con esto determinar los beneficios y ventajas que conlleva seguir ciertas reglas y recomendaciones, que no se deben pasar por alto en cuanto a la seguridad de los datos se refiera.

1.1PLANTEAMIENTO DEL PROBLEMA

¿Ayudará la Investigación y Análisis acerca de los fallos de protección existentes en los Sistemas Operativos Windows 2008 y Windows 7, optimizar los recursos y brindar la confiabilidad necesaria en beneficio del usuario final?

1.2 ANTECEDENTES

La informática tal y como se le conoce hoy día, surgió a raíz de la II Guerra Mundial, en la década de los 40. En esos años no existía siquiera el concepto de "Sistema Operativo" y los programadores interactuaban directamente con el hardware de las computadoras trabajando en lenguaje máquina, el concepto de Sistema Operativo surge en la década de los 50 de aquí que el primer Sistema Operativo de la historia fue creado en 1956 para un ordenador IBM 704, y básicamente lo único que hacía era comenzar la ejecución de un programa cuando el anterior terminaba [1], de ahí en adelante sucederían varios acontecimientos que dieron como resultado en la década de los 80 el comienzo del uso de sistemas operativos como MacOS, Windows y Linux que son multitarea, multiusuario, multiplataforma los mismos serian instalados en computadoras personales, para facilitar los trabajos comunes demandados en la actualidad por la sociedad.

Por esta razón tener un computador sin las debidas seguridades implementadas, se convierte en un terminal con la puerta de acceso a incalculables y complejos caminos que conducen a la infiltración de vecinos o deseados[2], por el simple hecho de usar y compartir información en redes interconectadas entre sí, ya que no se conoce a ciencia cierta todo tipo de amenazas existentes y de lo frágil y vulnerable que pueden ser estas para los usuarios de un computador.

---

[1] http://www.torrealday.com.ar/articulos/articulo005.htm

[2] http://g0tr00t.files.wordpress.com/2010/02/el-huevo-del-cuco.pdf

1.2.1 CAUSA – EFECTOS

Los perjuicios económicos que se derivan del robo de datos, en cualquier ambiente informático son verdaderamente costosos, y muchas veces esta información es crucial y no reemplazable para el usuario, perjudicando no solo al involucrado sino también al entorno donde se desenvuelve.

1.2.2 PRONÓSTICO Y CONTROL DEL PRONOSTICO

Pronóstico:

La no corrección a tiempo de los fallos existentes en los accesos de seguridad en Windows, conllevara que los perjuicios ocasionados por este sean cada vez mayores, afectando así todo ambiente en donde se utiliza la informática como un medio de trabajo.

Control del Pronóstico:

Con el estudio realizado se pretende entregar al usuario común de un computador, los resultados en cuanto a lo expuesto que puede estar ante cualquier ataque y robo de información, sino se realiza los correctivos necesarios a tiempo.

1.3 FORMULACION DE LA PROBLEMÁTICA ESPECIFICA

1.3.1 PROBLEMA PRINCIPAL

¿Permitirá la realización de un estudio que reflejé las vulnerabilidades existentes en el sistema operativo Windows Server 2008 y Windows 7, determinar los beneficios y ventajas que conlleva seguir ciertas reglas y recomendaciones, que no se deben pasar por alto en cuanto a la seguridad de los datos se refiera?

1.3.2 PROBLEMA SECUNDARIO

¿Permitirá la realización de una investigación científica acerca de las vulnerabilidades presentes, en las versiones de Windows Server 2008 y Windows 7 recopilar toda la información necesaria, que sustente los peligros a los que puede estar expuesta nuestra información?

¿Permitirá el informe resultante de la investigación, mostrar las vulnerabilidades, más comunes presentes en las versiones de Windows Server 2008 y Windows 7?

¿Permitirá la elaboración de un documento modelo, mostrar la correcta implementación para asegurar la información en la versión del Sistema Operativo Windows 7?

1.4 OBJETIVOS

1.4.1 OBJETIVO GENERAL

Realizar un estudio que reflejé las vulnerabilidades existentes en el sistema operativo Windows tomando como referencia la versión para servidor Windows Server 2008, y la versión para el usuario domestico Windows 7 .

1.4.2 OBJETIVOS ESPECÍFICOS

-Realizar una investigación científica acerca de las vulnerabilidades presentes, en las versiones de Windows Server 2008 y Windows 7 para recopilar toda la información necesaria, que sustente los peligros a los que pueden estar expuesta nuestra información.

-Presentar un informe referente a las vulnerabilidades, más comunes presentes en las versiones de Windows Server 2008 y Windows 7.

-Elaborar un documento modelo que muestre la correcta implementación para asegurar la información en la versión del sistema Operativo Windows 7.

1.5 JUSTIFICACIÓN

1.5.1 TEÓRICA

El uso de sistemas operativos en la actualidad, es muy común en la sociedad ya que se encuentran presentes en todos los campos por lo

tanto debido al gran intercambio de información que se realiza en todos estos escenarios, es necesario el uso y manejo de una interfaz de software que brinde la confianza en cuanto al control y consistencia del acceso a la información.

1.5.2 METODOLÓGICA

Para el desarrollo del tema propuesto se recolectará datos, en base a investigación e información disponible en la web así mismo haciendo uso de herramientas de control y monitoreo que nos permitirán tener una visión global de cómo se encuentra la seguridad en nuestro sistema operativo se realizará las correcciones necesarias para su óptimo funcionamiento.

1.5.3 PRÁCTICA

El conocimiento de fallos existentes en los accesos de seguridad en un sistema operativo, por parte del usuario, ayudará en gran medida a contrarrestar el uso inadecuado del mismo brindando así mayor provecho de los recursos disponibles y asegurando la información.

CAPITULO II

MARCO DE REFERENCIA

Para el desarrollo del tema propuesto se recolectará datos, en base a investigación e información disponible en la web así mismo haciendo uso de herramientas de control y monitoreo, que nos permitirán tener una visión global de cómo se encuentra la seguridad en nuestro sistema operativo, la información recolectada se detalla a continuación de manera que se pueda tener un concepto mas detallado del tema tratado.

MARCO ESPACIAL

El siguiente proyecto de investigación se lo realizara apoyándose en la web y libros disponibles acerca del tema, para las pruebas se contara con una computadora de hogar.

MARCO TEMPORAL

El correspondiente trabajo se lo desarrollara en un periodo de 1 mes y medio.

01. Concepto de Sistema Operativo

Al Sistema Operativo se le conoce como el programa principal del computador donde corren las aplicaciones, también se lo puede definir como el software básico que provee una interfaz entre el usuario y el hardware del PC para el manejo del resto de programas, proveyendo aspectos básicos como:

- Un ambiente conveniente de trabajo.
- Uso eficiente del Hardware.
- Una adecuada distribución de los recursos.

El Sistema Operativo a través del tiempo ha sufrido una serie de cambios, que se los conoce como generaciones hasta convertirse en si lo que conocemos hoy en día como un Sistema Operativo, en cuanto al hardware los cambios son generalmente establecidos por los componentes utilizados, pasando por válvulas, transistores hasta llegar a los circuitos integrados, estos cambios substanciales se ven reflejados en costo, tamaño, consumo de energía y lo más notorio que es la velocidad y capacidad de procesamiento del computador.

02. Concepto de Seguridad

Es un medio de protección contra acceso no autorizado a la información, que se puede interpretar como una disciplina que se encargara de proteger la integridad y la privacidad de la información almacenada en un sistema informático.

Se considera como una disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático**.**

De todas formas, no existe ninguna técnica que permita asegurar la inviolabilidad de un sistema.

Un sistema informático puede ser protegido desde un punto de vista lógico a esto se le conoce como seguridad informática y será complementado con lo físico que esta generalmente a puertas, candados, sistemas de alarma etc.

Pero no constante al seguir todas las normas de seguridad los más vulnerable es el factor humano que puede verse comprometido por varios escenarios como descargas e instalación de programas dañinos, virus etc. Que ingresan al sistema operativo y causan daños y vulnerabilidades en los accesos de seguridad de la información.

03. Concepto de Fallos Informáticos

Son las Vulnerabilidades existentes en el Sistema Operativo, que provocan errores informáticos, debido a de la deficiencia que se ejecuta durante el proceso de creación de programas de computadora.

Un defecto de software, es el resultado de un fallo o deficiencia durante el proceso de creación de programas de computadora conocido generalmente como software.

Este fallo puede presentarse en cualquiera de las etapas del ciclo de vida del software aunque los más evidentes se dan en la etapa de desarrollo y programación.

04. Windows 7

Es la versión más reciente del Sistema Operativo Windows, desarrollada por la Corporación Microsoft.

Figura 1

Esta versión está diseñada para uso en computadores personales, orientada al uso domestico y de oficina, con equipos de escritorio, portátiles, tablet, netbooks y equipos media center.

Windows 7 fue concebido como una actualización incremental y focalizada en Windows Vista y su núcleo Windows NT 6.0 que es el software que constituye la parte más importante del sistema operativo, el cual es responsable de facilitar el acceso a los programas con gestión de hardware y recursos a través de los diferentes servicios de Windows, esto permitió mantener cierto grado de compatibilidad con aplicaciones y hardware en los que éste ya era compatible.

Una importante meta que se dio con Windows 7 es la mejora de su interfaz para volverla más accesible al usuario e incluir nuevas características que permitieran hacer tareas de una manera más fácil y rápida, al mismo tiempo que se realizarían esfuerzos para lograr un sistema más ligero, estable y rápido.

05. Desarrollo de Windows 7

El desarrollo de este sistema operativo comenzó inmediatamente después del lanzamiento de Windows Vista.

El 20 de julio de 2007 se reveló que ese sistema operativo era llamado internamente por Microsoft como la versión 7.

Hasta ese momento la compañía había declarado que Windows 7 tendría soporte para plataformas de 32 bits y 64 bits, aunque la versión para servidores que comparte su mismo núcleo Windows Server 2008.

Ya para el 7 de enero de 2009, se publico la primera versión beta.

El 9 de enero se habilitó brevemente al público general mediante descarga directa en la página oficial, por percances en la descarga, Microsoft cambió el límite de descargas inicial de 2,5 millones de personas como disculpa por el problema del retraso, y creó un nuevo límite que no sería numérico sino por fecha, hasta el 10 de febrero del 2009.

El 5 de mayo se liberó la versión Release Candidate que era la versión candidata para el lanzamiento final porque se consideraba que el 90% del mismo estaba completamente funcional esta versión se libero inicialmente en 5 idiomas, entre ellos el español.

Esta versión candidata estuvo disponible para descargar hasta el 20 de agosto de 2009.

El 24 de julio, los directivos de Microsoft anunciaron la finalización del proceso de desarrollo con la compilación de la versión RTM (Release To Market), destinada a la distribución final de Windows 7.

06. Escritorio Windows 7

El escritorio de Windows es el área de la pantalla principal más visible y notoria para el usuario la cual se ve después de encender el equipo e iniciar sesión en el Sistema Operativo.

Al igual que la parte superior de un escritorio real, sirve de superficie de trabajo, para la interacción del usuario con la maquina.

Al abrir los programas o las carpetas, estos elementos aparecen en el escritorio.

También se puede colocar elementos en el escritorio, por ejemplo, archivos y carpetas, estos pueden ser organizados a gusto del usuario.

El escritorio a veces se define de un modo más amplio para incluir la barra de tareas la misma se encuentra en la parte inferior de la pantalla.

La barra de tareas nos muestra a cada momento qué programas están ejecutándose y permite cambiar de uno a otro, además del apilamiento de programas o archivos del mismo formato, para una organización mejor en cuanto a la apariencia de la barra.

Además, incluye el botón Inicio generalmente representado por el logo de la versión de Windows, el cual puede usar para obtener acceso a los programas, las carpetas y la configuración del equipo.

07. Interfaz Windows 7

Windows 7 permite ahora la personalización del equipo, al guardar temas completos; que incluye color de ventanas, imágenes incluidas, conjunto de sonidos, e incluso protector de pantalla.

Entre las mejoras para este sistema operativo nombraremos las siguientes:

• La calculadora, que anteriormente sólo disponía funciones científicas y estándares en otras versiones ahora incluye funciones propias de programación y de estadística

• La barra lateral de Windows, o más conocida como Windows Sidebar, se ha eliminado; permitiendo que los gadgets, puedan ubicarse libremente en cualquier lugar del escritorio.

• Reproductor de Windows Media 12, Es el nuevo reproductor multimedios, que se incluye como estándar en las versiones de Windows 7.

A diferencia de sus otras versiones, deja de tener una ubicación fija para los controles más básicos, además de manejar formatos ajenos a la empresa, como MOV, MP4, xvid y divx, entre otros.

• Aero Peek que corresponde a las previsualizaciones de Windows Aero se han mejorado pasando a ser más interactivas y útiles.

Cuando se posa el ratón sobre una aplicación abierta éste muestra una pre visualización de la ventana, donde muestra el nombre, la pre visualización y la opción de cerrarla.

• Windows Flip 3D, es una función de Windows Aero que mejora la función Windows Flip, mostrando a través de un efecto en 3D a las ventanas actualmente abiertas permitiendo así una búsqueda entre varias ventanas de forma más rápida y eficaz, esta función se activa con la combinación de teclas Windows y Tab.

08. Compatibilidad de Windows 7

Las versiones cliente de Windows 7 fueron lanzadas en versiones para arquitectura 32 bits y 64 bits en las ediciones Home Basic, Home Premium, Professional y Ultimate.

No obstante, las versiones servidor de este producto fueron lanzadas exclusivamente para arquitectura 64 bits.

Esto significa que las versiones cliente de 32 bits aún soportan programas Windows 16 bits y MS-DOS.

Las versiones 64 bits incluyendo todas las versiones de servidor soportan tanto programas de 32 como de 64 bits.

09. Release Candidate Windows 7

Las versiones Release Candidate además que son versiones de prueba del sistema operativo final antes de su lanzamiento, son también versiones que tienen validez y fecha de expiración antes del lanzamiento de la versión final, para que el usuario pueda adquirir o actualizarse a su versión final.

Luego del término del periodo de prueba el usuario recibirá avisos sobre la expiración de la versión de RC en tres etapas.

A partir del 15 de febrero de 2010, el proceso de notificación de expiración comienza de la siguiente manera.

El usuario recibirá una notificación de expiración en el área de notificación en parte inferior derecha de la barra de tareas, una vez por día.

La notificación será similar a la siguiente ilustración:

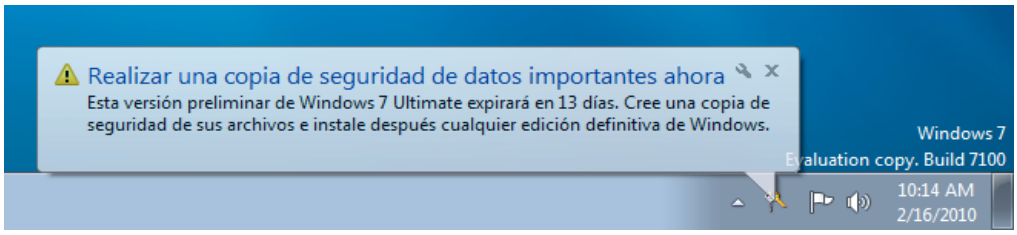


Figura 2

Luego de esto la notificación se hará visible una vez cada cuatro horas, luego una vez cada hora.

A partir del 1 de marzo de 2010, el Windows 7 RC entra en el próximo escenario de expiración.

Las notificaciones de expiración continuarán saliendo en el área de notificación.

El PC empezará a reinicializarse cada dos horas.

Las ventanas de los programas que esté utilizando al momento de reinicio, no guardarán su trabajo.

A partir del 1 de Junio de 2010, Windows 7 RC expira, el Windows inicia a un fondo de pantalla negro.

Se verá una ventana de activación de Windows, que dirá que la versión del Windows que se está utilizando no es genuina, y a partir de esto el usuario ya no podrá ingresar al sistema operativo.

La notificación será similar a la siguiente ilustración:

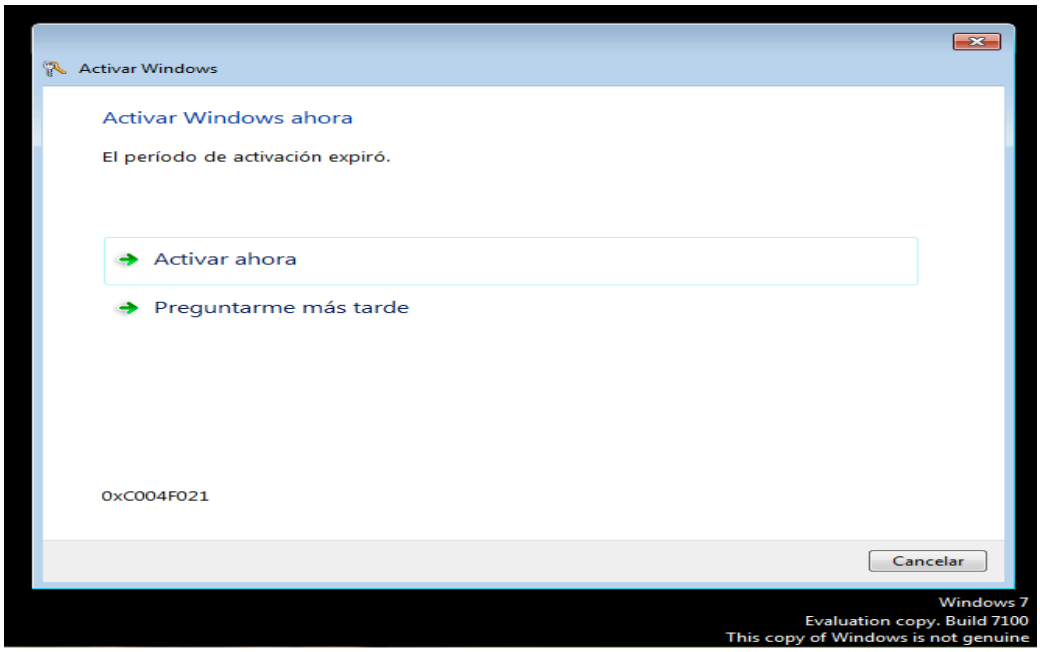


Figura 3

Para poder seguir utilizando Windows sino se quiere activar, también se puede optar por la opción de reinstalar a la versión previa de Windows, si se tiene el disco de instalación original.

Este reemplazará la versión Windows 7 RC con la versión de Windows que se estaba utilizando antes de que instalara el Windows 7, puede ser Vista, XP o cualquier otra distribución, la reinstalación a una versión anterior elimina todos los programas, archivos, y ajustes sobre la computadora así que se debe hacer una copia de seguridad de los archivos antes de que se realice este proceso.

10. Ediciones Finales de Windows 7

Existen seis ediciones de Windows 7, construidas una sobre otra de manera incremental, aunque solamente se centrarán en comercializar dos de ellas para el común de los usuarios: las ediciones Home Premium y Professional.

A estas dos, se suman las versiones Starter, Home Basic y Ultimate, además de la versión Enterprise, que está destinada a grupos empresariales que cuenten con licenciamiento Open o Select de Microsoft.

• Starter: Es la versión de Windows 7 con menos funcionalidades. Posee una versión incompleta de la interfaz Aero, está dirigida a PC de hardware limitado como netbooks, siendo licenciada únicamente para integradores y fabricantes OEM (Original Equipment Manufacturer) , esta versión implica que su venta está siempre ligada a un equipo nuevo, además de ser la única edición de Windows 7 sin disponibilidad de versión para hardware de 64 bits.

• Home Basic: Versión con más funciones de conectividad y personalización, aunque su interfaz seguirá siendo incompleta como en la edición Starter. Sólo estará disponible para integradores y fabricantes OEM en países en vías de desarrollo y mercados emergentes.

• Home Premium: Además de lo anterior, se incluye Windows Media Center, el tema Aero completo y soporte para múltiples códecs de formatos de archivos multimedia.

Disponible en canales de venta minoristas como librerías, tiendas y almacenes de cadena.

• Professional: Equivalente a Vista Business, pero ahora incluirá todas las funciones de la versión Home Premium más la Protección de datos con Copia de seguridad avanzada.

Además del uso de red administrada con soporte para dominios, impresión en red localizada y cifrado de archivos.

También disponible en canales de venta al público.

• Enterprise: Añade sobre la edición Professional de Windows 7, características de seguridad y protección de datos como BitLocker en discos duros externos e internos, soporte a imágenes virtualizadas de discos duros y el paquete de opción multilenguaje, únicamente se vende por volumen bajo contrato empresarial Microsoft.

• Ultimate: Esta edición es igual a la versión Enterprise pero sin las restricciones de licenciamiento por volumen, permitiéndose su compra en canales de venta al público general, aunque Microsoft ha declarado que en lugar de publicitarse en medios comunes, será ofrecida en promociones ocasionales de fabricantes y vendedores.

• Ediciones N: Las ediciones N están disponibles para actualizaciones y nuevas compras de Windows 7 Home Premium, Professional y Ultimate.

Las características son las mismas que sus versiones equivalentes, pero no incluyen Windows Media Player. El precio también es el mismo, ya que Windows Media Player puede descargarse gratuitamente desde la página de Microsoft.

11. Windows Server 2008

Windows Server 2008 es el nombre de un sistema operativo de Microsoft diseñado para servidor.

Figura 4

Es el sucesor de Windows Server 2003, distribuido al público casi cinco años antes.

Al igual que Windows Vista, Windows Server 2008 se basa en el núcleo Windows NT 6.0. este nucleo es el software que constituye la parte más importante del sistema operativo, el cual es responsable de facilitar el acceso a los programas con gestión de hardware y recursos a través de los diferentes servicios de Windows, esto permitió mantener cierto grado de compatibilidad con aplicaciones y hardware en los que éste ya era compatible.

Windows Server 2008 proporciona a los profesionales informáticos más control sobre sus servidores e infraestructura de red permitiéndoles centrarse en las necesidades críticas del negocio.

Mejoras ofertadas por esta versión permite automatizar tareas comunes facilitando las tareas de administrar y proteger las múltiples funciones de servidor en una empresa.

Incluye innovaciones de seguridad, como PatchGuard, que reducen la exposición a ataques del núcleo, lo que produce un entorno de servidor más seguro y estable.

12. Desarrollo Windows Server 2008

Fue conocido como Windows Server Longhorn hasta el 16 de mayo de 2007, cuando Bill Gates, presidente de Microsoft, anunció su título oficial Windows Server 2008.

El Windows Aero está deshabilitado y usa la interfaz clásica de versiones anteriores de Windows.

La beta 1 fue lanzada el 27 de julio de 2005.

La beta 2 fue anunciada y lanzada el 23 de mayo de 2006.

La beta 3 fue lanzada al público el 25 de abril de 2007.

Su lanzamiento fue el 27 de febrero de 2008.

Posteriormente se lanzó una segunda versión, denominada Windows Server 2008 R2 que trae mejoras y actualizaciones para el Sistema Operativo Servidor.

13. Escritorio Windows Server 2008

En Windows Server 2008, las funciones del escritorio comunes de versiones anteriores son posibles como tareas simples de crear carpetas, organizar archivos etc.

Sin embargo por defecto se encuentra desactivada la caracterisitica de experiencia de usuario, por lo tanto, si al momento de instalar el sistema tenemos un escritorio clasico de Windows, podemos seguir unos pasos para tener un escritorio con el tema Aero activado, para ello realizaremos lo siguiente:

- Abrir el Administrador del Servidor
- Buscamos la opcion del Menu para Administrar el Servidor
- Abrimos características y damos click en Agregar nueva caracteristica
- Seleccionamos Experiencia de Usuario
- Le damos Siguiente y luego Instalar.

Terminada la instalacion tendremos que reiniciar el sistema, una vez terminado de reiniciar se levanta el servicio automaticamente y estara listo el tema Aero.

Con esto, ya podremos ir a personalizar el escritorio y elegir el tema que mayor se adapte a nuestra necesidad y sea de nuestro agrado.

14. Interfaz Windows Server 2008

La interfaz de Windows Server 2008, con respecto a su versión anterior Server 2003 tiene grandes cambios ya que permite la personalización ,

gracias a que su interfaz esta basada en Windows Vista , que hace uso de la activación y manejo de la funcion Aero de Windows, lo cual hace que la experiencia , por parte del usuario sea mas aceptable en cuanto a la administración y personalización del sistema servidor , en comparación con versiones anteriores.

15. Compatibilidad Windows Server 2008

El sistema operativo Microsoft Windows Server 2008 proporciona increíbles niveles de rendimiento, confiabilidad y escalabilidad, además compite con los sistemas UNIX que es un sistema operativo multitarea y multiusuario, lo cual significa que puede ejecutar varios programas simultáneamente.

Windows Server 2008 para sistemas basados en Itanium que es un microprocesador Intel que utiliza la informática del conjunto de instrucciones explícitamente en paralelo y de 64 bits, está diseñado para cargas de trabajo de base de datos escalables, así como para aplicaciones tanto personalizadas como de línea de negocio.

Después de migrar un sistema que ejecuta una versión de Windows Server 2003 basada en Itanium a Windows Server 2008 para sistemas basados en Itanium, la mayoría de las aplicaciones deberá funcionar adecuadamente.

Casi todas las aplicaciones son compatibles con versiones anteriores, lo cual permite agregar cada vez más funcionalidades nuevas a las aplicaciones existentes, admite la funcionalidad del lado cliente para las herramientas de servidor y administración.

La migración de servicios o aplicaciones de sistemas basados en Itanium a sistemas con procesadores de 64 bits es similar a la

migración de un servicio o aplicación hospedado en una versión anterior de un sistema operativo a otra más actual, como, por ejemplo, migrar de Microsoft Windows 2000 Server a Windows Server 2003.

16. Release Candidate Windows Server 2008

La primera de la versión Release Candidate de Windows Server 2008, fue liberada para la descarga con cuatro variantes del Sistema Servidor como la Standard Edition, Enterprise, Datacenter, y también la RC 2008 Windows Web Server.

Un importante complemento para Windows Server 2008, RC, es el hecho que Microsoft haya incluido también la primera versión pública de Windows Server Virtualization utilizado para la ejecución de maquinas virtuales dentro del sistema operativo servidor.

Por primera vez Windows Server Virtualization va a formar parte del código base y disponible para todos los usuarios.

Con esto las organizaciones puedan iniciar las pruebas de virtualización con escenarios, como la consolidación de servidores como así como preparar para muchas de las demás características clave de Windows Server 2008.

Microsoft subraya el hecho que Windows Server 2008 haya finalizado la fase Beta 3, pero la versión Release Candidate es una indicación segura de que la compañía dispone su último sistema operativo servidor de 32 bits.

Windows Server 2008 inicialmente se planeo liberar a finales de 2007.

Microsoft no pudo realizar esa promesa e inserta la fecha en el RTM (Release To Market) colocándola en el primer trimestre de 2008.

El nuevo Windows Server 2008, fue lanzado oficialmente a finales de febrero 2008.

17. Ediciones Finales Windows Server 2008

La mayoría de las ediciones de Windows Server 2008 están disponibles en x86-64 conocida como versión de de 64 bits y x86 versión de 32 bits. Windows Server 2008 para sistemas basados en Itanium soporta procesadores IA-64 que es una arquitectura de intel desarrollada para versiones de 64 bits.

La versión IA-64 se ha optimizado para escenarios con altas cargas de trabajo como servidores de bases de datos y aplicaciones de línea de negocios.

Por ende no está optimizado para su uso como servidor de archivos o servidor de medios.

Microsoft anuncio que Windows Server 2008 será el último sistema operativo para servidores disponible en 32 bits.

Windows Server 2008 está disponible en las siguientes ediciones:

- Windows Server 2008 R2 Foudation (Solo 64Bit)
- Windows Server 2008 Standard (32 y 64 bits)
- Windows Server 2008 Enterprise (32 y 64 bits)
- Windows Server 2008 Datacenter (32 y 64 bits)
- Windows Web Server 2008 (32 y 64 bits)
- Windows HPC Server 2008 (Solo 64Bit)
- Windows Storage Server 2008 (32 y 64 bits)

CAPITULO III

METODOLOGIA

3.1.Marco Teórico Referencial

La metodología es el estudio sistemático y operacional de los métodos utilizados en la investigación científica, en sus diferentes áreas del saber humano y lograr perfeccionar la inteligencia creadora.

La metodología de la investigación nos permite engrandecer nuestros conocimientos de la naturaleza, de la sociedad y del hombre utilizando los métodos adecuados en la investigación.

3.1.1. Método Deductivo

La deducción es un proceso discursivo y descendente, pasa de lo genera a lo particular, esta se la puede considerar, como una demostración lógica donde necesariamente se la puede relacionar como una inferencia mediata o silogismo.

3.1.2. Método Analítico

El método analítico consiste en la desmembración de un todo, descomponiéndolo en sus partes o elementos para observar las causas, la naturaleza y los efectos. El análisis es la observación y examen de un hecho en particular. Es necesario conocer la naturaleza

del fenómeno y objeto que se estudia para comprender su esencia. Este método nos permite conocer más del objeto de estudio, con lo cual se puede: explicar, hacer analogías, comprender mejor su comportamiento y establecer nuevas teorías.

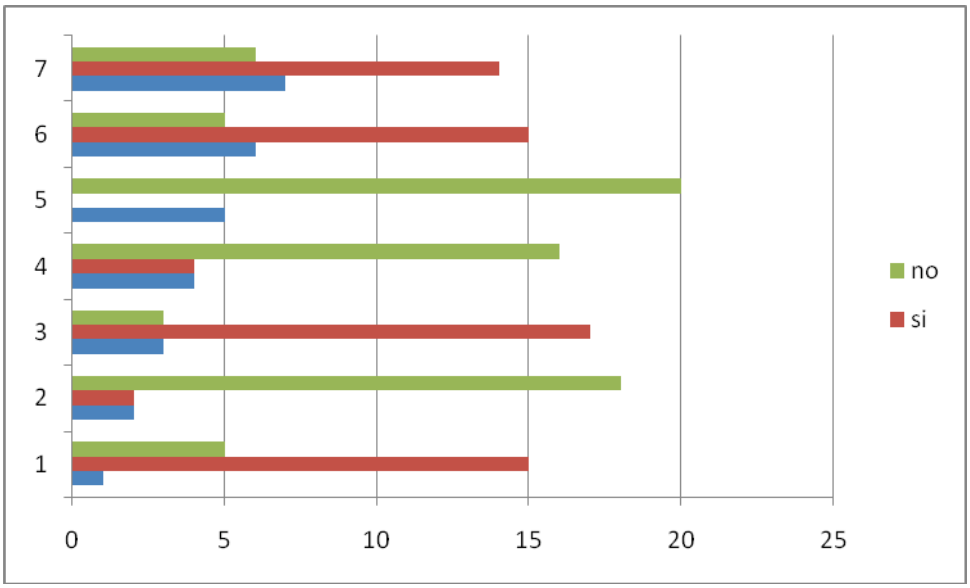
3.1.3.Técnicas.

Encuesta.- La encuesta es una técnica destinada a obtener datos de varias personas cuyas opiniones impersonales interesan al investigador. Para ello, a diferencia de la entrevista, se utiliza un listado de preguntas escritas que se entregan a los sujetos, a fin de que las contesten igualmente por escrito. Ese listado se denomina cuestionario.

Es impersonal porque el cuestionario no lleve el nombre ni otra identificación de la persona que lo responde, ya que no interesan esos datos.

Análisis del problema

Para una correcta investifgacion es necesario realizar el análisis adecuado del problema, por lo que se creyó conveniente realizar una breve encuesta que nos ayude a aclarar los inconvenientes mas comunes por parte del usuario al usar windows.



Ver detalle de encuentas en Anexo 1

Requerimientos técnicos

Para la investigación de campo , en la realizacion del siguiente proyecto consideraremos como requisito minimo lo siguiente.

- Computador con sus periféricos primordiales (teclado,mouse, pantalla)
- Distribución del Sistema operativo Windows 7
- Conexión a Internet

INVESTIGACION CIENTIFICA ACERCA DE LAS VULNERABILIDADES PRESENTES, EN LAS VERSIONES DE WINDOWS SERVER 2008 Y WINDOWS 7.

El Análisis para recopilar datos relevantes que hagan referencia a la investigación planteada, se la realizara atraves de consultas en la web y libros disponibles del tema, haciendo uso del tipo de investigación experimental asi mismo se empleara el método inductivo deductivo que permitirá organizar los datos obtenidos, conforme a la realidad existente en cuanto al uso normal del computador por la mayor parte de usuarios, con la técnica de recolección de datos.

Mediante la recolección de información disponible en la web, podemos encontrar los errores más comunes que provocan las vulnerabilidades presentes en los sistemas operativos Windows 7 y Windows server 2008 cuales son los temas para nuestra investigación, proseguiremos describiendo más a fondo cada versión así como sus características más sobresalientes, detallando cada una de sus ventajas y desventajas para al final hacer comparaciones relevantes que ayuden a solventar el tema propuesto.

01. Características de Windows 7

Windows 7 incluye varias características nuevas que ayudan a que la experiencia del usuario al manejar este sistema, sea más confortable y de fácil manejo como mejoras podemos destacar las siguientes:

- El reconocimiento de escritura a mano

- Soporte para discos duros virtuales
- Rendimiento mejorado en procesadores multinúcleo
- Mejor rendimiento de arranque y en su núcleo principal
- Nueva versión de Windows Media Center
- Paint, Wordpad y Calculadora rediseñadas
- Asistente para calibrar el color de la pantalla
- Calibrador de texto
- Administrador de credenciales
- Jump Lists guarda una lista de los archivos abiertos recientemente.

Abrir documentos recientes de Office, abrir pestañas recientes de Internet Explorer, escoger listas de reproducción en el reproductor, cambiar el estado en Windows Live Messenger etc., todas estas tareas hacen posible la nueva característica Jump Lists.

El Centro de seguridad de Windows cambio de nombre a Centro de actividades, y se integraron las categorías de seguridad y el mantenimiento del equipo en el.

La barra de tareas fue rediseñada, haciéndola más ancha, y los botones de las ventanas ya no traen texto, sino únicamente el icono de la aplicación.

En esta nueva versión no se incluye programas como Windows Mail, Windows Movie Maker y Windows Photo Gallery los mismos si desea el

usuario están disponibles para su descarga en el paquete de Windows Live Essentials.

02. Requisitos de Hardware Windows 7

Requisitos de hardware mínimos recomendados para Windows 7		
Arquitectura	32 bits	64 bits
Procesador	1 GHz	
Memoria RAM	1 GB de RAM	2 GB de RAM
Tarjeta gráfica	Dispositivo de gráficos DirectX 9	
Disco duro	16 GB de espacio libre	20 GB de espacio libre
Unidad óptica	DVD-R	

Figura 5

03. Actualizaciones Windows 7 (Service Pack)

El primer Service Pack SP1 de Windows 7 que son actualizaciones del sistema operativo, fue anunciado por primera vez el 18 de marzo de 2010.

Más adelante ese año, el 12 de julio, se publicaría una versión beta del service pack.

Microsoft confirmó que dicho service pack tendría poca trascendencia en comparación con otros service packs disponibles para versiones anteriores de Windows, particularmente Windows Vista.

Por lo que este service pack corrige únicamente algunos errores y problemas de seguridad encontrados anteriormente en la versión RTM de Windows 7 y mejora la estabilidad y rendimiento del sistema.

Para el 26 de octubre de 2010, Microsoft publicó de manera oficial una versión Release Candidate del Service Pack 1 de Windows 7.

El 22 de febrero de 2011, Microsoft publicó la versión terminada y final RTM del Service Pack 1 para Windows 7, se hizo disponible de forma generalizada para ser descargado desde la página de descargas de Microsoft, así como también mediante el servicio de actualizaciones automáticas Windows Update.

Service Pack 1 de Windows 7 incluye actualizaciones de seguridad, rendimiento y estabilidad para el sistema operativo, también incluye nuevas mejoras a las características y los servicios , como una mejor confiabilidad al conectar dispositivos de audio HDMI, imprimir mediante el visor de XPS y restaurar carpetas anteriores en el Explorador de Windows después de reiniciar.

04. Release Candidate Windows 7

La versión Release Candidate , es la versión previa al lanzamiento final del sistema operativo, la misma incorpora nuevas funcionalidades y mejoras a las ya presentes en la versión beta inicialmente puesta a prueba por la corporación Microsoft, dentro de las características más sobresalientes de la versión Release Candidate de Windows 7 enumeraremos las más destacadas.

- **Direct Access:** Permite a los responsables de TI Tecnología de la Información dotar a los usuarios móviles de un acceso fiable y seguro a los recursos disponibles en la red corporativa, sin tener que iniciar una conexión de Red Privada Virtual, esto ayuda aumentar la productividad en una empresa, esta funcionalidad requiere como mínimo el uso del sistema Windows 7 como cliente y Windows Server 2008 R2 como servidor.

- **BranchCache:** Permite reducir el tiempo empleado por los usuarios de las oficinas, sucursales etc. Para la descarga de archivos desde servidores remotos, gracias a la memorización de las rutas de accesos previos.

- **Búsqueda Federada en Windows 7:** Permite que se encuentre la información más fácilmente entre múltiples fuentes de datos, tales como sitios basados en SharePoint para poder iniciar la búsqueda desde Internet Explorer.

- **BitLocker:** Garantiza la protección de la información sensible de los usuarios independientemente del tipo de dispositivo que empleen, ofreciendo una estructura basada en reglas para especificar qué aplicaciones están disponibles y para qué usuarios finales, reduciendo el riesgo de exposición creado por las aplicaciones no autorizadas que se utilizan en las empresas.

- **Servicio de Inventario de Activos:** Permite mejorar las capacidades de cumplimiento de normativas, dotando de una visión global y completa del entorno corporativo mediante un inventario avanzado de software.

• **Compatibilidad con versiones anteriores:** El 90% de las aplicaciones empresariales desarrolladas sobre Windows Vista que han sido testadas corren perfectamente en Windows 7.

• **Virtualización de Windows XP:** Otra de las novedades es el XP Mode y Windows Virtual PC, que permiten a las pequeñas y medianas empresas ejecutar aplicaciones Windows XP directamente desde Windows 7 esta funcionalidad está disponible para usuarios de Windows 7 Professional y Windows 7 Ultimate, como descarga o directamente preinstalado en nuevos PCs.

• **Mejora de los procesos productivos:** La RC de Windows 7 hace la gestión y el despliegue de los escritorios, portátiles y entornos virtuales más sencillos, ayudando a automatizar la gestión del entorno del PC y liberando recursos, en beneficio del optimo desempeño del sistema.

05. Ediciones Finales Windows 7

Windows 7 está disponible en 6 diferentes versiones, de las cuales tres serán más comercializadas para el uso domestico Home Premium, Professional y Ultimate**.**

Las otras ediciones están enfocadas a mercados, tales como el del desarrollo o uso empresarial.

Cada versión de Windows 7 incluirá todas las funcionalidades de la versión inmediatamente inferior.

Excepto Windows 7 Starter, que es la versión más básica y económica de las versiones disponibles, todas las versiones soportarán tanto arquitectura 32-bit como 64-bit.

Los precios de las licencias fluctúan entre 200 y 350 dolares.

Aquí una pequeña descripción acerca de las funcionalidades que trae incorporada cada versión:

Windows 7 Starter:

La versión con menos características incluidas no posee Windows Aero, no dispone de la variante de 64-bit, y solo viene preinstalada por el fabricante del computador, lo que hace imposible su compra en cualquier tienda por parte del usuario.

Windows 7 Home Basic:

Esta versión se encuentra disponibles en países con economías emergentes tales como Bangladesh, Brasil, República de China, India, Indonesia, Méjico, Pakistán, Filipinas y Tailandia, algunas opciones del interfaz Aero están eliminadas.

Windows 7 Home Premium:

Esta edición contiene las funcionalidades más utilizadas en los hogares por usuarios no profesionales, tales como Windows Media Center, Windows Aero y controles para pantallas táctiles.

Windows 7 Professional:

Esta edición está dirigida a entusiastas de la tecnología y a pequeños negocios.

Además de todas las funcionalidades de Windows 7 Home Premium, incluye el uso del Dominio de Windows, Escritorio Remoto, Encriptación de archivos y el modo de Windows XP.

Windows 7 Enterprise:

Esta edición será vendida a las empresas que tienen con Microsoft un contrato de Licensamiento de Software.

Las funcionalidades adicionales son: Interfaz de Usuario Multilenguaje, Encriptación del Disco y soporte a aplicaciones UNIX.

Windows 7 Ultimate

Esta edición contiene todas las características de Windows 7 Enterprise pero se diferencia que esta edición estará disponible para los ordenadores de los hogares para usuarios en forma de una licencia individual por cada PC.

TABLA COMPARATIVA DE LAS VERSIONES WINDOWS 7

Versión	**Starter**	**Home Basic**	**Home Premium**	**Professional**	**Enterprise**	**Ultimate**
	Licencia OEM	Mercados emergentes	Tiendas y licencias OEM		Licencias contrato	Tiendas y licencia OEM
32-bit and 64-bit	Solo 32-bit	Ambas	Ambas	Ambas	Ambas	Ambas
Máximo CPU Soportados	1	1	1	2	2	2
Grupo de Trabajo	Solo unirse	Solo unirse	Si	Si	Si	Si
Centro de Recuperación	No	No	No	Si	Si	Si

Monitores Múltiples	No	Si	Si	Si	Si	Si
Centro Windows Mobility	No	Si	Si	Si	Si	Si
Windows Aero	No	Parcial	Si	Si	Si	Si
Multi-Touch	No	No	Si	Si	Si	Si
Windows Media Center	No	No	Si	Si	Si	Si
Sistema de Encriptación	No	No	No	Si	Si	Si
Escritorio Remoto	No	No	No	Si	Si	Si
Modo de Presentación	No	No	No	Si	Si	Si
Unirse al dominio	No	No	No	Si	Si	Si
BranchCache	No	No	No	No	Si	Si
DirectAccess	No	No	No	No	Si	Si
Subsistema para aplicaciones Unix	No	No	No	No	Si	Si
Paquete de Interfaz Multilenguaje	No	No	No	No	Si	Si

Figura 6

06. Boletines de Seguridad Windows 7

Dentro de las vulnerabilidades que se pueden presentar en los sistemas operativos, sea cual sea su versión y fabricante ya que ningún programa o software esta libres de errores, los mismos que causan inconvenientes al momento de trabajar con ellos y representan una

perdida de tiempo y dinero en cualquier ámbito informatico que se presentaren, por parte de la investigación propuesta Microsoft publica cada cierto tiempo las que más repercusiones y sobresalientes considera a continuación se detalla unos boletines publicados por dicha empresa.

06.1. Vulnerabilidad presente en protocolo SMB

Microsoft ha anunciado que ya está trabajando para solucionar la vulnerabilidad detectada en el protocolo utilizado para compartir archivos en Windows 7, el Server Message Block SMB.

Esta vulnerabilidad, que podría activarse a través de Internet Explorer, provocaría que el atacante bloquease el kernel, ya que no tendría problemas de saltarse el filtro firewall.

Aún no se dispone de un parche para reparar dicho problema sin embargo, Microsoft ha recomendado a los clientes que bloqueen los puertos TCP 139 y 445.

06.2. Vulnerabilidad en todas las versiones de Windows

Una vulnerabilidad recientemente publicada pone en peligro a cualquier usuario de Windows, sea cual sea su versión desde NT a Windows 7.

Dicho problema permite escalar privilegios actuar con permisos de sistema, el mayor grado de permiso bajo Windows.

Al parecer solo afecta a sistemas de 32 Bits, por lo que si se usa 64 en teoría se puede estar tranquilo.

El problema surge debido a una función que se ha ido heredando, llamada virtual DOS machine.

Lo peor de esto es que en Microsoft estaban informados desde Junio de 2009 y hasta el momento no existe ningún parche final que pueda solucionar este inconveniente.

06.3. Vulnerabilidad en Archivos Graficos

La explotación del grave agujero de seguridad de Windows que puede ser propagado mediante correo electrónico y mensajería instantánea, es extremadamente crítica, debido a que puede ser explotada incluso en sistemas Windows 7 totalmente actualizado.

Mediante la ejecución de los archivos WMF, Metarchivo de Windows, que contienen información que describe otro archivo, los intrusos pueden instalar código maligno en un sistema y vulnerarlo.

Al cambiar el nombre de la raíz de un archivo WMF por GIF o JPG, y enviarla como anexo en un mensaje de correo electrónico o en un diálogo de mensajería instantánea, es posible infectar un PC sin que el usuario siquiera haya visitado un sitio maligno en Internet, por lo que es posible que el código entre al sistema sin ser detectado ni por software antivirus ni por cortafuegos.

06.4. Desbordamiento de Buffer

Se ha descubierto una vulnerabilidad de desbordamiento de búfer en el componente Windows Redirector que puede permitir a un atacante local elevar sus privilegios.

El Windows Redirector se utiliza como un cliente Windows para el acceso a archivos tanto locales como remotos sin tener presente los protocolos de red en su uso.

Al parecer, esta aplicación utiliza un búfer para recibir información que no es comprobado debidamente.

La explotación de esta vulnerabilidad, mediante el envío de datos especialmente manipulados podría permitir que un atacante provocase la caída del sistema, o incluso ejecutase código arbitrario en él.

07. Conclusiones Sistema Operativo Windows 7

Como conclusiones generales tenemos:

- Esta ultima versión lanzada por la empresa Microsoft , para uso de hogares y oficina, tiene grandes cambios en cuanto a la personalización de su interfaz grafica, haciéndola de mas aceptación para el usuario, en comparación de sus versiones anteriores.

- La protección de la información, mejora notablemente con el sistema de encriptacion ya incorporado en algunas versiones.

- Al igual que otras versiones es necesario para incrementar la seguridad, en contra de ataques a la integridad del sistema, seguir ciertos parametros establecidos por la corporación Microsoft como lo son mantener los equipos debidamente actualizados en cuanto a parches , antivirus y service pack.

08. Características Windows Server 2008

Hay algunas diferencias con respecto a la arquitectura del nuevo Windows Server 2008, estos cambios afectan a la manera en que se gestiona el sistema hasta el punto de que se puede llegar a controlar el hardware de forma más efectiva, entre las mejoras que se incluyen, están:

• Nuevo proceso de reparación de sistemas NTFS, proceso en segundo plano que repara los archivos dañados.

• Creación de sesiones de usuario en paralelo, reduce tiempos de espera en los Terminal Services y en la creación de sesiones de usuario a gran escala.

• Cierre limpio de Servicios.

• Sistema de archivos SMB2 para compartir archivos en Windows, que es de 30 a 40 veces más rápido el acceso a los servidores multimedia.

• Protección contra malware en la carga de controladores en memoria.

• Windows Hardware Error Architecture que es el protocolo mejorado y estandarizado de reporte de errores.

• Virtualización de Windows Server, mejoras en el rendimiento de la virtualización.

• Server Core, el núcleo del sistema se ha renovado con muchas y nuevas mejoras.

09. Requisitos de hardware Windows Server 2008

	Mínimos	**Recomendados**
Procesador	1 GHz (x86) 1.4 GHz (x64)	2 GHz o superior
Memoria	512 MB RAM	2 GB RAM o más 4 GB RAM Edición Standard 64 GB RAM Enterprise, Datacenter
Tarjeta gráfica	VGA (800 x 600)	Super VGA o mayor
Espacio libre HDD	10 GB	50 GB o mas
Unidades	DVD-ROM	DVD-ROM o mejor
Otros dispositivos	Monitor Super VGA (800 x 600) o con resolución mayor, teclado y ratón	

Figura 7

10. Actualizaciones Windows Server 2008 (Service Pack)

Debido a que Windows Server 2008 se basa en el núcleo Windows NT 6.0 Service Pack 1, la versión final RTM es considerada como Service Pack 1; de acuerdo con esto, el primer service pack lanzado será llamado Service Pack 2.

Anunciado el 24 de octubre de 2008 este service pack contiene los mismos cambios y mejoras que el equivalente próximo Windows a salir.

Una guía preliminar publicada por la compañía describe muchas áreas de mejora, notablemente la inclusión de un número de nuevas características de virtualización incluyendo Live Migration.

Un reducido consumo de energía, un nuevo conjunto de herramientas de administración, nuevas características Active Directory como una papelera de reciclaje para objetos Active Directory borrados, una nueva versión de IIS 7.5 que incluye un renovado servidor FTP, y el aumento del número de núcleos de procesamiento de 64 a 256.

Los procesadores de 32-bits ya no están soportados.

Las mejoras en el rendimiento fueron un área de desarrollo importante en esta versión; Microsoft anunció que se habían realizado trabajos para disminuir el tiempo de arranque, mejorar la eficiencia de operaciones de entrada y salida a la vez que reducir potencia de procesamiento.

El 7 de enero de 2009, se lanzó una versión preliminar beta de Windows Server 2008 R2 para suscriptores de los programas de Microsoft, TechNet enfocado a profesionales de lainformacion y MSDN que es un programa para desarrolladores de software ambas se encuentran disponibles con portales web, Dos días después, se lanzó al público general mediante el Centro de descargas de Microsoft.

11. Ediciones Finales Windows Server 2008

Windows Server 2008 R2 Foundation: Es una base tecnológica rentable y de nivel básico orientada a propietarios de pequeñas

empresas y generalistas de TI que brindan soporte a pequeñas empresas.

Foundation es una tecnología no costosa, fácil de desplegar, probada y confiable que ofrece a las organizaciones la base para ejecutar las aplicaciones comerciales más predominantes, compartir información y recursos.

Windows Server 2008 R2 Standard: Es el sistema operativo de Windows Server más robusto hasta la fecha.

Con capacidades de virtualización y Web mejoradas e incorporadas, está diseñado para incrementar la confiabilidad y flexibilidad de su infraestructura de servidor al tanto que ayuda a ahorrar tiempo y reducir costos.

Las poderosas herramientas le ofrecen un mayor control sobre sus servidores y agilizan las tareas de configuración y administración.

Windows Server 2008 R2 Enterprise: Es una plataforma de servidor avanzada que ofrece un soporte más rentable y confiable para cargas de trabajo de misión crítica.

Ofrece características innovadoras para la virtualización, ahorros en energía y manejabilidad, ayuda a facilitar el acceso de los empleados móviles para el acceso a los recursos corporativos.

Windows Server 2008 R2 Datacenter: Ofrece una plataforma de clase empresarial para desplegar aplicaciones comerciales críticas y virtualización a gran escala en servidores grandes y pequeños.

Mejora la disponibilidad, optimiza la administración de energía e integra soluciones para empleados móviles y de sucursales.

Reduce los costos de infraestructuras al consolidar las aplicaciones con derechos de licenciamiento de virtualización ilimitados.

Windows Web Server 2008 R2: Es una plataforma poderosa de servicios y aplicaciones Web.

Con la presentación de Internet Information Services (IIS) 7.5 y diseñada exclusivamente como servidor orientado a Internet, ofrece una administración mejorada y herramientas de diagnóstico para ayudar a reducir los costos de infraestructura cuando se utiliza con una variedad de populares plataformas de desarrollo.

Con roles de Servidor Web y Servidor de Nombres de Dominio incluidos, como así también una confiabilidad y escalabilidad mejoradas

Windows HPC Server 2008: La última generación de informática de alto rendimiento HPC, ofrece herramientas de clase empresarial para un entorno HPC altamente productivo.

Windows HPC Server 2008 puede escalar en forma eficiente a miles de núcleos de procesamiento e incluye consolas de administración que le ayudan a monitorear en forma proactiva y mantener la salud y estabilidad del sistema.

Windows Server 2008 R2: Ofrece una plataforma de clase empresarial para desplegar aplicaciones comerciales críticas.

Base de datos escalable, línea de negocios y aplicaciones personalizadas cumplen con las crecientes necesidades comerciales.

Ayude a mejorar la disponibilidad con capacidades de agrupamiento ante fallas y partición dinámica de hardware.

12. Boletines de Seguridad Windows Server 2008

Dentro de las vulnerabilidades encontradas en el sistema operativo Windows Server 2008, Microsoft pública cada cierto tiempo las más relevantes a continuación se detallan la publicación de unos boletines.

12.1. Boletín MS10-010

Una vulnerabilidad en Windows Server 2008 Hyper-V podría permitir la denegación de servicio (977894).

La vulnerabilidad podría permitir la denegación de servicio si un usuario ejecuta una secuencia con formato incorrecto de instrucciones máquina en una de las máquinas virtuales invitadas que hospede el servidor Hyper-V.

Para aprovechar esta vulnerabilidad, el atacante debe tener credenciales de inicio de sesión válidas y ser capaz de iniciar una sesión localmente en una máquina virtual invitada.

Los usuarios anónimos o los usuarios remotos no pueden aprovechar esta vulnerabilidad.

Como recomendación se debe tener habilitada la actualización automática y no deben realizar ninguna acción porque esta actualización de seguridad se descargará e instalará automáticamente.

12.2. Boletín MS11-082

Vulnerabilidades en el Host Integration Server podría permitir la denegación de servicio.

Las vulnerabilidades podrían permitir la denegación de servicio si un atacante remoto envía paquetes especialmente diseñados para una red de Host Integration Server escucha en el puerto UDP 1478 o en los puertos TCP 1477 y 1478.

Las mejores prácticas de firewall y las configuraciones de firewall por defecto puede ayudar a proteger las redes frente a ataques que se originan fuera del perímetro de la empresa.

Como Recomendación se tendrá que habilitar la actualización automática para la descarga del parche automáticamente.

12.3. Boletin MS 10-070

Una vulnerabilidad en ASP.NET podría permitir la divulgación de información (2418042).

La vulnerabilidad podría permitir la divulgación de información, si un atacante se aprovechara de esta vulnerabilidad podría leer datos, tales como el estado de vista, que se ha cifrado en el servidor, si se aprovecha con éxito, se podría utilizar para descifrar y manipular los datos cifrados en el servidor.

Microsoft. NET Framework versiones anteriores a Microsoft. NET Framework 3.5 Service Pack 1 no se ven afectados por la divulgación de parte del archivo de contenido de esta vulnerabilidad.

La actualización de seguridad corrige la vulnerabilidad al firmar, todos los datos que se cifran por ASP.NET, también corrige la vulnerabilidad descrita por primera vez en la seguridad de Microsoft 2416728.

13. Conclusiones Windows Server 2008

Podemos determinar con lo antes mencionado acerca del sistema Windows Server 2008 , que su interfaz ha recibido un cambio relevante en cuanto a la forma que se ve y se trabaja en cuanto a su administracion.

A La larga lista de características que abarca este nuevo sistema, la que mas le importa a un administrador es el hecho el cambio relevante que ha sufrido este sistema en cuanto a la seguridad se refiere.

Para hacer de este el sistema servidor mas seguro que se ha creado según Microsoft , pero esto conlleva seguir ciertas reglas y parámetros al configurar el sistema, lo cual hace pensar que si las nuevas características hacen realmente que sea más seguro o simplemente hacen que el servidor sea más difícil de usar.

Sólo las pruebas y puestas en marcha en el trabajo diario por parte de los administradores del sistema, mostrará lo aceptable o repudiable que este Sistema Operativo Windows Server 2008 será.

14. Vulnerabilidades más comunes por parte del usuario, al usar el Sistema Operativo Windows 7

Como un medio de guía para saber cuales son los errores mas comunes al instlar Windows tenemos:

14.1. Uso de Instalaciones por defecto

Cuando instalamos la mayoría del software, como sistemas operativos o aplicaciones los mismos vienen con scripts de instalación, lo que hace es facilitar la instalación pero esto trae consigo un sinnúmero de

riesgos ocultos como instalación de software malintencionado, dejar puertos abiertos los mismos que podrían ser utilizados por atacantes.

14.2. Cuentas sin contraseña o contraseñas débiles

Al instalar Windows 7 pasamos por alto muchas veces ,el no uso de una contraseña para la cuenta administrador, pero esto conlleva un peligro inminente a corto plazo, también se cometen errores como el uso de contraseñas muy débiles o de fácil deducción para un atacante, por lo que se recomienda identificar estos tipos de vulnerabilidades y eliminarlas del sistema.

14.3. No manejo del Registro de Eventos

Los registros le proporcionan los detalles de lo que está ocurriendo, qué sistemas se encuentran bajo ataque y qué sistemas han sido comprometidos, pero generalmente un usuario común de computador no utiliza esta funcionalidad por lo que se hace más difícil detectar cuando una intromisión no deseada está ocurriendo.

14.4. Recursos Compartidos no protegidos

El protocolo SMB, permite habilitar la compartición de recursos a través de la red, esta característica se encuentra activada por defecto en todas las versiones de Windows, basta que un usuario tenga acceso a la red donde se encuentra la victima para poder acceder a la información si no se tiene cuidado en protegerla con alguna contraseña.

14.5. Deshabilitacion del Firewall

Un Firewall es un sistema ubicado entre dos redes, y que ejerce una política de seguridad establecida, se ve como un mecanismo encargado de proteger una red confiable de una que no lo es por ejemplo Internet, este mecanismo puede consistir en controlar todo el tráfico desde dentro hacia fuera, y viceversa, pero en mucho de los casos mantenemos la costumbre de dejar el firewall deshabilitado, conllevado con esta mala práctica a que no haya ningún control en cuanto al tráfico de la red se refiera dejando con esto política de seguridad local desatendidas y vulnerables fáciles blancos para un atacante informático.

CAPITULO IV

DESARROLLO

01. INFORME REFERENTE A LAS VULNERABILIDADES, MÁS COMUNES PRESENTES EN LAS VERSIONES DE WINDOWS SERVER 2008 Y WINDOWS 7.

El tema de seguridad informática es muy complejo, por lo que atravez de los años se han venido produciendo diferentes fallos de la plataforma, los cuales son recogidos analizados y debidamente publicados por la empresa Microsoft, por medio de boletines de seguridad, para el desarrollo de la propuesta de investigación, analizaremos los fallos que fueron mencionados en el capitulo anterior para poder llegar a conclusiones de las mas comunes y poder determinar cuales son los mas importantes y que se deben de prestar mas atención, para un buen manejo del sistema operativo Windows 7 y Windows Server 2008.

Entre las vulnerabilidades mas comunes tenemos:

- Uso permisivo con elevación de privilegios de la cuenta Administrador.
- Comparticion de archivos desatendidas.
- Uso de contraseñas vacias o muy simples.
- No control en los puertos abiertos.
- Deshabilitacion de Firewall.
- Actualizaciones casi nulas.
- Desactualizacion del antivirus.
- No uso de la auditoria de seguridad de Windows.
- Instalación de software no confiable.
- Activacion innecesaria de servicios como FTP, Telnet, SMTP etc.
- Descarga de correo electrónico no confiable.

- Uso de navegadores obsoletos.
- No parcheo de aplicativos instalados en el Sistema Operativo.

02. ELABORACION DE UN DOCUMENTO MODELO QUE MUESTRE LA CORRECTA IMPLEMENTACION, PARA ASEGURAR LA INFORMACION EN LA VERSION DEL SISTEMA OPERATIVO WINDOWS 7

Como un medio para la correcta implementación y funcionamiento de nuestro Sistema Windows 7, tendremos como referencia seguir las recomendaciones enumeradas a continuación:

02.1. Instalación de Parches publicados por Microsoft.

En el medio informático cualquier programa, que se encuentre instalado en un computador necesita de actualizaciones periódicas, para poder con esto solucionar posibles problemas que se hayan descubierto en el software o también para ofrecer una nueva funcionalidad al mismo.

Las actualizaciones son especialmente necesarias e importantes en el sistema operativo, ya que es este el que ofrece los servicios al resto de programas y el que más problemas de seguridad puede provocar.

Estas actualizaciones son ofrecidas generalmente en forma de parches que solucionan los errores de seguridad que se van descubriendo, cuando se llegan a un número considerable de parches, dan cabida para que todos estos sean recolectados y publicados como un service pack.

Por lo tanto es muy importante estar al día para un usuario de computador con estas actualizaciones, ayudando así a evitar posibles problemas, que se puedan presentar al usar el sistema operativo.

Estas actualizaciones están disponibles para descargar de forma gratuita, desde el sitio de Microsoft donde se explica también la forma de aplicarlos.

Como otros medios aparte de las actualizaciones publicadas por Microsoft, cuando esta corporación no emite a la brevedad las actualizaciones para el sistema Operativo se puede hacer uso de WinUp como herramienta complementaria que trabaja en conjunto con Microsoft, este es un paquete con casi todas las actualizaciones que han salido para Windows hasta determinada fecha.

La principal ventaja de WinUp radica en que es muy sencillo e intuitivo.

Sin embargo, no permite seleccionar qué se quiere y qué no instalar. s, WinUp es la opción recomendada para usuarios domésticos que tan sólo quieren tener su Windows actualizado sin tener que batallar con la configuración de Windows Update.

Ademas existe otra herramienta complementaria como lo es Windows updates Downloader que es un programa para descargar las actualizaciones de Windows y otros programas.

Funciona con un sistema de listas disponibles en su página web en las que se puede seleccionar qué se va ha descargar.

Se tiene que tener en cuenta que las listas no siempre están actualizadas a las últimas versiones , Además, no instala los parches, sólo los descarga, es por ello que esta más enfocado a administradores del sistema que a usuarios comunes del computador.

02.2. Configuración de Windows Update

Una forma muy sencilla de mantener nuestro sistema operativo actualizado es a través del uso de Windows Update, esta es la web oficial de Microsoft donde a través de esta, podemos ver cuáles son las actualizaciones que tenemos instaladas actualmente y cuales son las que nos falta por instalar.

Cuando ingresamos a este portal de descarga por defecto, el sistema selecciona automáticamente todas las actualizaciones críticas y Service Packs últimos que se encuentran disponibles ayudando con esto, al usuario común su correcta descarga e implementación.

02.3. Actualizaciones Automáticas

Una función importante incluida en las versiones de Windows es la llamada Actualizaciones Automaticas, la cual se puede configurar para comodidad del usuario, estableciendo dia y hora para la actualización, esto ayuda de gran manera a que las mismas no interfieran en el trabajo del usuario final, Aunque la primera vez que vayamos a instalar actualizaciones para el sistema operativo es recomendable hacerlo a

través de Windows Update como una forma cómodo de mantenerse al día.

Para la habilitación de las actualizaciones automaticas seguimos unos pasos sencillos como lo son ir a Inicio, abrir el panel de control,damos click sobre el icono de Windows Update y configuramos las opciones según nuestra conveniencia.

02.4. Uso de la Herramienta MBSA

Una herramienta que nos permite mantener nuestro sistema al día es Microsoft Baseline Security Analizer (MBSA), un software de Microsoft que nos comprobará el sistema de forma parecida a Windows Update.

La diferencia entre Windows Update y MBSA es que el primero nos ofrece más actualizaciones que el segundo, ya que también nos da la posibilidad de instalar nuevo software, mientras que MBSA se preocupa solamente de las actualizaciones de seguridad.

MBSA nos ofrece las siguientes características:

• Buscar vulnerabilidades en las aplicaciones Windows desde su versión NT, 2000, XP, 7, 2003 hasta la 2008, Internet Explorer, Microsoft Office, Windows Media Player, la máquina virtual Java y otras aplicaciones.

• Comprobacion de la configuración y activación del Internet Connection Firewall.

• Comprueba que la configuración de las zonas de Internet Explorer sea la correcta

• Comprueba que las actualizaciones automáticas estén activadas

• Detecta servicios innecesarios que tengamos activados como las de defecto FTP, Telnet, WWW y SMTP.

• Detecta contraseñas vacías o muy sencillas de adivinar.

02.5. Actualizaciones del resto de programas

Además de mantener actualizado nuestro sistema operativo es importante, también, que actualicemos el resto de programas que estén instalados en nuestro ordenador, especialmente los que necesiten acceder a la red para funcionar por ejemplo, el lector de correo o el programa de mensajería instantánea.

02.6. Uso de Contraseñas Complejas

En la mayoría de los casos, la autenticación en los ordenadores es decir, demostrar quién somos ante el ordenador para poder acceder a algún recurso se hace a través de contraseñas.

Esto es bastante peligroso, ya que mucha gente no conoce el método para escoger una buena contraseña y, aunque lo conozca, la mayoría de personas no son capaces de recordar una contraseña que sea lo suficientemente segura.

Un buen sistema de autenticación debe basarse en combinaciones de varios factores a la vez: algo que sabemos, algo que tenemos, algo que somos, Por ejemplo, para identificarnos en un cajero automático utilizamos dos factores: algo que tenemos la tarjeta de crédito y algo que sabemos el número secreto o PIN.

En el caso de las contraseñas, solo estamos utilizando uno de los factores, algo que sabemos, por lo que este debe ser lo más seguro posible.

02.7. Configuración para no recordar las contraseñas

La mayoría de navegadores incluyen una función para recordar las contraseñas de los diferentes sitios que visitamos.

Usar esta funcionalidad ayuda a no tener que usar la misma contraseña para cada sitio que visitemos, evitando tener recordar cientos de contraseñas diferentes.

Pero esto se torna un serio problema, si el navegador es capaz de enviar nuestras contraseñas sin que nosotros tengamos que indicarle nada, porque no pueden hacerlo el resto de programas, debemos quitar la opción autocompletar.

02.8. Conocimiento de los Virus y sus Repercusiones

La característica básica de un virus informático es la capacidad de crear copias de sí mismo y replicarse en otros ordenadores.

Además de ello, algunos virus son malignos y además de rutinas para reproducirse incorporan otras para destrucción de datos.

Los virus no solamente afectan a los ficheros ejecutables los típicos .exe, sino que pueden estar contenidos en cualquier tipo de fichero que contenga código que vaya a ser interpretado.

Un ejemplo son los ficheros del programa Microsoft Office, en cuyo interior puede haber macros, trozos de código que Office ejecuta; estas macros pueden contener virus y infectar otros archivos, por lo que

debemos tener cuidado con ficheros de cualquier tipo y no solo ejecutables corrientes.

Aunque anteriormente los virus viajaban de un ordenador a otro a través de disquetes, hoy en día la forma más habitual de reproducción de estos es a través del correo electrónico.

Muchos virus disponen de la capacidad de buscar direcciones de correo dentro de nuestro ordenador no solamente en la agenda de nuestro programa de correo, sino en cualquier fichero del disco duro y de enviarse automáticamente a esas direcciones.

Debemos tener una especial precaución para evitar ser infectados por un virus a través del correo electrónico, por lo que nunca debemos abrir un fichero que hayamos recibido, aunque el remitente sea de confianza.

En primer lugar deberemos asegurarnos que el fichero ha sido realmente enviado por el remitente; en este caso puede ser muy útil una simple llamada de teléfono para confirmarlo.

En caso de que no sea posible ponerse en contacto con el remitente, nunca debemos abrir directamente el fichero desde el programa de correo.

Para asegurarnos de la inocuidad de este, lo guardaremos primero en el disco y lo escanearemos con un programa antivirus.

02.9. Uso de antivirus adecuado

En la actualidad en el medio informatico podemos escoger entre una gran variedad de antivirus, algunos pagados y otros gratuitos para su descarga.

Cuando seleccionemos el antivirus que queremos instalar debemos tener en cuenta varios factores, como el hecho de que esté mantenido, es decir, que haya gente trabajando en él y de que las actualizaciones de sus bases de datos de virus sean frecuentes, pues de nada nos servirá un antivirus que no pueda detectar las nuevas variantes de virus que vayan apareciendo.

Podemos ver una pequeña comparación de antivirus gratuitos en el Internet cada uno de ellos es mejor en una u otra cuestión puede ser esta correo, seguridad , red corporativa etc.

Pero ninguna podra abarcar todos los ambientes para llegar a ser un antivirus indestructible, por lo que se recomienda el uso de un solo antivirus instalado en el PC.

02.10. Instalación de programas anti-Spyware

El spyware es cualquier tipo de programa que registra alguna actividad en nuestro ordenador para después enviarla sin nuestro consentimiento.

La actividad registrada puede ser de cualquier tipo, las páginas por las que navegamos, los teclas que pulsamos,etc.

Dentro del spyware, uno de los tipos menos peligrosos pero más molestos es el conocido como adware, el cual nos muestra ventanas con publicidad, normalmente relacionada con aquellas páginas que estamos visitando.

Otros tipos de spyware son mucho más peligrosos, ya que pueden capturar nuestras contraseñas, nuestras cuentas bancarias, y transmitirlas posteriormente a quien controle ese programa.

Estos programas pueden entrar de diversas formas a nuestro ordenador.

Las más comunes son acompañando a algún programa que instalemos o bien a través de nuestro navegador si este no es lo suficientemente seguro.

02.11. Instalación de programas anti-Ad-aware

Este programa nos permite eliminar de nuestro ordenador multitud de parásitos, tanto spyware como dialers, troyanos.

Una vez descargado e instalado el programa debemos comprobar si existen actualizaciones de su base de datos, cosa que podemos hacer desde el mismo programa con la opción Check for updates now.

Una vez actualizados los ficheros necesarios, procedemos a comprobar nuestro sistema y Ad-aware buscará rastros de ficheros sospechosos en nuestro disco.

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

Como conclusiones generales tenemos:

- Todo software que es desarrollado y lanzado al mercado, siempre tendrá algún tipo de fallo o vulnerabilidad luego de su puesta en marcha, el cual la mayoría de veces es corregido haciendo uso de parches o actualizaciones para el mismo.

- La protección de la información en un sistema operativo , mejora notablemente con el sistema de encriptacion ya incorporado en algunas versiones de Windows .

- Se debe seguir ciertos parametros establecidos por la corporación Microsoft, como mantener los equipos actualizados en cuanto a parches , antivirus y service pack.

- No se debe confiar en todo el software que podamos descargar gratis en internet, ya que el mismo puede contener codigo malicioso que puede afectar la estabilidad del sistema.

- Todo el tráfico de información sin su debida seguridad, será fácil blanco del ataque de hackers o personas mal intencionadas que puedan hacer mal uso de la misma.

- Al instalar todas la recomendaciones antes mencionadas , no estaremos 100% libres de cualquier ataque por eso se debe poner una debida atención al correcto mantenimiento periódico del sitema.

RECOMENDACIONES

Como recomendaciones generales tenemos:

Para Windows 7

• Se debe hacer uso de contraseñas complejas, para el inicio de sesión, no utilizar password demasiados obvios y mucho menos dejarlas en blanco.

• Tener gran énfasis en la habilitación permanente del firewall de Windows, ya que este es el encargado de controlar todo el trafico que se pueda tener hacia el exterior, como otras computadoras o el internet.

• No se debe descargar ningún tipo de software o información, de la cual no estemos completamente seguros de la confianza y seguridad de su origen.

• Actualizacion permanente del sistema principal Windows, como asi de sus utilitarios que funcionan dentro de este entorno como el antivirus.

• La navegación de Internet se debe hacer en lo posible en sitios seguros, y con navegadores actualizados.

• En lo posible hacer uso de la Herramienta de Microsoft MBSA para mejor control de nuestro sistema operativo.

Para Windows Server 2008

- Mantener reglas y estándares al momento de crear usuarios y al delegar permisos a los mismos.

- No se tiene que escatimar esfuerzos en cuanto a las configuraciones debidas que se debe de hacer para el uso del sistema operativo, ya que como un sistema servidor deberá estar la mayoría del tiempo disponible.

- Se debe mantener abiertos solo los puertos necesarios, y saber porque de la habilitación de cada puerto.

- Uso permanente del firewall de Windows.

- Las contraseñas para administración deben contener al menos , la combinación de letras, números y caracteres especiales, y estas con traseñas deberán ser cambiadas periódicamente.

- Uso y manejo de un antivirus adecuado y confiable, que nos permita una fluidez del trabajo correcta.

- Habilitacion y configuración de la Auditoria de Windows para control de accesos al sistema.

BIBLIOGRAFIA

1) Gustavo F.Torrealday copiado el 25-09-2011 de: http://www.torrealday.com.ar/articulos/articulo005.htm

2) (n.d.) copiado el 23-09-2011 de:http://definicion.de/seguridad-informatica/

3) (n.d.) copiado el 23-09-2011 de: http://www.masadelante.com/faqs/sistema-operativo

4) Clifford Stoll The cuckoo's egg copiado El 25-09-2011 de: http://g0tr00t.files.wordpress.com/2010/02/el-huevo-del-cuco.pdf

5) (n.d.) copiado el 23-09-2011 de: http://es.wikipedia.org/wiki/Error_de_software

6) (n.d.) copiado el 05-10-2011 de:

http://www.pulsaf5.com/agujero-de-seguridad-critico-en-todas-las-versiones-de-windows/

7) (n.d.) copiado el 05-10-2011 de: http://www.principiantes.info/seguridad/macro-guia_seguridad.php

8) (n.d.) copiado el 27-09-2011 de: http://www.psicofxp.com/forums/noticias.60/313676-agujero-seguridad-windows-explotado-via-e.html

9) (n.d.) copiado el 27-09-2011 de:

http://www.itespresso.es/microsoft-soluciona-25-agujeros-de-seguridad-en-windows-office-y-exchange-44536.html

10) (n.d.) copiado el 07-10-2011 de: http://www.taringa.net/posts/info/6018069/Descubierto-un-nuevo-agujero-de-seguridad-en-WindowsXp.html

11) (n.d.) copiado el 07-10-2011 de:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-005.asp

12) (n.d.) copiado el 09-10-2011 de:

http://www.microsoft.com/spain/prensa/noticia.aspx?infoid=2010/04/n007

13) (n.d.) copiado el 09-10-2011 de:

http://www.vsantivirus.com/20vul.htm

14) (n.d.) copiado el 05-10-2011 de:

http://es.wikipedia.org/wiki/Windows_7

15) (n.d.) copiado el 05-10-2011 de:
http://es.wikipedia.org/wiki/Windows_2008

16) (n.d.) copiado el 09-10-2011 de:
http://www.monografias.com/trabajos6/hiso/hiso.shtml

17) (n.d.) copiado el 10-10-2011 de:

http://Release Candidate (RC) de Windows 7.mht

18) (n.d.) copiado el 11-10-2011 de:

http://www.microsoft.com/windowsserver2008/es/xl/R2-Download.aspx

19) (n.d.) copiado el 12-10-2011 de:

http://technet.microsoft.com/es-es/security/bulletin/ms10-010

ANEXOS

ENCUESTA PARA ANÁLISIS DE SITUACIÓN ACTUAL DEL MANEJO DEL SISTEMA OPERATIVO POR PARTE DEL USUARIO FINAL

Nombre_____ Fecha_____

Por favor sírvase llenar la presente encuesta.

1) Utiliza el Sistema Operativo Windows?

SI __ NO__

2) Conoce Ud. Que es un Firewall?

SI __ NO__

3) Utiliza antivirus pagado?

SI __ NO__

4) Sabe para que sirven las Actualizaciones Automaticas.

SI__ NO__

5) Conoce para que sirve la herramienta MBSA

SI__ NO__

6) Instala Service Pack del Sistema Operativo

SI__ NO__

7) Utiliza Internet Frecuentemente

SI__ NO__

MANUAL BASICO PARA EL USUARIO FINAL

- Utilizar Windows original por las ventajas que conlleva en comparación de la versión pirata de Windows.

- Hacer uso como minimo, la versión de Windows 7 Profesional por las seguridades que trae la misma , en comparación de sus versiones inferiores.

- Utilizar si es posible versión Windows de 64 bit por ser mas segura.

- Por ningún motivo deshabilitar el Firewall de Windows.

- Instalar en el equipo solo programas confiables, no programas sospechosos como juegos, protectores de pantalla desconocidos etc.

- Usar un antivirus pagado para estar mas protegidos en comparación de uno gratuito.

- Abrir correo electrónico solo confiable y que estemos seguros de su origen lo mismo aplica al trabajar con pentdrive.

- Al navegar por internet hacerlo en sitios seguros como son los que comienzan con https, mucho mas si se va ha realizar pagos, transferencias bancarias en línea.

- Colocar en Windows contraseñas complejas pero que sean fáciles de recordar para ud.

GLOSARIO DE TERMINOS

PatchGuard: Protección contra revisiones del núcleo, que previene parchear el núcleo.

Itanium: Un microprocesador Intel que utiliza la informática del conjunto de instrucciones explícitamente en paralelo y de 64 bits.

MS-DOS: Sistema operativo de disco de Microsoft, es un sistema operativo para computadores basados en x86.

Release Candidate: Candidata para su lanzamiento, comprende un producto final, preparado para publicarse como versión definitiva.

RTM: Release To Market, para referirse como productos comercial, versión considerada muy estable y relativamente libre de errores.

Licencia OEM: Original Equipment Manufacturer, caso concreto de software, una versión OEM implica que su venta está siempre ligada a un equipo nuevo.

Kernel: Núcleo de un sistema operativo, es decir, la parte central del funcionamiento y arranque del sistema.

SMB: Server Message Block o Bloque de mensajes de servidor, protocolo de red usado por las redes de Microsoft Windows para acceder a sistemas de archivos de otras máquinas.

WMF: Metarchivo de Windows, significa que este archivo contiene la información que describe o especifica otro archivo.

NTFS: Sistema de Archivos de Nueva Tecnología, es usado por las versiones de Windows.

Terminal Services: Servicios de Terminal, permite a un usuario acceder a las aplicaciones y datos almacenados en otro ordenador mediante un acceso remoto por red.

TechNet: Microsoft TechNet proporciona recursos y ayuda técnica a los profesionales TI de manera sencilla e inteligente, para ayudarles a evaluar, desarrollar y dar soporte eficaz sobre las soluciones Microsoft.

MSDN: Se refiere tanto a los servicios web orientados a desarrolladores de software basado en plataformas Microsoft.

HPC: High Performance Computing, Esta tecnología permite enlazar servidores Windows en un clúster de alto poder.

Hyper-V: Es la funcionalidad de virtualización basada en el hypervisor, incluida como un rol de servidor en el sistema operativo Windows server 2008.

UNIX: Es un sistema operativo multitarea y multiusuario, lo cual significa que puede ejecutar varios programas simultáneamente, y que puede gestionar a varios usuarios simultáneamente.