UNIVERSIDAD TECNOLÓGICA ISRAEL

CARRERA DE SISTEMAS INFORMÁTICOS

Análisis de Vulnerabilidades en los mejores Antivirus del 2012 a Nivel Corporativo.

Estudiante

Manuel Arturo González González

Tutor

Ing. Paúl Diestra.

Quito – Ecuador

Septiembre 2012

UNIVERSIDAD TECNOLÓGICA ISRAEL

CARRERA DE SISTEMAS INFORMÁTICOS

CERTIFICADO DE RESPONSABILIDAD

Yo Ing. Paul Diestra certifico que el Sr. Manuel Arturo González González con C.C. No. 0105760649 realizo la presente tesis con título de **"Análisis de Seguridad de la información en los Dispositivos Móviles Smartphone"** y que es autor intelectual del mismo, que es original, autentica y personal.

_____

Ing. Paul Diestra

UNIVERSIDAD TECNOLÓGICA ISRAEL

CARRERA DE SISTEMAS INFORMÁTICOS

ACTA DE SESIÓN DE DERECHOS

Yo, **Manuel Arturo González González**, 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 inversiones, 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".

Cuenca, Diciembre 4 del 2012

UNIVERSIDAD TENOLÓGICA ISRAEL

CARRERA DE SISTEMAS INFORMATICOS

CERTIFICADO DE AUTORÍA

El documento de tesis con título "**Análisis de Vulnerabilidades en los mejores Antivirus del 2012 a Nivel Corporativo**" ha sido desarrollado por Manuel Arturo González González con C.C. No. 010576064 9 persona que posee los derechos de autoría y responsabilidad, restringiéndose la copia o utilizacion de cada uno de los productos de esta tesis sin previa autorización.

……

Manuel Arturo González González

DEDICATORIA

A mis padres por ser el apoyo constante en todo lo que soy, en toda mi educación, tanto académica, como personal, por su apoyo económico y moral, incondicional y perfectamente mantenido a través del tiempo.

Todo este trabajo ha sido posible gracias a ellos.

AGRADECIMIENTO

Gracias a Dios.

A mis padres y hermanas que siempre fueron un pilar fundamental en mi formación moral y apoyo incondicional para mi formación profesional, a mis grandes y queridos amigos tanto de aula como de trabajo, a mis profesores , tutor Paúl Diestra, quienes día a día nos inculcan con sus conocimientos.

RESUMEN

El presente proyecto investigativo se realizara un análisis de vulnerabilidades en los mejores antivirus del 2012 a nivel corporativo, para lo cual basamos el estudio en diferentes secciones, primero se realizo encuestas en 5 empresas de la ciudad de Cuenca, para poder determinar si dichas empresas contaban con software antivirus corporativo, además recopilar datos de conformidad de los usuarios con dicho antivirus; segundo, realizar un análisis de vulnerabilidades instalando cada uno de los 6 mejores antivirus a nivel corporativo según AV-TEST hasta el 23 de Septiembre del 2012 con el objetivo de detectar vulnerabilidades, en base a resultados obtenidos se procedió a tabular los datos y obtener resultados para poder hacer un folleto informativo con dichas vulnerabilidades y recomendaciones a las empresas.

SUMMARY

This research project will undertake an analysis of vulnerabilities in the best antivirus of 2012 at the corporate level, for which we base the study in different sections, the first survey was conducted in five companies in the city of Cuenca, in order to determine whether these companies had with corporate antivirus software, and collect data in accordance with said user antivirus, secondly, vulnerability analysis installing each of the 6 best antivirus corporate level AV-TEST according to the September 23, 2012 with the objective of detect vulnerabilities, based on results we proceeded to tabulate the data and results in order to make a brochure with these vulnerabilities and recommendations to companies.

TABLA DE CONTENIDO

INDICE DE FIGURAS Y TABLAS

TABLAS

FIGURAS

CAPITULO I

1. INTRODUCCIÓN

En la actualidad, es necesario mantener nuestros datos seguros y más aún en el ambiente corporativo, es decir las empresas requieren seguridad adicional por la gran magnitud de datos que se pueden manejar y su delicada información.

Sin embargo ningún software antivirus en el mercado tecnológico garantiza al cien por ciento la seguridad de sufrir un ataque por los virus informáticos.

El objetivo del presente trabajo está enfocado a investigar y realizar un estudio detallado acerca de las vulnerabilidades de los antivirus más famosos y con mejor reputación en el mercado, usados a nivel corporativo, cuáles son sus debilidades, en cuanto a tiempo de ejecución, carga de trabajo en el sistema operativo y que posibles recomendaciones se podría dar, de esta manera aportar al ambiente tecnológico y seguridad corporativa.

Es imposible erradicar al cien por ciento o evitar que cada día personas o incluso organizaciones creen nuevos virus informáticos con variadas intenciones desde simple curiosidad hasta fines más corporativos de obtener datos importantes de organizaciones y demás fines más avanzados, pero también se debe enfocar el lado positivo gente que se esfuerza día a día en mejorar, actualizar y sacar nuevas herramientas que ayuden a proteger datos que hoy en día es lo más valioso a nivel corporativo.

1.1.Antecedentes

La expresión "cuál es el mejor antivirus", puede variar de un usuario a otro. Es evidente que para un usuario inexperto el término define casi con seguridad al software que es más fácil de instalar y utilizar, algo totalmente intranscendente para usuarios expertos, administradores de redes, etc.

No se puede afirmar que exista un solo sistema antivirus que presente todas las características necesarias para la protección total de las computadoras; algunos fallan en unos aspectos, otros tienen determinados problemas o carecen de ciertas facilidades.

Ante la masiva proliferación, tanto de virus como de productos dirigidos a su tratamiento, existe la necesidad de que algún organismo reconocido de carácter internacional certifique los productos antivirus y asegure su correcto rendimiento.

En un antivirus lo más importante es la detección del virus y, al estudio de tal fin se dedican asociaciones como la ICSA que es la Asociación Internacional de Seguridad Computacional

Dicha certificación se realiza cuatro veces al año, sin el conocimiento del fabricante y con una versión totalmente comercial, con lo que se asegura que la versión que se certifica es la que recibe directamente el usuario y no una especialmente preparada para la prueba.

A nivel corporativo la protección debería ser al 100% ya que los datos que se manejan son

muy importantes y delicados.

A nivel local se tiene una idea leve de todas las vulnerabilidades que pueden tener y causar un antivirus no eficiente a nivel corporativo, ya que en la gran mayoría de empresas se maneja un departamento de sistemas y el encargado del mismo debe asesorar al gerente de la empresa recomendando siempre la mejor opción, este trabajo pretende hacer un análisis entre todos los mejores antivirus corporativos del 2012 y así aportar y servir como guía al personal de sistemas.

1.2.Planteamiento del Problema

1.2.1. Tema de Investigación

"Análisis de Vulnerabilidades en los mejores Antivirus del 2012 a Nivel Corporativo".

1.3.Sistematización

1.3.1. Diagnostico

Causas

- Baja efectividad por parte de algunos antivirus para el análisis de software malicioso.
- Carga de trabajo que usan los antivirus es mayor cuando emplea métodos basados en firmas.
- Detección proactiva constituida por falsos positivos.
- Bibliotecas propensas a vulnerabilidades que pueden provocar desbordamiento en búfer de memoria.
- Manejo incorrecto en archivos .EXE

1.3.2. Pronóstico

- Mayor probabilidad de sufrir infecciones a nivel de sistema operativo, y pérdida de datos que en una organización son de vital importancia.
- Análisis de software malicioso más lento y por lo tanto más propenso a vulnerabilidades y mayor consumo de recursos del ordenador.
- Detección y eliminación de archivos que no son virus y que pueden provocar perdida de archivos importantes.
- Mal funcionamiento del software antivirus que provocan desbordamiento, por tanto aumenta vulnerabilidad en protección y puede causar infiltraciones y pérdida de datos importantes de la organización.
- Algoritmos deficientes que pueden causar eliminación de archivos, programas innecesarios.

1.3.3. Control de Pronóstico

- Optimizar algoritmos de búsqueda del software antivirus a nivel corporativo.
- Optimizar el tiempo de búsqueda usado para detectar software malicioso.
- Controlar el desbordamiento de memoria en software antivirus a nivel corporativo.
- Mejorar algoritmos de detección de falsos positivos en software antivirus a nivel corporativo.

1.4. Objetivos

1.4.1. Objetivo General

Realizar un estudio y análisis de vulnerabilidades en los mejores antivirus del 2012 a nivel corporativo.

1.4.2. Objetivos Específicos

- Realizar estudios en empresas usuarias de antivirus objeto de estudio.
- Instalar en una laptop dichos antivirus, en un periodo determinado, para objetos de estudio.
- Determinar vulnerabilidades en base a estudio y análisis.
- Realizar un folleto informativo sobre vulnerabilidades en los mejores antivirus del año 2012 a nivel corporativo.

1.5. Justificación

1.5.1. Justificación Teórica

La ventaja de investigar sobre las vulnerabilidades que tienen los mejores antivirus del 2012 a nivel corporativo es que, se tendrá una mayor información al momento de implementar un antivirus para la empresa, además servirá como guía al personal de sistemas de información para tomar las precauciones necesarias si es que ya se está usando uno de estos antivirus.

Es fundamental en toda organización adquiera software antivirus acorde a sus necesidades generales y específicas recordando siempre lo siguiente:

- Determinar necesidades internas y externas de la empresa.
- Las necesidades de seguridad de una empresa son distintas a las necesidades de los usuarios normales (usuarios finales).
- También se debe prever y mantener planes de contingencia en software antivirus; ninguna empresa esta exenta de ser victima de infecciones, robos de información, daños en los sistemas operativos que usan para actividades diarias

y con una cantidad de información importantísima, es por eso que en el departamento de sistemas recaerá la obligación de reducir al máximo que se den estos hechos, teniendo siempre actualizado su antivirus y si es mejor copias de seguridad y varias actividades que maximicen la protección de la empresa.

1.5.2. Justificación Práctica

La importancia de esta investigación amerita un análisis sobre vulnerabilidades de dichos antivirus en empresas por lo que se busca generar entregables como folletos que se distribuirá a organizaciones dentro del departamento de sistemas de información, que sirva como guía e informativo al momento de implementar software antivirus dentro de las organizaciones.

1.5.3. Justificación Metodológica

Se usara la siguiente metodología:

Inductiva: El estudio se realizara en el área propia de investigación.

Deductiva: En base a otras fuentes que no necesariamente puede ser el área propia de investigación, esta metodología permitirá sacar conclusiones en base a este método aplicado.

1.6. Alcance y Limitaciones

1.6.1. Alcance

El proyecto pretende obtener como objetivo final presentar un folleto informativo sobre el estudio de las vulnerabilidades encontradas en los mejores antivirus del 2012 orientados al nivel corporativo, además este folleto entregar a empresas para

mejorar o de alguna manera guiar a tomar en cuenta mejores decisiones al momento de hablar seguridades en sus organizaciones y así proteger de manera más efectiva sus datos.

1.6.2. Limitaciones

La realización de este trabajo investigativo no contempla:

- Mejoramiento de algoritmos en dichos antivirus sometidos a análisis de vulnerabilidades.
- Informes a empresas desarrolladores de software antivirus, solo será a nivel de organizaciones usuarias no a creadoras.
- Mejorar métodos de búsquedas usados, tiempos de escaneo, recursos que ocupan en los ordenadores.

1.7. Estudios de Factibilidad

1.7.1. Factibilidad Técnica

En esta sección se tomará en cuenta los recursos tecnológicos que ayudaran a la consecución del presente proyecto.

- El uso de la herramienta Internet.
- Una portátil para realizar investigaciones

Estas herramientas tecnológicas nos ayudaran a obtener un folleto sobre el análisis de las vulnerabilidades en los mejores antivirus usados en el 2012 a nivel corporativo, en un tiempo más reducido, minimizando costos de estudio.

1.7.2. Operativa

La obtención de un folleto sobre las vulnerabilidades presentadas en dichos antivirus que normalmente son usados en las organizaciones tendrá un impacto favorable en los usuarios, en este caso las organizaciones ya que ayudará a tomar medidas más preventivas al momento de implementar u orientarse por un determinado software antivirus, orientación a través de la información presentada en el folleto resultante.

1.7.3. Económica

Su costo esta determinado por los siguientes factores:

Nombre	Inversión Anual	Valor
Kaspersky:Endpoint Security 8.1	5 Pc's	$ 200,00
Symantec: Endpoint Protection 12.1	5 Pc's	$ 150,00
F-Secure: Client Security 9.31	5 Pc's	$ 168,00
Sophos: Endpoint Security and Control 10.0	5 Pc's	$ 192,22
Microsoft: Forefront Endpoint Protection 2010	5 Pc's	$ 142,00
Webroot: Secure Anywhere Endpoint Protection 8.0	5 Pc's	$ 174,60

Tabla 1. Costo Antivirus Corporativos

Beneficio:

Protección de software avanzada y con gestión centralizada permitiendo ajustarse a las necesidades reales empresariales.

CAPITULO II

2. MARCO DE REFERENCIA

2.1.¿Qué es un Antivirus?

En informática un software antivirus es un programa creado con el objetivo de detectar y eliminar virus informáticos. Aparecieron por la década de los 80 y con el pasar del tiempo, la aparición de sistemas operativos más avanzados e Internet han obligado a que estos programas estén en mejora e implementación de nuevos módulos de manera constante.

Los programas antivirus se encargan de encontrar y en lo posible eliminar o dejar sin efecto la acción de los virus informáticos y otro tipo de programas malignos**.**

2.1.1. ¿Cómo funciona un antivirus?

A partir de una base de datos que contiene parte de los códigos de cada virus, el programa antivirus compara el código binario de cada archivo ejecutable con las definiciones (también llamadas firmas o vacunas) almacenadas en la misma.

Es decir que si poseemos un archivo .exe en Windows y un programa antivirus está activado para controlar la ejecución de cada ejecutable, cuando corramos el mismo revisará su código binario comparándolo con los códigos que existan en la base de datos, y en caso de dar positivo sabrá de qué virus se trata y cómo eliminarlo o detener su accionar: en ciertas oportunidades la única solución es poner el archivo ejecutable en cuarentena, dado que no se puede quitar la parte vírica del mismo.

2.1.2. Clasificación de los Antivirus

- **Antivirus para Usuarios Finales.-** Son aquellos programas antivirus destinados a uso personal, de hogar.
- **Antivirus Corporativos.-** Son aquellos programas antivirus destinados a uso empresarial, se caracterizan por brindar una protección más amplia como son los requerimientos que demandan las empresas de salvaguardar sus datos y sistemas de información.

2.1.3. Diferencia entre Antivirus Corporativo y Usuarios Finales

Permite ser administrado desde un servidor, en cuanto a configuración, políticas de seguridad y aplicación de actualizaciones. Cada pc cuenta con su Antivirus cliente instalado, pero este es administrado por una aplicación Antivirus Server.

A diferencia de un antivirus normal que es autónomo e independiente en cuanto a estas cuestiones.

2.1.4. Antivirus a Nivel Corporativo

Las empresas dedicadas a desarrollar sistemas de antivirus, anti espías, anti spam, etc., discriminan dos tipos de mercado para brindar soluciones a medida de los usuarios.

Los tipos de usuarios son:

- Para usuarios del hogar y empresas de hogar
- Para usuarios empresariales

Los usuarios empresariales tienen requerimientos adicionales a los usuarios del hogar, por esto se han creado los Sistemas de Antivirus Corporativos que tienen características para redes.

Requisitos de Usuarios Corporativos.

Los requisitos de este tipo de usuarios son:

- Administración centralizada de actualizaciones automáticas.
- Protección para los servidores, estaciones de trabajo, plataformas de mensajería, Firewalls y servidores proxy.
- Monitoreo centralizado de todos los componentes del sistema.
- Administración de usuarios eventuales, que trabajan desde su hogar o los visitantes que se conectan a la red eventualmente; se permite la implementación de políticas de seguridad unificada en redes heterogéneas, tomando acciones de aislamiento de equipos hasta que cumplan con las políticas para ingresar a la red.
- Soluciones escalables e integrales, la modularidad de estos sistemas incrementan sus servicios según las necesidades de la empresa.
- Protección para comunicaciones vía email.
- Protección proactiva del sistema de antivirus y sus módulos adicionales de anti espías, anti spam, etc.
- Restricción de aplicaciones no autorizadas.
- Actualizaciones independientes cuando algún computador de escritorio portátil no está conectado al servidor de antivirus de la empresa.

Se debe implementar un Sistema Antivirus Corporativo que cumpla con la mayoría de especificaciones antes mencionadas para precautelar la seguridad de la red, en conjunto con sistemas complementarios de prevención contra intrusos, firewalls, entre otros.

Algunos ejemplos de Sistemas de Antivirus Corporativos son:

- Symantec Antivirus
- Kaspersky Endpoint
- Panda Antivirus Corporativo
- McAffe Antivirus Corporativo
- Trend Micro Office Scan
- Otros

Ventajas de Antivirus Corporativos

Ofrecen:

- Una protección global y uniforme para estaciones de trabajo, servidores de ficheros, plataformas de mensajería y colaboración, firewalls y proxy`s
- actualizaciones completamente automáticas, gestión centralizada y rendimiento optimizado de forma inteligente en todos los puntos.

2.2.Institutos Dedicados a Evaluar Periódicamente los Antivirus.

Para poder posicionar los distintos antivirus que existen en el mercado cada determinado tiempo, es necesaria la intervención de empresas, institutos encargados de evaluar y posicionar los antivirus a nivel de usuarios y a nivel corporativo bajo ciertos parámetros de evaluación que deben cumplir para poder ser certificados y por ende posicionados.

Empresas evaluadoras de software antivirus:

1. AV-TEST
2. AV-COMPARATIVES

Estos 2 institutos si bien no son los únicos desde un punto de vista técnico son las más

famosas y cuentan con una excelente reputación ante las empresas desarrolladoras de software antivirus.

A continuación hablaré cada una de estas empresas y en los parámetros que toman en cuenta para establecer un Ranking de los antivirus.

2.2.1. AV-Test

Fig. 1. Logo AV-TEST

Fuente: www.av-test.org

AV-Test se encarga de testear cada año los mejores antivirus en dos grupos:

1. Para Usuarios Finales
2. Empresas (Corporativo).

Además también evalúa malware y demás amenazas, en base a su evaluación publica anualmente los mejores software antivirus para personas y empresas, durante los dos últimos años 2011 y 2012 el mejor evaluado ha sido Bitdefender Internet Security a nivel Usuario Final y a nivel Corporativo figura como mejor evaluado Kaspersky: EndPoint Security 8.1.

AV-Test, testea los antivirus en base a módulos:

- Protección,

- Reparación y
- Utilidad.

Cabe enfatizar que este año 2012 hasta el 23 de Septiembre se presentaron 23 antivirus para certificación, de los cuales 21 a nivel de usuario final pasaron en las categorías de Protección, Reparación y Utilidad por ende obtuvieron el Certificado AV-TEST, en la categoría de antivirus empresariales 7 antivirus obtuvieron certificación AV-TEST ENPOINT.

2.2.2. AV-Comparatives

Fig. 2. Logo AV-COMPARATIVES

Fuente: www.av-comparatives.org

AV-Comparatives es un instituto austriaco sin ánimo de lucro, que proporciona antivirus independientes pruebas de software libre para el público.

Y sus parámetros de evaluación son los siguientes:

- Protección en tiempo real
- Detección de archivos maliciosos
- Protección Proactiva
- Falsos Positivos
- Rendimiento
- Anti-pishing

- Protección en dispositivos móviles.
- Seguridad a nivel de Red.

2.2.3 Seis Mejores Antivirus a Nivel de Usuario Final 2012 Según AV-TEST.

La siguiente imagen muestra la clasificación de antivirus para Usuarios Finales en cuanto a protección que brindan los mismos.

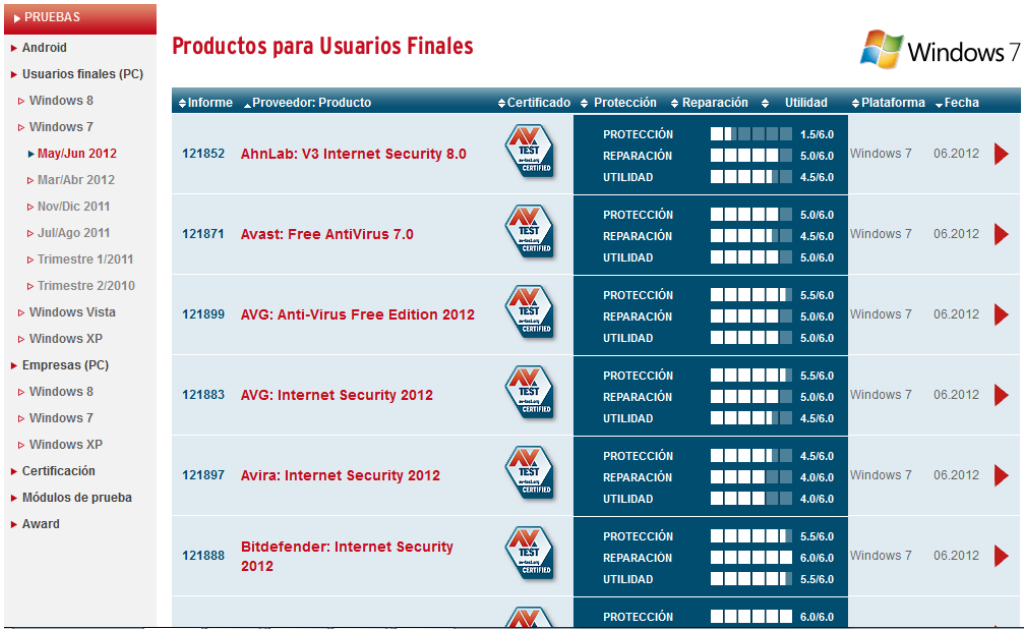


Fig. 3. Certificación AV-TEST para Usuarios Finales

Fuente: http://www.av-test.org/es/pruebas/usuarios-finales/windows-7/sepoct-2012/

Ranking	Software Antivirus	Puntuación Obtenida AV-TEST
1	BitDefender: Internet Security 2012	17/18
2	Kaspersky: Internet Security 2012	16,5/16
3	F-Secure: Internet Security 2012	16.5/18
4	Check Point: Zone Alarm Free Antivirus + Firewall 10.2	16/18
5	Symantec: Norton Internet Security 2012	15.5/18
6	AVG: Internet Security 2012	15.5/18

Tabla 2. Ranking 6 mejores antivirus a usuario final según AV-TEST

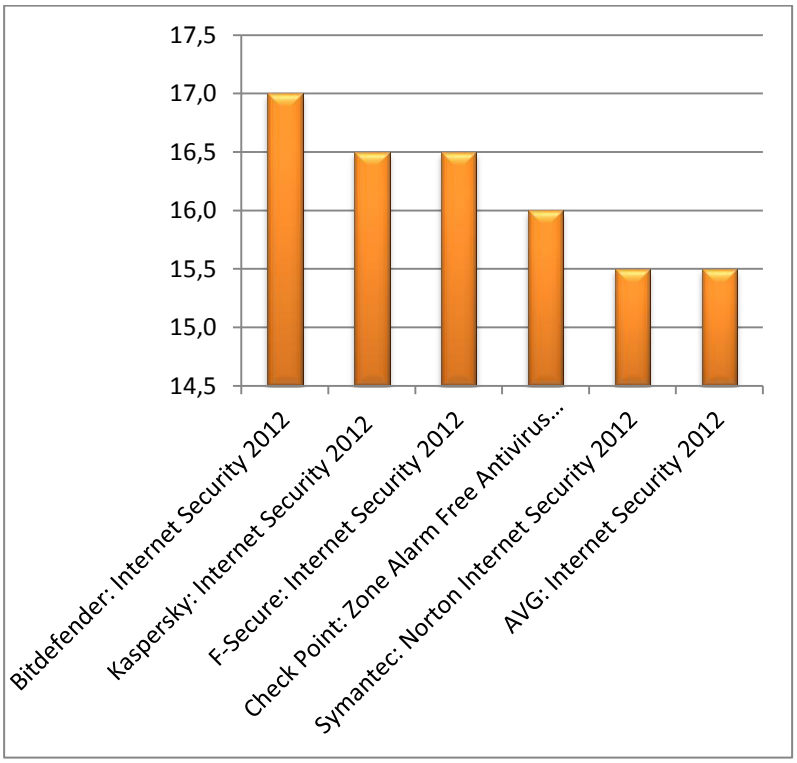


Fig. 4. Ranking 6 mejores antivirus a usuario final según AV-TEST

2.2.4 Seis Mejores Antivirus a Nivel Corporativo 2012 Según AV-TEST.

La siguiente imagen muestra la clasificación de antivirus para EMPRESAS

Fig. 5. Certificación antivirus por AV-TEST para Empresas

Fuente: http://www.av-test.org/es/pruebas/empresas/windows-7/sepoct-2012/

Cabe recalcar que el orden de la imagen anterior no muestra cual esta en primer lugar, ya que se debe sumar la puntuación total obtenida por cada uno de ellos quedando de la siguiente manera:

Ranking	Software Antivirus	Puntuación obtenida AV-TEST
1	Kaspersky: EndPoint Security 8.1	16.5/18
2	Symantec: Endpoint Protection 12.1	16/18
3	F-Secure: Client Security 9.31	15.5/18
4	Sophos: Endpoint Security and Control 10.0	14/18
5	Microsoft: Forefront Endpoint Protection 2010	13/18
6	Webroot: Secure Aywhere Endpoint Protection 8.0	12/18

Tabla 3. Ranking 6 mejores antivirus Corporativos según AV-TEST

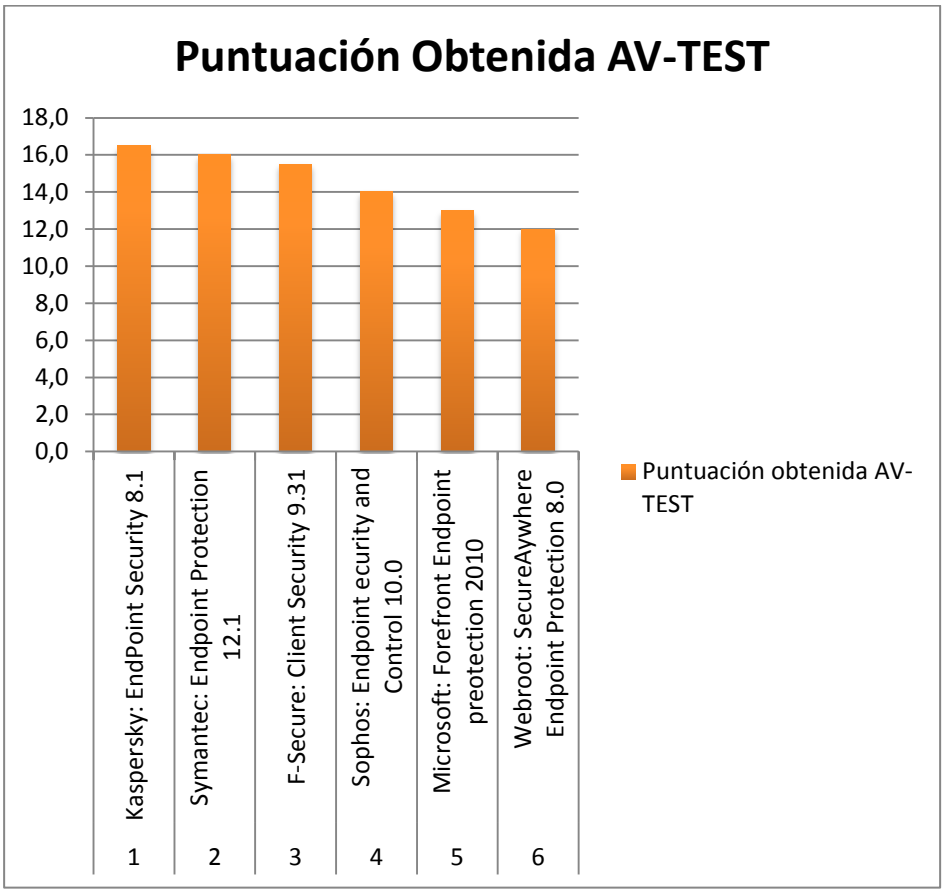


Fig. 6. Ranking 6 mejores antivirus a nivel corporativo según AV-TEST

AV-TEST evalúa los antivirus en distintas plataformas de sistemas operativos desde XP, VISTA, Windows 7 y Windows8, en el presente informe se tratará de Microsoft Windows 7 como plataforma única de estudio.

2.2.5 Parámetros de Evaluación Según AV-TEST

¿Como AV-TEST evalúa un antivirus en Windows 7?

Se evalúa en una plataforma de Windows 7 que no ha sido infectado y en el cual se simulan ataques de cientos y miles de virus de distintas formas, además archivos adjuntos en correo electrónico, paginas infectadas, etc.

Como se mencionó en un inicio AV-TEST se basa o clasifica las evaluaciones en base a PROTECCION, REPARACION Y USABILIDAD.

A continuación se describirá de manera individual que contempla cada modulo inmerso a análisis según AV-TEST.

- **Protección**: Se lleva a cabo test en un sistema (Windows 7) el cual nunca a sido infectado y en el que se van a simular ataques de miles de virus en distintas formas, archivos adjuntos en correos electrónicos, páginas infectadas, archivos infectados que se introducen con dispositivos externos, etc. AV-Test se centra en la completa funcionalidad del sistema antivirus.
- **Reparación**: En esta sección lo que se busca es evaluar cuan preparado esta el sistema antivirus para poder reparar el sistema, eliminar archivos corruptos, etc. Para lograra esto lo que hacemos es trabajar sobre un sistema ya corrupto por distintos virus y se evalúa y mide la capacidad de eliminar los malware activos y el saneamiento del sistema, revirtiendo los cambios hechos por los software maliciosos, así como eliminar los software maliciosos especiales escondidos conocidos como Rootkits.
- **Usabilidad:** También llamada y conocida como utilidad hace referencia al impacto que tiene el antivirus en el sistema, buscando medir deficiencias en el sistema luego de instalado el antivirus, así como falsas alarmas y avisos y demás cargas que causan impacto de reducción en recursos del sistema operativo.

2.6 Seis Mejores Antivirus a Nivel Corporativo Según AV-TEST

A continuación se describirá de forma breve los 6 mejores antivirus a nivel empresarial o también conocidos como antivirus corporativos.

2.6.1 Sexto Lugar: Webroot: Secure Aywhere Endpoint Protection 8.0

Fig. 7. Logo Webroot: SecureAnywhere

Fuente: www.webroot.com

Es un antivirus a nivel empresarial con múltiples ventajas a los antivirus destinados a usuario finales.

Su instalación en muy rápida, los escaneos se realizan en menos de 2 minutos y cada vez esta en mejora constante a través del entorno es decir cuenta con una tecnología de autoaprendizaje (inteligencia colectiva) y cada día se vuelve mas inteligente ante amenazas nuevas.

Posee una base de datos en la nube Red de Inteligencia Webroot desde la cual con los 700kb desde el cliente puede acceder a más de 75 TB de datos malware en la nube de Webroot.

Brinda una completa protección en un tiempo real aunque al mismo tiempo esta mejorando su inteligencia colectiva, a mas de esto recoge mas de 200 GB de datos únicos URL e IP de socios estratégicos que mejoran la inteligencia malware de Webroot.

Se puede decir que Webroot Secure Anywhere se vuelve más potente e inteligente cada minuto, y más eficaz cada vez que se agrega algo de sus clientes en todo el mundo.

2.6.2 Quinto Lugar: Microsoft: Forefront Endpoint Protection 2010

Fig. 8. Logo Microsoft Forefront Endpoint Pro 2010

Fuente: www.microsoft.com

Antes llamado Microsoft Forefront Client Security es una completa protección corporativa, ayuda a proteger la información de negocios, protege los sistemas operativos del servidor y clientes de malware y demás riesgos de seguridad informática.

Microsoft: Forefront EndPoint Protection 2010 esta basado en la plataforma Microsoft System Center Configuration Manager 2007, proporciona una única infraestructura que mejora la visibilidad y control de los sistemas al mismo tiempo reduce los costos del cliente

2.6.3 Cuarto Lugar: Sophos: Endpoint Security and Control 10.0

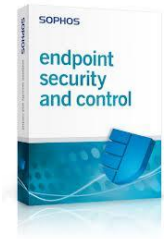


Fig. 9. Logo Sophos: Endpoint Security and Control 10.0

Fuente: www.sophos.com

Con esta versión existen varias características nuevas y mejoras.

Con el lanzamiento de Sophos EndPoint Security and Control 10 hay muchas nuevas características y mejoras.

Como mencionábamos anteriormente aquí se muestran algunas de las funciones principales y mejoras que se destacan en este software antivirus.

Funciones: Primero detallare las Funciones y una breve descripción de cada una:

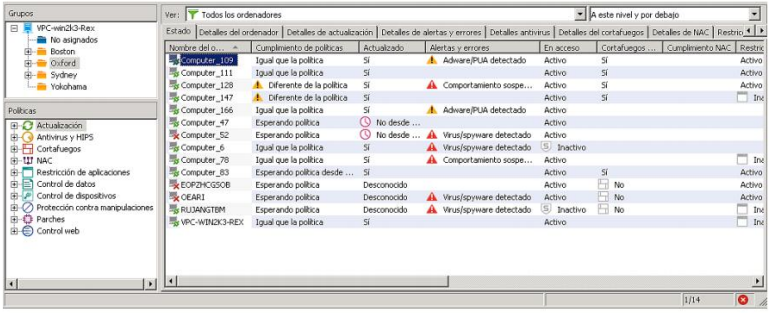


Fig. 10. Funciones de Sophos EndPoint Security and Control 10

Fuente: www.shopos.com

- **Evaluación Nuevo Parche.-** esta función permite implementar un agente en los equipos de punto final que se identifican los parches que faltan y enviar esta información al servidor Sophos Enterprise Console.

- **Parche de Evaluación de Seguimiento de los Productos más Ampliamente Utilizados.-** Adobe, Apple, Citrix, Microsoft y otros. Las tasas de SophosLabs parches como crítico, alto, medio y bajo y le dice que las amenazas de un parche evita de esta manera puede identificar los más importantes.

- **Filtrado Web.-** Con esta función se puede restringir el acceso a ciertas categorías de sitios web con el fin de controlar el uso de Internet y evitar cualquier impacto en la productividad laboral, esta función es compatible con los cinco principales navegadores: Internet Explorer, Firefox, Chrome, Safari y Opera.

  El filtrado Web e puede utilizar en dos configuraciones diferentes:

  1. Punto final sólo para controlar el uso de páginas web inapropiadas que no requiere ningún hardware o software adicional.
  2. Web Protection Suite sincroniza inmediatamente con puntos finales a través de la nube eliminando el número de dispositivos de puerta de enlace necesarios.

- **Cifrado Integrado.-** Encriptación de disco completo integrado en 10 puntos finales sin una implementación independiente o consola, la instalación de encriptación de discos se hace con tan solo 6 clics.

La evaluación de parches, Control Web y funciones integradas de cifrado se no se incluye con todas las licencias. Si se desea usar se debe modificar la licencia.

- **Mejoras de las Funciones.-** Pues bien he mencionado algunas funciones importantes en esta versión, ahora veremos brevemente algunas de muchas mejoras en las funciones con versiones anteriores.

- **Mejora en Consola de Instalador**

  - Menos reinicios necesarios cuando se actualiza.
  - El Asesor de actualizaciones no es un programa independiente y ahora se ejecuta durante la instalación y por lo tanto no tiene que ser ejecutado antes de la instalación.
  - Durante la instalación, puede seleccionar una instancia existente de SQL Server para la base de datos de Sophos u optar por crear una instancia SOPHOS nuevo.

- **Mejoras en Consola a Nivel General**
  - Función de búsqueda en la consola para localizar un ordenador, por dirección IP o nombre de host, o el rango de computadoras por nombre de host
  - Importar o exportar exclusiones de un Anti-Virus y la política de la IS
  - Selección múltiple de alertas y errores.
  - Management Console cuenta con una nueva combinación de colores y la iconografía, pero no hay un cambio significativo en la composición.

- **Mejoras EndPoint**
  - Más rápido para computadoras.
  - El aumento en acceso y en demanda rendimiento de lectura.
  - Protección Web de análisis de contenido ha sido re-escrito y ya no depende de Browser Helper Objects, que sólo son aplicables a Internet Explorer. Exploración Web de contenido ahora es compatible con todos los navegadores principales de Internet Explorer, Firefox, Chrome, Safari y Opera y sin dependencia BHO por lo que es más seguro ya prueba de manipulaciones.
  - Buffer Overflow Protección para Windows Vista, Windows 7 clientes bajo equipos de 64 bits).

  La configuración del escáner en acceso por defecto se establece ahora para la mejor protección.

- **Mejora en Análisis Automático o Programado:** La opción 'Limpiar automáticamente elementos con virus / malware' está habilitada para nuevos análisis automático.
- **Mejora en Alerta de Virus al Usuario** Ya sea que una amenaza se ha limpiado o no el usuario final verá un mensaje de globo asesoramiento de la detección, y que ha sido trasladado al área de cuarentena.
- **Mejora en Consola de Informes de Virus.-** Debido al cambio de permitir la limpieza automática, alertas de virus que corresponden a una amenaza que se ha afrontado con éxito, no aparecerá en la interfaz de la consola y no habrá advertencia que se muestra en contra de la computadora. Sin embargo, usted podrá ver las detecciones y las acciones bajo los detalles

del equipo para un equipo de referencia y las detecciones aparecerá en ninguna amenaza informa de ejecutar.

2.6.4 Tercer Lugar: F-Secure: Client Security 9.31

Fig. 11. Logo F-Secure: Client Security 9.31

Fuente: www.f-secure.com

Como su frase lo dice es un antivirus para las empresas de todos los tamaños**, e**s un software propiamente para brindar alta seguridad a ordenadores portátiles como de trabajo.

Funciones Importantes en éste Antivirus: Entre sus funciones importantes a parte de las que viene ya incorporado un antivirus a nivel de usuario final como son antispam, antipishing, protección de correo, protección en tiempo real, etc. F-Secure: Client Security 9.31 destaca modulos adicionales como son:

- **Exclusiones de Procesos**: puede excluir procesos de confianza del análisis en tiempo real.
- **DNS Intervalo de Actualización**: se puede configurar la frecuencia con la que desea resolver direcciones IP de nombres DNS, que se especifican en las reglas del firewall F-Secure.
- **Protección a Nivel de Red**: para estaciones de trabajo asegura el nivel de seguridad y ordenadores portátiles que se conectan a la red antes de concederles acceso.

- **Detecta y Bloquea a los Hackers:** y nuevos tipos de gusano, actualizaciones 2 veces por día.
- **Asegura el Nivel de Seguridad de Ordenadores Portátiles Remotos**: Que estén conectados a la red de la empresa fuera de oficinas antes de concederles acceso usando a través del modulo Cuarentena de Red.
- **Administración Central:** F-Secure Client Security puede ser remotamente instalado, configurado y controlado desde una ubicación central.

Plataformas Recomendadas.- También a continuación se destaca bajo que plataformas trabaja:

- Microsoft Windows XP con SP3 (x 32 bits)
- Microsoft Windows Vista (32-bit y 64-bit)
- Microsoft Windows Vista con SP1 o posterior (32-bit y 64-bit)
- Microsoft Windows 7 (32-bit y 64-bit)
- Microsoft Windows 7 con SP1 o posterior (32-bit y 64-bit)

2.6.5 Segundo Lugar: Symantec: Endpoint Protection 12.1

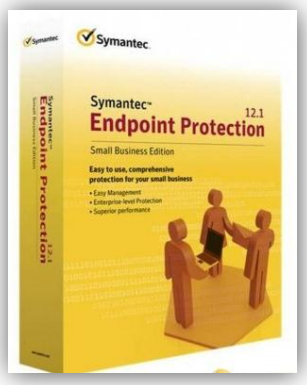


Fig. 12. Portada de Symantec: Endpoint Protection 12.1

Fuente: www.symantec.com

El producto Symantec EndPoint Protection 12.0 es una completa defensa inigualable contra software malicioso para ordenadores portátiles, ordenadores de mesa y servidores, utiliza la tecnología de Insight el cual es un panel de informes dinámico que ofrece información en tiempo real sobre indicadores claves del rendimiento, ofrece una protección eficiente y confiable.

Principales Características:

- Elimina los códigos maliciosos, como virus, gusanos, troyanos, spyware, adware, bots y amenazas desconocidas y rootkits.
- Previene epidemias relacionadas con la seguridad, y reduce la carga administrativa.
- Protección fiable de los entornos físicos y virtuales.
- Reduce el coste total de propiedad de los sistemas finales

Funciones:

- Alta seguridad y rendimiento.
- Como cualquier antivirus actual traer integrado modulos de anti-spyware, firewall, prevención de intrusiones, aplicaciones y dispositivos de gestión.
- Ofrece una gestión centralizada de la seguridad en entornos físicos y virtuales final los sistemas Windows y Mac
- Actualizaciones instantáneas NAC auto-activation sin tener que instalar software adicional
- Este software antivirus ofrece una completa protección contra virus y spyware para plataformas Windows, Mac y Linux
- Diseñado para proteger su infraestructura virtual, es decir esta versión de antivirus es creado especialmente para entornos empresariales y por ende brinda una protección de los entornos físicos y virtuales.

2.6.6 Primer Lugar: Kaspersky: EndPoint Security 8.1

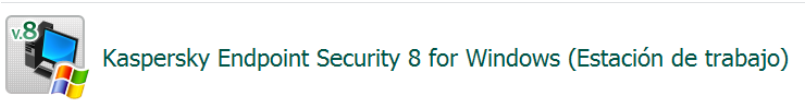


Fig. 13. Kaspersky: EndPoint Security 8.1

Fuente: www.kaspersky.com

Sin lugar a dudas la Kaspersky es una empresa de gran prestigio a nivel mundial por sus productos antivirus; y según la evaluación AV-TEST es el mejor evaluado a nivel corporativo ocupando el 1er lugar y el 2do lugar en protección orientada a nivel de usuarios

finales, ofreciendo soluciones que cumplen los estándares de funcionamiento que los que deben regirse los antivirus, además brinda una completa solución empresarial.

Kaspersky Endpoint Security 8 es un software multifuncional de protección de datos en las redes corporativas.

La aplicación proporciona una protección contra virus y otros malware, amenazas desconocidas y estafas en Internet. Además permite controlar la ejecución de aplicaciones por los usuarios, y su acceso a dispositivos y recursos de red.

La combinación de medios de protección cubre todos los canales de recepción y transmisión de datos. La configuración flexible a todos los componentes de protección y control permite adaptar Kaspersky Endpoint Security 8 a las necesidades de cualquier organización.

2.7 Vulnerabilidades en Antivirus

Según SECUNIA, la mayoría de grandes antivirus no están preparados para cubrir los exploits, y que siguen anclados en la heurística y en la protección sólo frente a archivos descargados en el ordenador. Esa acusación de falta de visión ha molestado mucho a las empresas analizadas en el estudio y sus reacciones no se han hecho esperar.

Lo primero que han hecho es leer con atención el estudio de **SECUNIA**: Según ellos, la manera de utilizar los antivirus no ha sido la correcta. Al parecer han escaneado el código malicioso sin tener en cuenta las herramientas de las suites que, justamente, protegen de las vulnerabilidades.

También se han quejado de que el análisis se hace “en frío”, es decir, sin que se intente ejecutar dicho código. La mayoría de los antivirus funcionan cuando el código se activa,

así que de esa forma era difícil que actuaran de algún modo.

2.7.1 ¿Que es Vulnerabilidad en Antivirus Informáticos?

En informática son errores, brechas en los antivirus que permiten el ingreso desde el exterior a programas considerados dañinos, los mismos que han sido desarrollados por personas que buscan múltiples objetivos, que van desde dañar los sistemas operativos, sistemas de información, también buscan obtener acceso a información confidencial de la empresa atacada con varios fines, obtener ventajas competitivas, causar daños, etc.

Según la informes de una página web con fecha 22-03 del presente año dos investigadores de seguridad de la Universidad de Texas han presentado un informe en el cual se dan a conocer 45 formas de engañar a 38 de los motores de antivirus mas importantes a nivel mundial.

La mayoría de vulnerabilidades detectadas están relacionadas con el tratamiento de cierto tipos de ficheros que permiten que malware pase sin ser detectado por el motor del antivirus convirtiéndose en una herramienta inocua ante esta amenaza

Nos muestra una lista con orden relevante de los ficheros manipulables que tienen las extensiones .tar, .elf, .exe, Ficheros Microsoft Office, .rar, .cab, .chm, .gzip y .zip.

Antivirus	Número de vulnerabilidades
eSafe:	22
QuickHeal	20
Rising Antivirus	20
Emsisoft	19
Ikarus Virus Utilities T3 Command Line Scanner	19
Panda Antivirus	19
Norman Antivirus	18
Fortinet Antivirus	17
Sophos Anti-Virus	16
McAfee Gateway	13
Kaspersky Anti-Virus	11
McAfee Anti-Virus Scanning Engine	11
NOD32 Antivirus	11
F-Prot	10
Command Antivirus	10
AVEngine	9
Antiy Labs AVL	9
Jiangmin Antivirus	9
AhnLab	8
BitDefender	8
Comodo	8
F-Secure	8
Trend Micro	8
K7 Antivirus	7
PC Tools AntiVirus	7
AVG	6
Clamav	5
ClamAV	5
Microsoft Security Essentials	5
nProtect Anti-Virus	5
VBA32	5
Avira AntiVir	4
Avast	3
Dr.Web	3
eTrust Vet Antivirus	3
G Data AntiVirus	3

Tabla 4. Vulnerabilidades en antivirus a nivel general

Fuente: http://www.identi.li/index.php?topic=67312

2.7.2 ¿Qué Consecuencias traen las Vulnerabilidades en Empresas?

Si bien las empresas de gran tamaño son más propensas a grandes ataques informáticos, las empresas de pequeño y mediano tamaño se han registrado con un porcentaje por día del 36 % en ataques de software malicioso.

Como lo menciona un editorial en internet hoy en día la información es sinónimo de poder y los atacantes lo saben, por tal motivo aquellos ataques exitosos pueden generar desde un simple alimento de ego del atacante hasta lograr tener ventajas financieras significativas para los criminales cibernéticos que realizan los ataques.

- Simplifican un ataque, permitiendo a los crackers obtener más permisos en el equipo víctima y poder usarlo al libre albedrío
- El sistema puede ejecutar automáticamente códigos maliciosos, abrir puertos, o en algunos casos es el almacenamiento incorrecto de datos privados, como contraseñas

2.8 Marco Legal

Tanto en el software propietario como en el libre, la licencia de uso es el instrumento legal por el cual el proveedor permite el uso del software a terceros, los usuarios. Pero el esquema de derechos y limitaciones cambia completamente según si se trata de una licencia de software propietario o de software libre.

2.9 Marco Espacial

El análisis tiene como objetivo aplicar un folleto informativo y orientativo a las empresas a nivel nacional a tomar decisiones o mejorar el esquema actual, en cuanto a seguridades brindadas por los antivirus objetos de estudio y riesgos a los que se encuentran propensos.

CAPITULO III

3 METODOLOGÍA

3.7 Proceso de Investigación

3.7.1 Unidad de Análisis

Se tomará como unidad de análisis, empresas corporativas que representan el universo, más específicamente en la Ciudad de Cuenca, la investigación estará basada en la evaluación de vulnerabilidades de los mejores antivirus corporativos obtenidas de una exploración de campo en la empresa ACSAM Consultores Cía. LTDA, entre otras y también basándonos en datos de Internet.

3.7.2 Tipo de Investigación

Se usaran los siguientes tipos de investigación:

- **Campo:** Es necesario hacer este tipo de investigación para poder observar, realizar estudios propios en el área misma de las empresas.
- **Descriptiva:** El proyecto al ser un análisis de vulnerabilidades de los mejores antivirus usados a nivel corporativo, es necesario realizar un folleto descriptivo de las vulnerabilidades dadas en los objetos de investigación, con el objetivo de informar y orientar a las empresas sobre recomendaciones que podrían mejorar la seguridad.
- **Aplicada:** Objetivo final realización de folleto sobre el análisis y aplicarla a las empresas corporativas.

3.7.3 Método

Se usará los siguientes métodos:

- **Inductivo:** Necesario aplicar este método ya que la investigación será de lleno, en el área de investigación.
- **Deductivo:** Porque necesitamos basarnos en otras fuentes que no necesariamente serán el área propia de investigación y sacar nuestras conclusiones en base a este método aplicado.

3.7.4 Técnica

Se usara las siguientes técnicas de recolección de información:

- **Entrevistas:** A usuarios del software antivirus en la empresa, con el director de departamento de sistemas.
- **Encuestas:** De igual manera a usuarios del software antivirus en las empresas objeto de estudio.
- **Observación directa:** Se lo aplicará en mayor parte en las mismas empresas fuentes de información, y en menor parte en instalación propia de estos antivirus para poder realizar una evaluación más minuciosa.

3.7.5 Instrumento

- En las encuestas se usara un cuestionario de encuestas.
- En las entrevistas se usará un cuestionario de entrevistas
- Y para observación directa se usarán fichas de Observación.

CAPITULO IV

4 RESULTADOS

4.1 Análisis de Vulnerabilidades en Mejores Antivirus 2012 para poder dar un Informe y Realización de un Folleto Informativo.

Para poder realizar esta parte práctica es necesario basarnos en varios métodos propuestos con anterioridad para obtención de datos que nos ayuden a tener una mejor visión de la situación en las empresas y los antivirus a someterse a análisis de vulnerabilidades:

- Procederemos a la realización de una encuesta en empresas, con puntos generales para poder obtener una visión general del software antivirus con la que cuentan las empresas. Además poder determinar en base a esta técnica si el software antivirus usado en las empresas es realmente para las necesidades requeridas; es decir si empresas usan antivirus corporativos o están usando antivirus normales "Usuario Final".

Las encuestas se las realizo en las siguientes empresas:

- ACSAM Consultores Cía. LTDA: Empresa Consultora de Ingeniería Civil.
- ACSAM Consulproy Cía. LTDA.: Empresa Consultora de Ingeniería Civil.
- BC Compu: Empresa de Venta de equipos informáticos y Suministros.
- Constructora Chaca: Empresa Consultora de Ingeniería Civil.
- Cerámicas Rialto S.A: Empresa Industrial en Elaboración de Cerámica.
- MotorAlmor: Empresa de Servicio en Sistemas informáticos.
- EL HIERRO: Centro Comercial.

- COORDINACION ZONAL 6 MIES AZUAY: Ministerio de Inclusión Económica y Social Azuay Zona 6.
- Graficompu: Empresa de venta de equipos informáticos y suministros.

Los resultados obtenidos por pregunta son los siguientes:

1. **Porcentaje de empresas que usan antivirus corporativos**

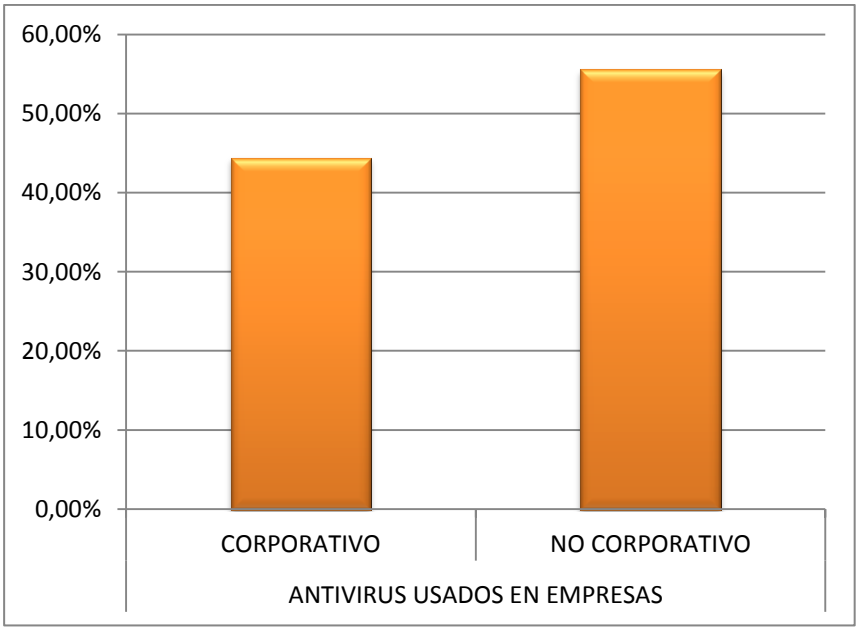


Fig. 14. Empresas que usan antivirus corporativos

El porcentaje de empresas que usan antivirus corporativos es 44,40% frente a un 55,60% que no usan antivirus corporativos

2. ¿Antes de adquirir un antivirus que parámetros analiza?

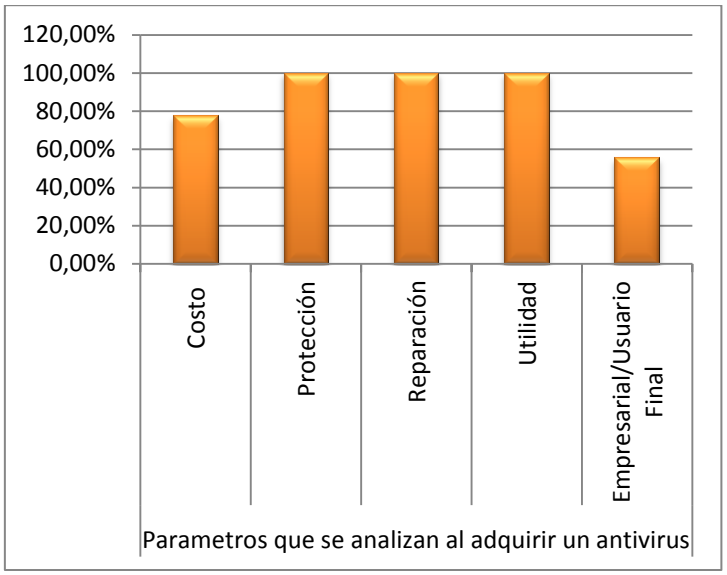


Fig. 15. Parámetros que se analizan antes de adquirir un antivirus

Los resultados obtenidos en esta pregunta son:

Costo: 78,80%

Protección: 100%

Reparación: 100%

Utilidad: 100%

Empresarial o Usuario Final: 55,60 %

3. **¿En su empresa se usa algún complemento adicional para maximizar la seguridad a parte del software antivirus?**

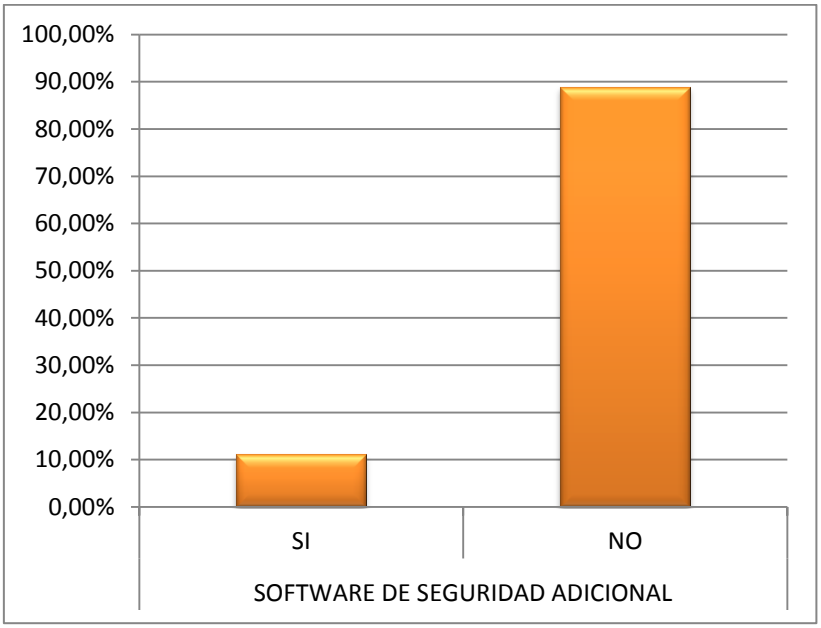


Fig. 16. Complemento adicional para maximizar la seguridad en empresas

Los resultados obtenidos son los siguientes:

Un 88,90 % no usa algún software de seguridad adicional frente a un 11,10% que si lo usa.

4. **¿Han sufrido ataques o infiltraciones de software malicioso?**

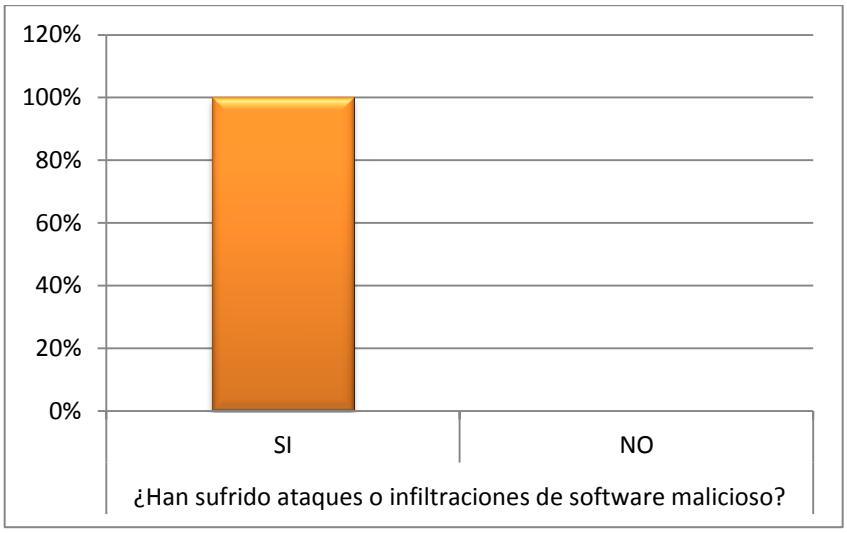


Fig. 17. Porcentaje de empresas que han sufrido ataques de software malicioso

Los resultados indican que todas las empresas en alguna ocasión han sufrido ataques de virus o software malicioso con un 100 %

5. **¿Esta satisfecho con su antivirus corporativo actual?**

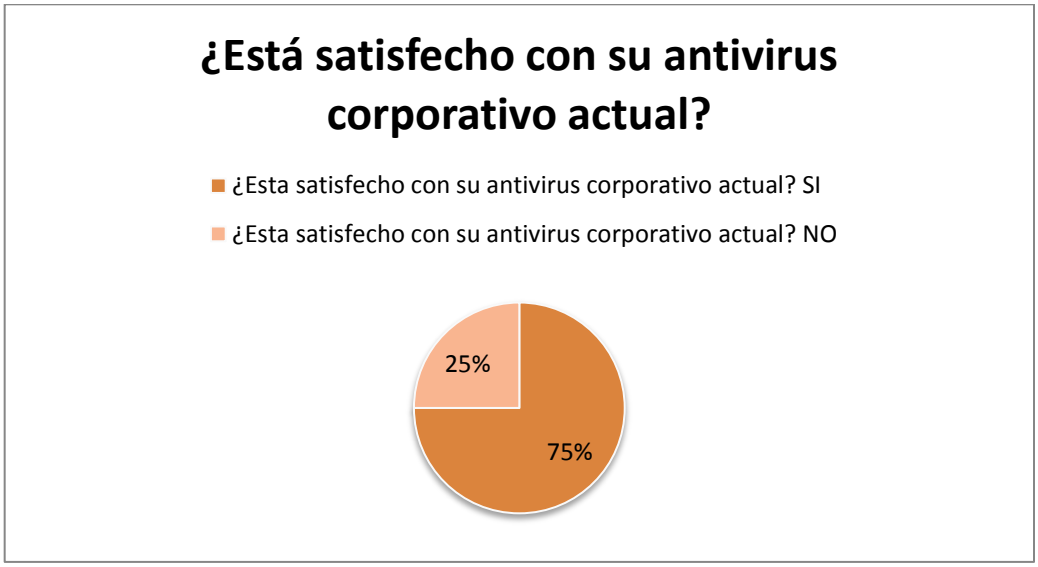


Fig. 18. Porcentaje de conformidad de antivirus corporativo actual

De las encuestas realizadas solo tomando los resultados de las empresas que utilizan antivirus corporativo tenemos que el 75% esta conforme con la seguridad que brinda su antivirus frente a un 25% de empresas que no están conformes.

4.2 Prueba de Vulnerabilidades en Windows 7 32 bits.

Para poder determinar vulnerabilidades en los antivirus se basará de manera un tanto general al método usado por AV-TEST teniendo en cuenta que este tipo de análisis no se podrá comparar con el análisis realizado por AV-TEST ya que existen muchos expertos trabajando y realizando pruebas continuas con ataques de cientos de virus, etc.

1- Buscar vulnerabilidades en base a 3 parámetros usados por AV-TEST:
2- Empezamos por evaluar cada antivirus en cuanto a protección que brinda a los ordenadores, esto implica evaluar:
    - Detección y eliminación de software malicioso.
    - Archivos infectados provenientes de dispositivos externos
    - Firewall y su protección.
    - Amenazas provenientes de correos electrónicos en archivos adjuntos.
    - Actualizaciones por día.
    - Protección en tiempo real.

Una vez definido los parámetros de evaluación en base a protección se pasara a la evaluación de los antivirus en base a su capacidad de REPARACION, tomando en cuenta los siguientes lineamientos:

- La evaluación se la realiza en un Sistema Operativo que ya este infectado o haya sido infectado y se tomara en cuenta la capacidad de reacción que

tiene el antivirus ante el software malicioso.

- Evaluación de la capacidad de eliminar software malicioso activo.
- Evaluación de reparación de los cambios que afectaron al sistema.
- Evaluación de la capacidad para localizar y eliminar software malicioso que se hayan escondido como rootkits.

Y como último punto de evaluación tenemos UTILIDAD, en esta sección se trata d evaluar parámetros como:

- Influencia que causa el antivirus en la utilidad del sistema
- Mensajes de advertencia, avisos generales, bloqueos, falsos positivos durante el análisis del sistema.
- Ordenador lento durante su uso, es decir la carga sobre el sistema operativo.

Para poder evaluar en un periodo de tiempo establecido los antivirus se instalo en 3 máquinas Windows 7 Profesional 32 bits para objetos de estudio y para determinar si existen vulnerabilidades en dichos antivirus.

Día	**Antivirus empresariales**	**Parámetros a evaluar**
1	Webroot: Secure Aywhere Endpoint Protection 8.0	Protección, Reparación, Utilidad
2	Microsoft: Forefront Endpoint Protection 2010	
3	Sophos: Endpoint Security and Control 10.0	
4	F-Secure: Client Security 9.31	
5	Symantec: Endpoint Protection 12.1	
6	Kaspersky: EndPoint Security 8.1	

Tabla 5. Cronograma de evaluación de antivirus

Listado de algunos virus usados para realizar ataques y poder evaluar la reacción de

cada uno de los antivirus objetos de estudio.

Virus/spyware	W32/AutoRun-BQJ	G:\System Volume Information_restore{9259FEB0-700C-45C3-AAAC-D520FAC14C3F}\RP120\A0041864.lnk
Virus/spyware	Troj/Keygen-DJ	G:\kariC\Autodesk\AutoCAD_2010_Spanish_MLD_WIN_32bit\xf-a2010.exe
Virus/spyware	Troj/Crack-AJ	G:\BIBLIOTECA DE PROGRAMAS\SISTEMAS OPERAT\Windows Vista Activation 2008\Activation.exe
Virus/spyware	Mal/Scribble-D	G:\System Volume Information_restore{96ED533F-4CAF-439C-BA52-05A5A4DA133B}\RP138\A0024612.exe
Virus/spyware	Mal/Keygen-K	G:\BIBLIOTECA DE PROGRAMAS\PROGRAMACION\DREAM WEAVER 8\KEYGEN.EXE
Virus/spyware	Mal/Generic-S	G:\karin\doc\Descargas\etypesetup.exe
Virus/spyware	Mal/Generic-L	G:\BIBLIOTECA DE PROGRAMAS\PASSW ARCHIVOS\Androsa\afp_1.4.2.exe
Virus/spyware	Mal/Fear-A	G:\KARIESC\DOCUMENTOS ESCRITORIO\Auto Cad 2006\Autodesk Autocad 2006 Keygen.exe
Adware/PUA	Solimba Installer	Otro
Adware/PUA	RemoveWAT	Herramienta de ataque remoto
Adware/PUA	NirSoft	Herramienta de ataque remoto
Adware/PUA	Generic PUA NL	Otro
Adware/PUA	DomainIQ pay-p...	Otro

Fig. 19. Virus usados para evaluación de antivirus corporativos

4.3 Descarga, Instalación y Análisis de Antivirus Corporativos

Se procedió a descargar e instalar versiones de prueba de los mejores antivirus a nivel corporativo según AV-TEST.

4.3.1 Kaspersky: EndPoint Security 8.1

Fig. 20. Proceso de descarga de Kaspersky versión corporativa

Fuente: http://www.kaspersky.com/downloads/productupdates/endpoint-security-windows

Resultados del Antivirus Kaspersky: Endpoint Security 8.1.- Se realizo la evaluación en el periodo determinado y concluimos con el siguiente resultado:

Protección:

Parámetro	Resultado W 7 x32		Comentarios / Detalle Vulnerabilidad Encontrada
	Aprobado	Reprobado	
Detección y eliminación de software malicioso		X	Exploración de archivos con extensiones largas, error de lectura al tratar de acceder a ciertos archivos
Archivos infectados provenientes de dispositivos externos	X		Sin novedades
Firewall y Protección en navegación WEB.		X	Fallo al analizarse el trafico de determinados sitios web
Amenazas provenientes de correos electrónicos en archivos adjuntos	X		Sin novedades
Actualizaciones por día.	X		Sin novedades, primera vez dio error de actualización.
Protección en tiempo real	X		Sin novedades

Tabla 6. Vulnerabilidades en Kaspersky Endpoint Security 8.1 en base a protección

Análisis: En base a parámetros de evaluación el antivirus ha encontrado 2 vulnerabilidades a nivel de PROTECCION, Kaspersky: EndPoint Security 8.1 presenta fallos al analizar el tráfico de determinados sitios web, esto implica una brecha de posibles infiltraciones y ataques provenientes de internet y pondría en riesgo el Sistema Operativo como los datos de la empresa que son los mas importantes y segunda vulnerabilidad esta dada con el análisis de algunos archivos con extensiones muy largas error al tener acceso en análisis esto también se torna en un peligro para los datos de la empresa ya que puede ser que en dichos archivos este filtrándose información y dañando al sistema.

Reparación:

Parámetro	Resultado W 7 x32		Comentarios / Detalle Vulnerabilidad Encontrada
	Aprobado	Reprobado	
Capacidad de reacción que tiene el antivirus ante el software malicioso	**X**		Sin novedades
Capacidad de eliminar software malicioso activo	**X**		Sin novedades
Reparación de los cambios que afectaron al sistema	**X**		Sin novedades
Capacidad para localizar y eliminar software malicioso que se hayan escondido como rootkits	**X**		Sin novedades

Tabla 7. Vulnerabilidades en Kaspersky Endpoint Security 8.1 en base a reparación

Análisis: En cuanto a reparación respecta Kaspersky es una de las mejores opciones, excelente herramienta**,** detecta virus que están en el sistema operativo infectado para poder observar su forma de reacción y reparación de ficheros dañados, como el AutoKSM.EXE que es un autoejecutable para activación de Office y su posterior eliminación y trata de reparar los cambios que afectaron al sistema además muy excelente buscador y eliminación de rootkits que son software malicioso que permanecen ocultos en el sistema.

Utilidad:

Parámetro	Resultado W 7 x32		Comentarios / Detalle Vulnerabilidad Encontrada
	Novedad	Sin Novedad	
Influencia que causa el antivirus en la utilidad del sistema		X	- Error de exploración de disco no se ejecuta al arrancar el sistema después de ejecutar chkdsk /f. - Error en 1era. Actualización después de la instalación. - Tareas de actualización locales no se actualizan después de crear alguna política en el centro de seguridad
Mensajes de advertencia, avisos generales, bloqueos, falsos positivos durante el análisis del sistema		X	Opción posponer tarea programada causa mensaje de rendimiento fijo incorrecto.
Ralentizamiento del ordenador durante su uso, es decir la carga sobre el sistema operativo	X		Sin novedad

Tabla 8. Vulnerabilidades en Kaspersky Endpoint Security 8.1 en base a utilidad

Análisis:

En cuanto a utilidad, recursos que ocupa en el sistema, mensajes a nivel general puedo decir que:

Esta versión corporativa ENDPOINT a diferencia de otros productos Kaspersky donde primaba el gran consumo de recursos a nivel de hardware es mucho mas ligera y versátil con una consola de administración ni mucho ni poco fácil de uso pero también se toma en cuenta que este tipo de software es y debe ser administrado por un experto de sistemas.

En cuanto a la influencia que causa el antivirus en la Utilidad del sistema se presenta lo siguiente:

1. Error de exploración de disco no se ejecuta al arrancar el sistema después de ejecutar chkdsk /f.

   Este mensaje se da cuando se quiere hacer una comprobación de disco, se detiene el motor de exploración de Kaspersky por ciertos minutos tornándose un tanto peligrosa para posibles infiltraciones que pueden aprovechar a penas segundos para causar daños.

2. Error en primera actualización después de la instalación.

   Este mensaje aparece después de la instalación y se procede a su actualización del motor de base de datos del mismo, desde mi punto de vista un antivirus de ese nivel no debería darse esta tipo de error además se torna lento en recopilar información y enviar a los laboratorios de Kaspersky.

3. Tareas de actualización locales no se actualizan después de crear alguna política en el centro de seguridad.

   Mensaje de error luego de agregar una tarea programada en el centro de seguridad, esto crea confusión al usuario ya que según la interfaz no se actualiza o agrega la nueva tarea además crea inseguridad e inconsistencia en la protección.

Por ultimo al momento que posponer una tarea programada el software envía el siguiente mensaje “mensaje de rendimiento fijo incorrecto”.

4.3.2 Symantec: Endpoint Protection 12.1

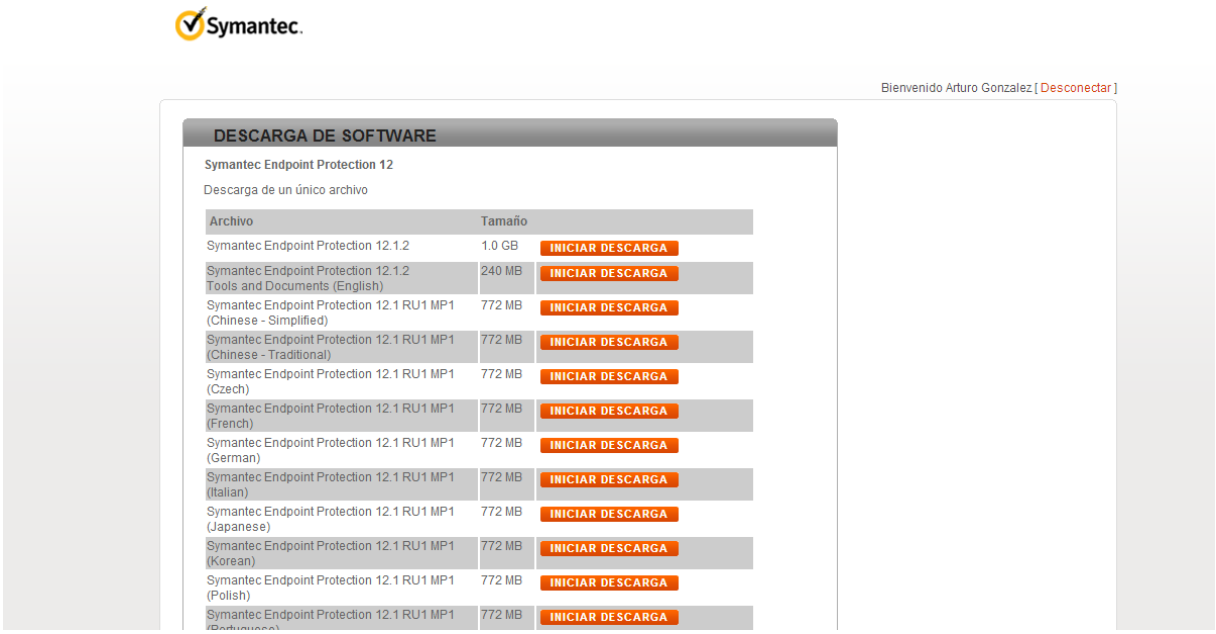


Fig. 21. Proceso de descarga de Symantec versión corporativa

Fuente: http://www.symantec.com/business/support/index?page=content&id=AL1284

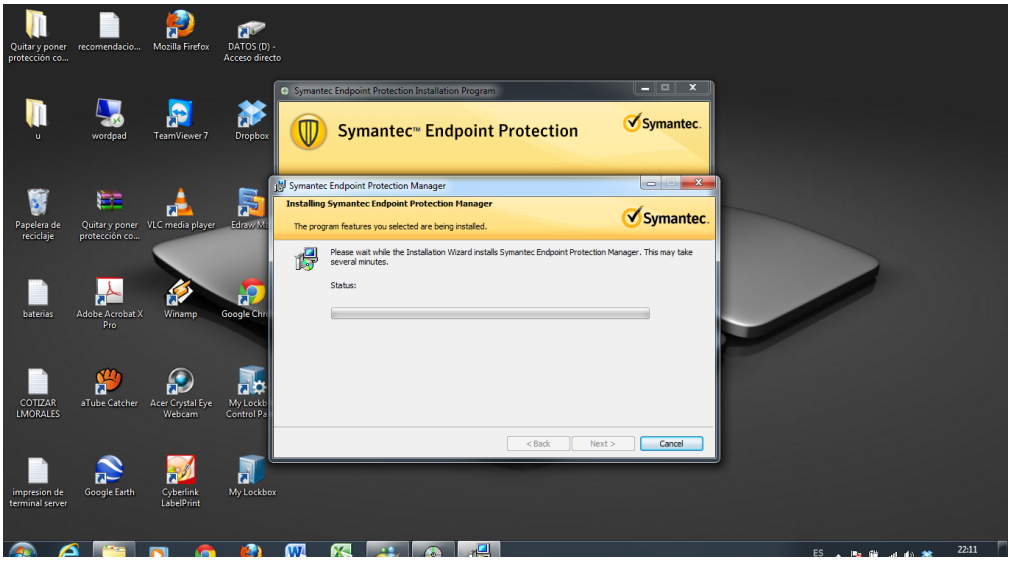


Fig. 22. Proceso de instalación de Symantec versión corporativa

Resultados del Antvirus Symantec: Endpoint Protection 12.1.- Se realizo la evaluación en el periodo determinado y concluimos con el siguiente resultado:

Protección:

Parámetro	Resultado W 7 x32		Comentarios / Detalle Vulnerabilidad Encontrada
	Aprobado	Reprobado	
Detección y eliminación de software malicioso	**X**		Sin novedades
Archivos infectados provenientes de dispositivos externos		**X**	No detección de virus troyano proveniente de un disco duro externo
Firewall y Protección en navegación WEB.	**X**		Sin novedades
Amenazas provenientes de correos electrónicos en archivos adjuntos	**X**		Sin novedades
Actualizaciones por día.		**X**	Al actualizar de forma manual simplemente dice que todo esta al día y se cierra
Protección en tiempo real	**X**		Sin novedades

Tabla 9. Vulnerabilidades en Symantec: Endpoint Protection 12.1en base a protección

Análisis: En cuanto a protección respecta **Symantec: Endpoint Protection 12.1** no fue capaz de detectar el mismo archivo malicioso usado para pruebas con Kaspersky desde un disco externo pero lo detecto al momento de abrir la carpeta contenedora del virus informático considerando una vulnerabilidad en infiltración de virus al sistema lo cual se convierte en una amenaza para los datos de la empresa que podría dar acceso exterior o llegar incluso a perder dichos datos de forma permanente, además se ha encontrado error al momento de intentar actualizar de forma manual no se actualiza simplemente visualiza que no es necesario actualizar y se cierra el antivirus, es un error de programación del antivirus ya que en forma automática se actualiza pero de forma manual no dejando una brecha de

inseguridad al no actualizar su base de datos.

Reparación:

Parámetro	Resultado W 7 x32		Comentarios / Detalle Vulnerabilidad Encontrada
	Aprobado	Reprobado	
Capacidad de reacción que tiene el antivirus ante el software malicioso	**X**		Sin novedades
Capacidad de eliminar software malicioso activo	**X**		Sin novedades
Reparación de los cambios que afectaron al sistema	**X**		Sin novedades
Capacidad para localizar y eliminar software malicioso que se hayan escondido como rootkits	**X**		Sin novedades

Tabla 10. Vulnerabilidades en Symantec: Endpoint Protection 12.1en base a reparación

Análisis: En cuando a reparación es una de las mejores opciones conjuntamente con Kaspersky no presenta vulnerabilidades en esta sección, excelente herramienta**,** detecta y elimina virus sobre el ordenador infectado previamente como archivos ocultos como rootkits que son software malicioso oculto, usados para evaluar Kaspersky. A mi criterio podría decir que la protección que brinda Symantec Endpoint Protection en cuanto a reparación respecta esta a nivel de Kaspersky Endpoint Security 8.1

Utilidad:

Parámetro	Resultado W 7 x32		Comentarios / Detalle Vulnerabilidad Encontrada
	Novedad	Sin Novedad	
Influencia que causa el antivirus en la utilidad del sistema	**X**		Sin novedades
Mensajes de advertencia, avisos generales, bloqueos, falsos positivos durante el análisis del sistema		**X**	Browser Network error: Mensaje erróneo al momento de tratar de crear una instalación para los clientes.
Ralentizamiento del ordenador durante su uso, es decir la carga sobre el sistema operativo		**X**	Requiere mínimo 4 GB de memoria RAM y microprocesador lo cual hace que el computador trabaje un poco lento, además en su desinstalación demora mucho.

Tabla 11. Vulnerabilidades en Symantec: Endpoint Protection 12.1en base a utilidad

Análisis: En cuanto a la utilidad este antivirus es bastante versátil y tiene mas ventajas que desventajas pero sin embargo no esta exento de ciertos errores y vulnerabilidades, ocupa bastantes recursos en el sistema por lo cual hace que el sistema se ralentice, también se pudo observar un mensaje erróneo al momento de crear un instalador para las maquinas clientes, y por ultimo punto al momento de proceder a su desinstalación se demora y vuelve el ordenador lento.

4.3.3 F-Secure: Client Security 9.31

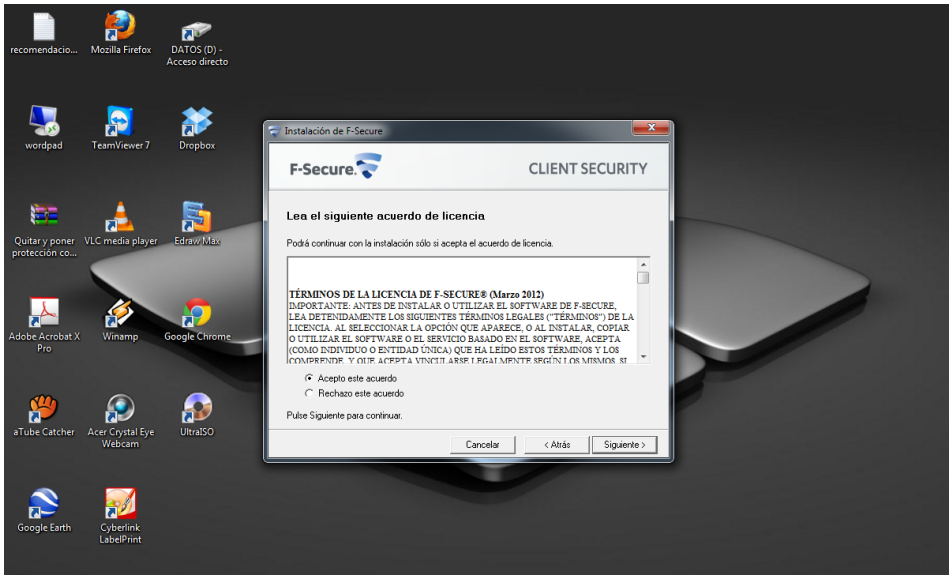


Fig. 23. Proceso de instalación de F-Secure: Client Security 9.31

Resultados del Antivirus F-Secure: Client Security 9.31.- Se procedió a su evaluación se encontraron las siguientes vulnerabilidades:

Protección:

Parámetro	Resultado W 7 x32		Comentarios / Detalle Vulnerabilidad Encontrada
	Aprobado	Reprobado	
Detección y eliminación de software malicioso	X		Sin novedades
Archivos infectados provenientes de dispositivos externos	X		Sin novedades
Firewall y Protección en navegación WEB.		X	Firewall Daemon tiene problemas de apagado
Amenazas provenientes de correos electrónicos en archivos adjuntos	X		Sin novedades
Actualizaciones por día.	X		Sin novedades
Protección en tiempo real	X		Sin novedades

Tabla 12. Vulnerabilidades en F-Secure: Client Security 9.31 en base a protección

Análisis: En cuanto a protección respecta de este antivirus se han encontrado algunas vulnerabilidades como en la protección que brinda el firewall del mismo ya que el firewall Daemon tiene problemas de apagado; es decir se desactiva su protección este es un error del antivirus que acarrea una vulnerabilidad para el sistema operativo y los datos manejados por la empresa ya que al no tener firewall activado se pueden dar infiltraciones de software malicioso provenientes de la Web.

Reparación:

Parámetro	Resultado W 7 x32		Comentarios / Detalle Vulnerabilidad Encontrada
	Aprobado	Reprobado	
Capacidad de reacción que tiene el antivirus ante el software malicioso		X	Permite la filtración de virus troyanos los elimina pero no repara los ficheros dañados.
Capacidad de eliminar software malicioso activo	X		Sin novedades
Reparación de los cambios que afectaron al sistema	X		Sin novedades
Capacidad para localizar y eliminar software malicioso que se hayan escondido como rootkits		X	No detecta archivos maliciosos ocultos rootkits que afectan al sistema y no repara ficheros dañados.

Tabla 13. Vulnerabilidades en F-Secure: Client Security 9.31 en base a reparación

Análisis: En cuando a reparación se concluye lo siguiente en cuanto a Reparación permite la infección de virus informáticos como troyanos a pesar de eliminarlos no es capaz de reparar los ficheros dañados causados por este tipo de ataque, además también permite la infiltración de software malicioso como rootkits en el sistema y tampoco es capaz de reparar los ficheros

dañados, esto deja vulnerabilidades graves en cuanto a seguridad y protección de los datos de la empresa.

Utilidad:

Parámetro	Resultado W 7 x32		Comentarios / Detalle Vulnerabilidad Encontrada
	Novedad	Sin Novedad	
Influencia que causa el antivirus en la utilidad del sistema	**X**		F-Secure Client Security Microsoft NAP plug-in permanece en el equipo cliente después de desinstalar Client Security a través de la consola de Policy Manager.
Mensajes de advertencia, avisos generales, bloqueos, falsos positivos durante el análisis del sistema	**X**		A pesar de descargarse una versión trial llenando los datos pide serial al momento de su instalación sin opción de instalarlo sino se coloca el mismo.
Ralentizamiento del ordenador durante su uso, es decir la carga sobre el sistema operativo	**X**		Ralentiza el ordenador

Tabla 14. Vulnerabilidades en F-Secure: Client Security 9.31 en base a utilidad

Análisis: En cuanto a la utilidad se ha encontrado 3vulnerabilidades como:

- Al momento de evaluar un antivirus se descarga una versión trial al igual que se realizo con los anteriores llenando los datos en la página oficial, los anteriores no piden serial pero F-Secure Client Security pide serial a pesar de ser una versión trial sin opción alguna de instalarlo como trial y si no se coloca el serial no se puede proceder con dicha instalación y se cierra esto es causado por falta de control en cuanto a roles que se da en las descargas este mensaje es muy molesto

para el usuario final de estar buscando la manera de completar la instalación además que es un error en muchos casos menos grave pero deja mucho que desear en lo que respecta a la utilidad sobre el sistema.

- F-Secure Client Security Microsoft NAP plug-in permanece en el equipo cliente después de desinstalar Client Security a través de la consola de Policy Manager: esta vulnerabilidad en la utilidad: esta vulnerabilidad se da cuando se desinstala un plug-in usando la consola de Administrador de Políticas el mismo no se desinstala, esto acarrea a que el antivirus se torne inestable ya que el usuario desea quitar dicho componente por cambio de necesidades en políticas y las mismas no se pueden desinstalar.
- Ocupa bastantes recursos del ordenador lo que da como resultado un antivirus un poco pesado para uso en donde se necesita la administración lo mas optima posible.

4.3.4 Sophos: Endpoint Security and Control 10.0

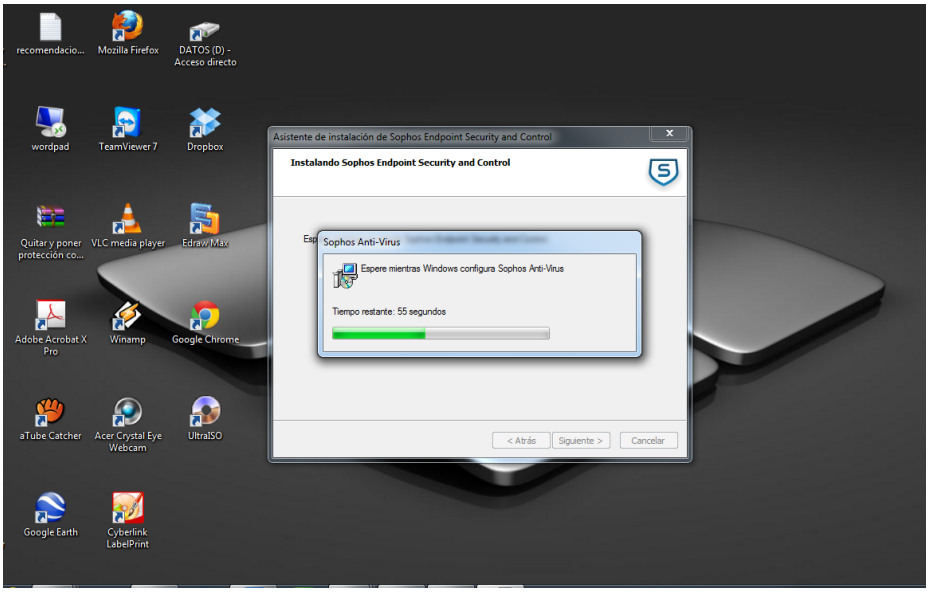


Fig. 24. Proceso de instalación de Sophos: Endpoint Security and Control 10.0

Resultados del Antivirus Sophos: Endpoint Security and Control 10.0.- Este antivirus a nivel empresarial se recomienda instalarlo en las versiones:

Windows Server 2003/2008/2008 R2 para obtener el mayor beneficio a nivel corporativo, sin embargo nuestra investigación esta orientada únicamente a entorno de Windows 7 así que la evaluación se la realizará basándose en dichos parámetros:

Protección:

Parámetro	Resultado W 7 x32		Comentarios / Detalle Vulnerabilidad Encontrada
	Aprobado	Reprobado	
Detección y eliminación de software malicioso	**X**		Sin novedades
Archivos infectados provenientes de dispositivos externos		**X**	No detecta virus troyano AutoInf-BF, Mal/Generic-S, Mal/Agent-ACR provenientes de discos un disco duro externo
Firewall y Protección en navegación WEB.		**X**	Antivirus no se activa automáticamente, necesita reinicio del sistema
Amenazas provenientes de correos electrónicos en archivos adjuntos	**X**		Sin novedades
Actualizaciones por día.	**X**		Sin novedades
Protección en tiempo real	**X**		Sin novedades

Tabla 15. Vulnerabilidades en Sophos: Endpoint Security and Control 10.0 en base a protección.

Análisis: Luego de instalar el antivirus y procedes a su evaluación tenemos:

- El firewall no se activa de forma predeterminada sino que se activa luego de reiniciar el sistema, esto es una vulnerabilidad que puede causar infiltraciones de software malicioso.
- Antivirus no detecta troyano, malware y spyware objetos de estudio provenientes de una unidad externa, consecuencias graves en el sistema.
- Por los demás puntos no hay inconveniente alguno.

Reparación:

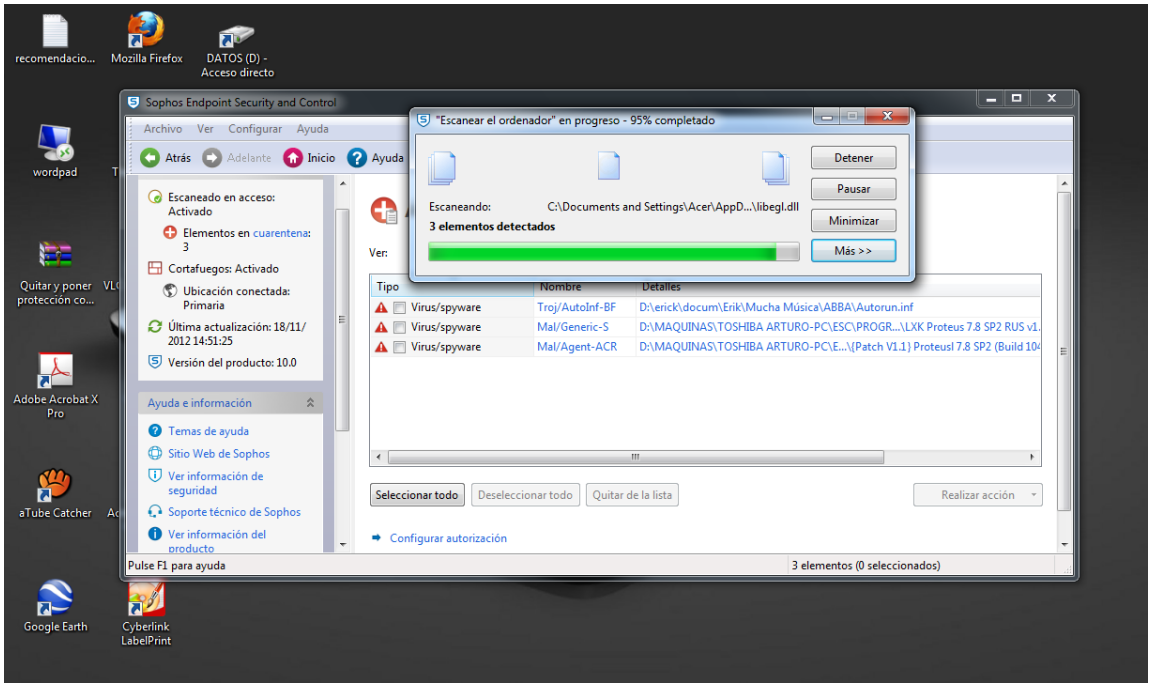


Fig. 25. Proceso de análisis de vulnerabilidades Sophos: Endpoint Security and Control 10.0

Parámetro	Resultado W 7 x32		Comentarios / Detalle Vulnerabilidad Encontrada
	Aprobado	Reprobado	
Capacidad de reacción que tiene el antivirus ante el software malicioso		X	No detecta mientras no se haga un análisis completo del sistema
Capacidad de eliminar software malicioso activo	X		Sin novedades
Reparación de los cambios que afectaron al sistema	X		Sin novedades
Capacidad para localizar y eliminar software malicioso que se hayan escondido como rootkits	X		Sin novedades

Tabla 16. Vulnerabilidades en Sophos: Endpoint Security and Control 10.0 en base a reparación.

Análisis: Buena reacción en cuanto a la reparación del sistema aunque no al 100%, detecta el software malicioso implantado ya en el sistema pone en cuarentena, da la opción al usuario de hacer una limpieza luego de haber enviado dicho software malicioso a cuarentena, además indica que tipo de software malicioso es y realiza reparación de ficheros, el único inconveniente y vulnerabilidad que presenta en esta sección es que para detectar el software malicioso activo ya implantado en el sistema requiere de un análisis profundo de forma manual del sistema ya que de forma automática no detecta el software malicioso con el que se realizo la prueba, también pondría en riesgo los datos y aumentaría en riesgo de sufrir ataques externos y daño en archivos.

Utilidad:

Parámetro	Resultado W 7 x32		Comentarios / Detalle Vulnerabilidad Encontrada
	Novedad	Sin Novedad	
Influencia que causa el antivirus en la utilidad del sistema	**X**		Sin novedades
Mensajes de advertencia, avisos generales, bloqueos, falsos positivos durante el análisis del sistema		**X**	Falso positivo de Shh/Updater-B
Ralentizamiento del ordenador durante su uso, es decir la carga sobre el sistema operativo	**X**		Sin novedades

Tabla 17. Vulnerabilidades en Sophos: Endpoint Security and Control 10.0 en base a utilidad.

Análisis: Detección de falso positivo de Shh y Updater-B esto se puede dar por causas propias del antivirus como la heurística que usan es la reacción que tienen los antivirus para bloquear archivos como si fuese virus, malware u otro tipo de amenaza, la heurística no es perfecta y causa este tipo de errores y vulnerabilidades en los antivirus, la causa de estos falsos positivos se da porque no se accede a una base de datos.

4.3.5 Microsoft: Forefront Endpoint Protection 2010.

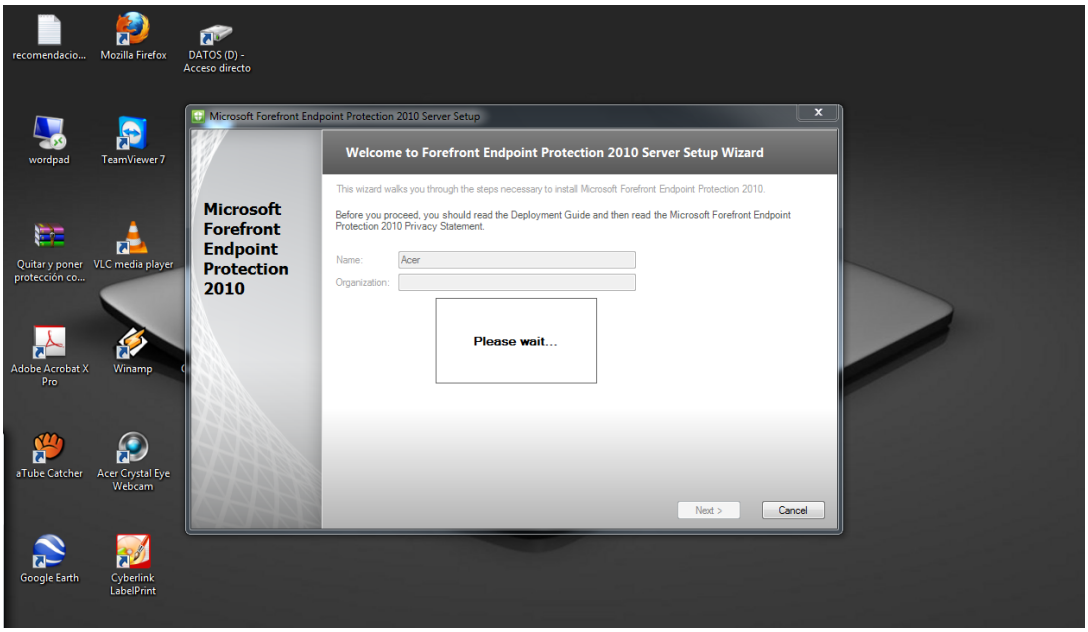


Fig. 26. Proceso de instalación Forefront Endpoint Protection 2010.

Resultado del Antivirus Microsoft: Forefront Endpoint Protection 2010.- Se analizo las vulnerabilidades en base a los 3 niveles de parámetros y se determino lo siguiente:

Protección:

Parámetro	Resultado W 7 x32		Comentarios / Detalle Vulnerabilidad Encontrada
	Aprobado	Reprobado	
Detección y eliminación de software malicioso		X	Presenta inconvenientes al momento del análisis proactivo Eliminación de software malicioso
Archivos infectados provenientes de dispositivos externos		X	Existe software malicioso que no es detectado al momento de insertar un disco duro externo de 1TB.

Firewall y Protección en navegación WEB.		**X**	No bloquea algunas páginas con contenido peligroso (emergentes) que detectadas por otros antivirus.
Amenazas provenientes de correos electrónicos en archivos adjuntos	**X**		Sin novedades
Actualizaciones por día.	**X**		Sin novedades
Protección en tiempo real		**X**	Existe carencia en este modulo, algunos virus no son detectados en tiempo real.

Tabla 18. Vulnerabilidades en Microsoft: Forefront Endpoint Protection 2010 en base a protección.

Análisis: Los resultados obtenidos según el estudio realizado es algo preocupante ya que en varios parámetros se encuentra filtraciones y no brinda una protección al 100%.

- Existe software malicioso que no es detectado al momento de insertar un disco duro externo de 1TB, esto provoca expansión de los virus desde dispositivos externos hacia el sistema y pone en riesgo la integridad de los datos.
- Inconvenientes en análisis proactivo y eliminación de algunos virus informáticos; esta vulnerabilidad también causa inseguridad en nuestras maquinas ya que deja abierta una brecha para posibles infiltraciones mas graves.

Reparación:

Parámetro	Resultado W 7 x32		Comentarios / Detalle Vulnerabilidad Encontrada
	Aprobado	Reprobado	
Capacidad de reacción que tiene el antivirus ante el software malicioso	**X**		Sin novedades
Capacidad de eliminar software malicioso activo	**X**		Sin novedades
Reparación de los cambios que afectaron al sistema	**X**		Sin novedades
Capacidad para localizar y eliminar software malicioso que se hayan escondido como rootkits		**X**	Rootkits y detección.

Tabla 19. Vulnerabilidades en Microsoft: Forefront Endpoint Protection 2010 en base a reparación.

Análisis: A pesar de que en la sección de PROTECCIÓN deja mucho que desear, en mucho compensa la capacidad que tiene el software para REPARAR y ELIMINAR software malicioso como virus activos; es decir que ya hayan existido antes de que sea instalado el antivirus y además estén causando aún daño en el sistema, el único inconveniente es que no detecta algunos rootkits aunque los que detectan sean reparados hay algunos que no detecta y que si han sido detectados por otros antivirus mencionados en este análisis a nivel corporativo.

Utilidad:

Parámetro	Resultado W 7 x32		Comentarios / Detalle Vulnerabilidad Encontrada
	Novedad	Sin Novedad	
Influencia que causa el antivirus en la utilidad del sistema		**X**	Sin novedades
Mensajes de advertencia, avisos generales, bloqueos, falsos positivos durante el análisis del sistema	**X**		Mensaje erróneo 0x80005000
Ralentizamiento del ordenador durante su uso, es decir la carga sobre el sistema operativo	**X**		Carga sobre el sistema operativo es relativamente intermedia.

Tabla 20. Vulnerabilidades en Microsoft: Forefront Endpoint Protection 2010 en base a utilidad.

Análisis: Se analizo en busca de vulnerabilidades en cuanto a las usabilidad o utilidad en el sistema y se encontró lo siguiente:

- La carga sobre el sistema operativo es relativamente intermedia por una parte este tipo de antivirus corporativos Endpoint son un poco mas pesados que los a nivel de usuarios final pero eso no es justificativo para que haya bastante carga en el sistema, por ejemplo el antivirus ENDPOINT de Kaspersky esta en 1er lugar y su carga del sistema es baja y brinda un protección, reparación y usabilidad excelente.
- Mensaje erróneo 0x80005000 la cuenta no puede ser determinada esto sucede al momento de proceder con la instalación sin embargo deja continuar con la instalación de manera normal, esto sucede por falta de control en los mensajes

del antivirus, siendo una deficiencia y vulnerabilidad a nivel de programación, en lo que respecta a la USABILIDAD no presenta vulnerabilidades mayores en donde presenta un poco de preocupación es el la PROTECCIÓN según AV-TEST tiene una puntuación 2/6 siendo una cifra preocupante.

4.3.6 Webroot: Secure Aywhere Endpoint Protection 8.0

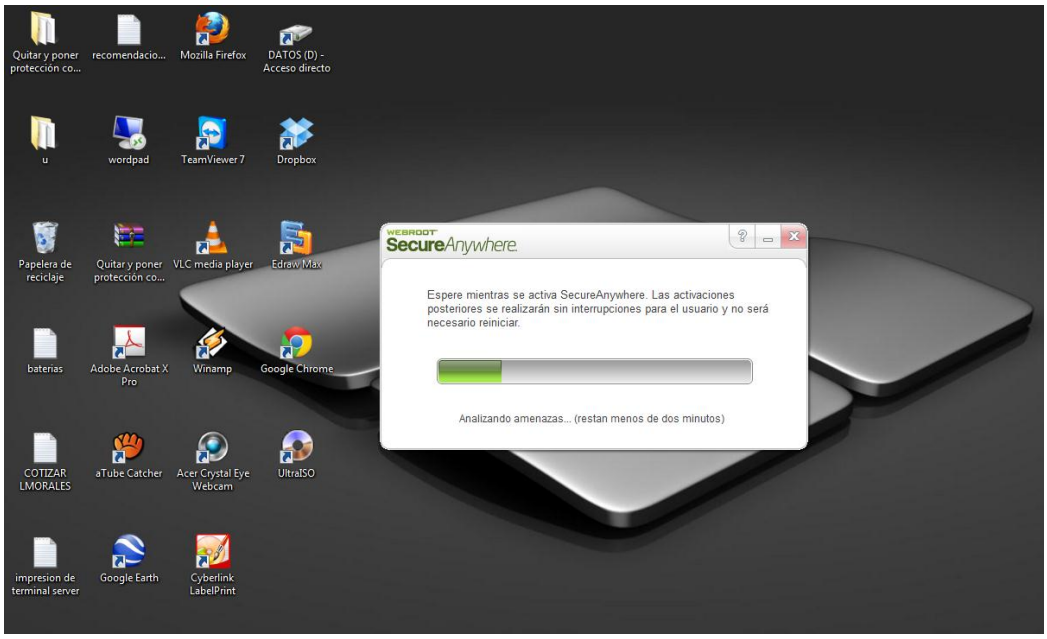


Fig. 27. Proceso de instalación y activación Webroot Endpoint, Consola web

Resultado del Antivirus Webroot: Secure Aywhere Endpoint Protection 8.0.- Se analizo las vulnerabilidades en base a los 3 niveles de parámetros y se determino lo siguiente:

Protección:

Parámetro	Resultado W 7 x32		Comentarios / Detalle Vulnerabilidad Encontrada
	Aprobado	Reprobado	
Detección y eliminación de software malicioso		X	No detecta 4 de 13 virus, spyware, malware usados para evaluación, los que detecta si los elimina.
Archivos infectados provenientes de dispositivos externos		X	También no detecto algunos virus expuestos desde el disco externo de 1TB. Usado para realizar dicha evaluación.
Firewall y Protección en navegación WEB.	X		
Amenazas provenientes de correos electrónicos en archivos adjuntos		X	Crack usado para activación de Windows 7 pasa inadvertido.
Actualizaciones por día.	X		Sin novedades
Protección en tiempo real		X	También existe carencia en este parámetro, algunos virus no son detectados en tiempo real.

Tabla 21. Vulnerabilidades en Webroot: Secure Aywhere Endpoint Protection 8.0 en base a protección.

Análisis: No brinda protección 100% efectiva al someter la protección del antivirus al sistema operativo que no ha sufrido ataques anteriormente, se introdujeron 13 tipos de virus, malware, spyware de los cuales fue capaz de detectar 9, deja brechas de seguridad para software malicioso que afecte al sistema operativo y la integridad de los datos

- Además se observo que no detectó algunos virus del anteriormente mencionado

colocados en el disco duro externo.

- Se procedió a enviar un troyano vía web correo electrónico y al momento de descargarlo ni descomprimirlo no lo reconoció como software malicioso.
- También se observo un poco de carencia en cuanto a la protección en tiempo real si bien no detecto virus inmediatamente, no se realizaron muchas pruebas para poder determinar si en verdad existe una vulnerabilidad mas amplia de la mencionada.

Reparación:

Parámetro	**Resultado W 7 x32**		**Comentarios / Detalle Vulnerabilidad Encontrada**
	Aprobado	**Reprobado**	
Capacidad de reacción que tiene el antivirus ante el software malicioso		**X**	No detecta algunos software malicioso y por consiguiente no se hace reparación de ficheros
Capacidad de eliminar software malicioso activo	**X**		Sin novedades
Reparación de los cambios que afectaron al sistema		**X**	En ciertas ocasiones no se repara los daños causados por los virus
Capacidad para localizar y eliminar software malicioso que se hayan escondido como rootkits		**X**	Rootkits y detección de software malicioso oculto.

Tabla 22. Vulnerabilidades en Webroot: Secure Aywhere Endpoint Protection 8.0 en base a reparación.

Análisis:

Problemas al detectar y eliminar algunos software malicioso ocultos como rootkits, además existe un poco de carencia en cuanto a la reparación de ficheros que han sido dañados por los ataques recibidos de virus, malware, brinda un nivel de reparación de un 75%.

Utilidad:

Parámetro	Resultado W 7 x32		Comentarios / Detalle Vulnerabilidad Encontrada
	Novedad	Sin Novedad	
Influencia que causa el antivirus en la utilidad del sistema		X	Sin novedades
Mensajes de advertencia, avisos generales, bloqueos, falsos positivos durante el análisis del sistema	X		Falso positivo detectado en enlaces compartidos YouTube y al iniciar live Messenger
Ralentizamiento del ordenador durante su uso, es decir la carga sobre el sistema operativo	X		Hace que el ordenador trabaje lento en determinadas ocasiones

Tabla 23. Vulnerabilidades en Webroot: Secure Aywhere Endpoint Protection 8.0 en base a utilidad.

Análisis:

Falso positivo detectado el sistema de seguridad de Webroot tuvo inconvenientes al clasificar algunos videos provenientes de compartir videos en YouTube se lo clasificaba como enlace que pudiera, potencialmente, causar daño a la computadora del usuario, además se presencia otro falso positivo en el uso de live Messenger al momento de iniciar sesión, esto se debe como mencioné en paginas anteriores a que el antivirus usa la heurística para detectar nuevas amenazas y no es al 100% efectivo, ya que no se hace uso de ninguna base de datos.

CAPITULO V

5 CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

Se determino en base a encuestas realizadas en 9 empresas de la ciudad de Cuenca que menos del 50% de las empresas no cuentan con antivirus corporativos, una cifra un tanto alarmante ya que al ser empresas sus necesidades son distintas a las de un usuario final, la falta de información podría ser la causante de esto según la entrevista realizada al Ing. Luis Méndez Garay de la empresa ACSAM Consultores Cía.LTDA.

Si bien los antivirus corporativos brindan una mejor protección a empresas por su fuerte seguridad dedicada a dichos fines se ha determinado que:

- No están exentos de vulnerabilidades y errores en su funcionamiento como: vulnerabilidades en filtrado de ciertas páginas web, detección de código malicioso ocultos como rootkits, errores de actualización por problemas con sus bases de datos internas entre otras vulnerabilidades,
- Tienen problemas de mensajes erróneos en ciertos casos
- Interfaz poco intuitiva para usuarios nuevos

Aunque un antivirus corporativo brinde mejor seguridad a empresas, siempre habrá brechas de vulnerabilidades, ya que al igual que un antivirus a nivel de usuario final no brinda una protección al 100% de igual manera un antivirus corporativo tampoco logra dar una protección al 100%.

5.2 Recomendaciones

Se recomienda:

- Tomar medidas de seguridad adicionales en el departamento de sistemas de las empresas, creando copias de seguridad continuamente,
- Realizar monitoreo del sistema, actualización y análisis periódicos,
- Tener una buena administración de los equipos clientes con los antivirus corporativos.
- Informarse constantemente sobre las ventajas y desventajas que posee un antivirus corporativo antes de adquirirlo, además informarse que un antivirus corporativo es justamente para empresas y un antivirus normal es para uso personal, hogar y otros fines no empresariales.

Todo esto contribuirá a obtener mayor provecho del antivirus y aumentará la protección en las empresas y sus datos.

Bibliografía

AV COMPARATIVES. (s.f.). Recuperado el 25 de 10 de 2012, de http://www.av-comparatives.org/

AV TEST. (s.f.). Recuperado el 20 de 10 de 2012, de http://www.av-test.org/es/pruebas/empresas/

BITDEFENDER. (s.f.). Recuperado el 25 de 10 de 2012, de http://www.bitdefender.es/

ESET. (s.f.). Recuperado el 28 de 10 de 2012, de http://www.eset-la.com/pdf/prensa/informe/heuristica_antivirus_deteccion_proactiva_malware.pdf

F-SECURE. (s.f.). Recuperado el 07 de 11 de 2012, de http://www.f-secure.com/en/web/home_global

KASPERSKY. (s.f.). Recuperado el 28 de 10 de 2012, de http://latam.kaspersky.com/proteccion-hybrida?ICID=INT1673836

MASTERMAGAZINE. (s.f.). Recuperado el 15 de 10 de 2012, de http://www.mastermagazine.info/termino/3864.php

Regalado, O. L. (s.f.). *PLANEACION ESTRATEGICA.* Recuperado el 04 de 11 de 2012, de http://www.slideshare.net/oscarlopezregalado/instrumentos-de-investigacin-9217795

SAHW. (s.f.). Recuperado el 22 de 10 de 2012, de http://www.sahw.com/wp/archivos/2006/07/03/asi-funciona-una-heuristica-antivirus-primera-parte/

SCRIBD. (s.f.). Recuperado el 20 de Octubre de 2012, de http://es.scribd.com/doc/56654176/42/SISTEMA-DE-ANTIVIRUS-DE- CORPORATIVO PAG. 118.

SITIOS ARGENTINA. (s.f.). Recuperado el 28 de 10 de 2012, de http://www.sitiosargentina.com.ar/webmaster/cursos%20y%20tutoriales/que_es_un_antivirus.htm

SOPHOS. (s.f.). Recuperado el 11 de 11 de 2012, de http://www.sophos.com/es-es/products/endpoint/endpoint-protection.aspx

TENDENCIAS21. (s.f.). Recuperado el 01 de 11 de 2012, de http://www.tendencias21.net/Los-algoritmos-avanzados-posibilitan-una-nueva- generacion-de-antivirus_a7880.html

UN-OJO-CURIOSO.BLOGSPOT. (s.f.). Recuperado el 20 de 10 de 2012, de http://un-ojo-curioso.blogspot.com/2011/10/los-17-mejores-antivirus-versiones-

VSAANTIVIRUS. (s.f.). Recuperado el 24 de 10 de 2012, de http://www.vsantivirus.com/sbam-debilidades.htm

ZONE ALARM. (s.f.). Recuperado el 07 de 11 de 2012, de http://www.zonealarm.com/security/en-us/zonealarm-free-antivirus-firewall.htm

ANEXOS.

Anexo 1: Folleto Informativo Vulnerabilidades En Mejores Antivirus Corporativos 2012

Fig. 28. Folleto informativo sobre vulnerabilidades en antivirus corporativos 2012.

Anexo 2: Formato Encuesta Realizada A Empresas

ANALISIS DE VULNERABILIDADES EN MEJORES ANTIVIRUS DEL 2012 A NIVEL CORPORATIVO.
Encuesta Realizada A La Empresa

"----------"

Nombre: _____
Cargo: _____

1. ¿En su empresa se usa antivirus corporativo?
- SI
- NO

Seleccione de la lista
- Webroot: Secure Aywhere Endpoint Protection 8.0
- Microsoft: Forefront Endpoint Protection 2010
- Sophos: Endpoint Security and Control 10.0
- F-Secure: Client Security 9.31
- Symantec: Endpoint Protection 12.1
- Kaspersky: EndPoint Security 8.1
- Ninguno de los anteriores/otros.

Porque_____
_____

2. ¿Antes de adquirir su antivirus que parámetros analiza?
- Costo
- Nivel de Protección
- Nivel de Reparación en el Sistema Operativo
- Carga en el Sistema operativo (Que no ralentice los equipos)
- De acuerdo a necesidades es decir, empresarial o usuario Final

3. ¿En su empresa se usa algún complemento adicional para maximizar la seguridad a parte del software antivirus?
- SI
- NO

Enumere_____
_____
_____

4. ¿Han sufrido ataques o infiltración de software malicioso?

5. ¿Está satisfecho con su antivirus corporativo actual?

- SI
- NO

Anexo 3: Bases Del Anteproyecto

TEMA: Análisis de Vulnerabilidades en mejores Antivirus del 2012 a Nivel Corporativo.

1. Bases del Anteproyecto

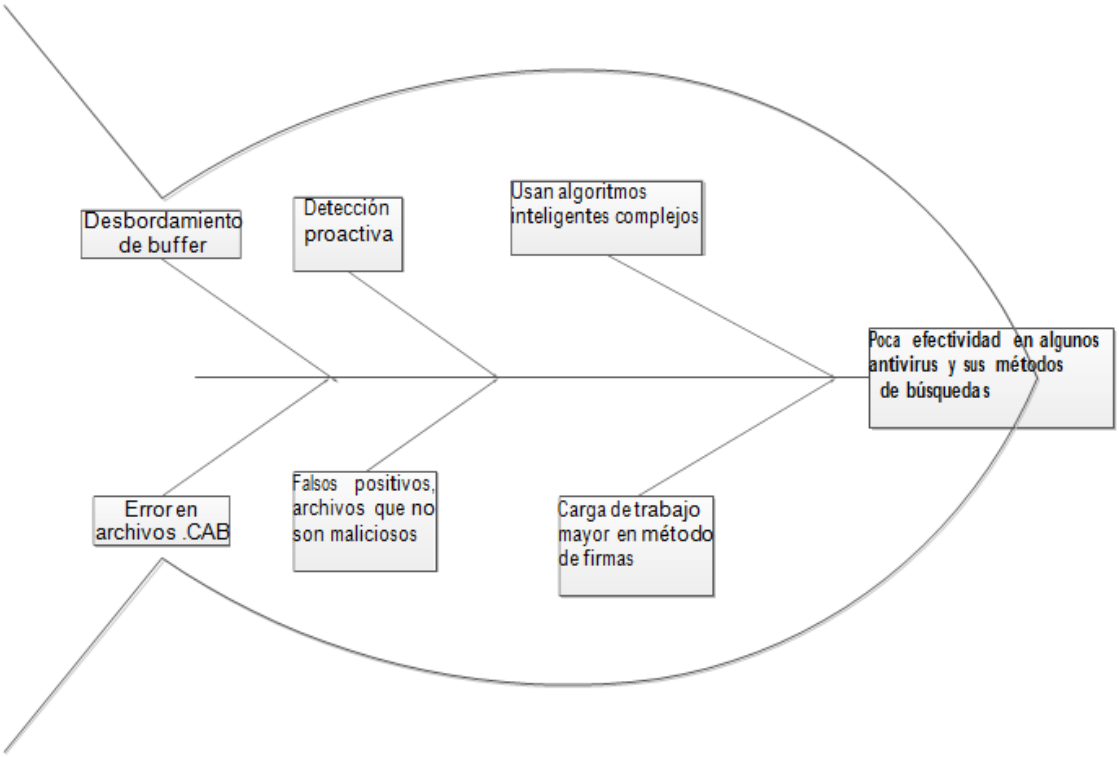
1) ¿Cuál es el Problema?

Poca efectividad en algunos casos para el análisis de software malicioso se da los siguientes problemas:

- Al estar basados los algoritmos heurísticos en inteligencia artificial, poseen relativas desventajas, que deben ser eliminadas para hacer su funcionamiento más eficiente.
- Al utilizar algoritmos inteligentes complejos, la carga de trabajo que posee el antivirus puede ser mayor que cuando se emplea el método basado en firmas (una simple exploración en una base de datos).
- El otro factor de riesgo para los algoritmos de detección proactiva está constituido por los falsos positivos: archivos que no son códigos maliciosos, y son detectados como tales.

- Bibliotecas son propensas a una vulnerabilidad no especificada, pueden provocar un desbordamiento de búfer en la memoria HEAP (la porción de memoria disponible para un programa, también llamada área de memoria dinámica), desbordamiento en archivos .CAB
- Panda Antivirus presentaba un error en su manejo de los archivos EXE, que también generaban un desbordamiento de buffer.

Espina De Pescado



2) ¿Por qué es importante investigar sobre el tema?

- Mejorar algoritmos de búsqueda de software malicioso.
- Agilizar los algoritmos para agilizar el trabajo del antivirus.
- Corregir errores en falso positivos.
- Control de desbordamiento de búfer en la memoria HEAP.
- Corregir errores en manejo de archivos .EXE evitando desbordamientos.

3) ¿Qué se conoce al respecto hasta el momento, dentro y fuera del país?

Las vulnerabilidades de antivirus son conocidas a nivel mundial, cada día existe mas software malicioso que trata de irrumpir la seguridad que nos brindan las empresas dedicadas al desarrollo de software antivirus.

El uso de antivirus es fundamental en nuestro medio nacional e internacional; un antivirus es un software con el objetivo de detectar virus informáticos, existen distintos métodos de búsqueda que usa un software antivirus, sin embargo ningún antivirus garantiza el 100% de seguridad. Es decir acaso la ineficiencia de los métodos de búsqueda usuales son ineficientes.

[1]http://un-ojo-curioso.blogspot.com/2011/10/los-17-mejores-antivirus-versiones-2012.html

[2]http://www.sahw.com/wp/archivos/2006/07/03/asi-funciona-una-heuristica-antivirus-primera-parte/

[3]http://www.vsantivirus.com/sbam-debilidades.htm

[4]http://www.tendencias21.net/Los-algoritmos-avanzados-posibilitan-una-nueva-generacion-de-antivirus_a7880.html

[5]http://www.eset-la.com/pdf/prensa/informe/heuristica_antivirus_deteccion_proactiva_malware.pdf

[6]http://www.sitiosargentina.com.ar/webmaster/cursos%20y%20tutoriales/que_es_un_antivirus.htm

4) ¿Por qué lo va hacer?

Para detectar vulnerabilidades en los antivirus mas usados a nivel mundial enfocándonos mas a un nivel corporativo y presentar posibles soluciones a estas inconsistencias.

5) ¿Cómo lo va a realizar?

El trabajo a realizar es en base a estudio; a realizar análisis y para ello obtener información realizando investigaciones a nivel corporativo.

6) ¿Cuáles son los resultados esperados?

Con el presente trabajo se espera dar a conocer que tan vulnerables son los antivirus a nivel corporativo, para que su estudio de valor y se pueda tomar en cuenta en las organizaciones corporativas.

Como es un análisis se realizará un folleto en donde contenga la información más relevante del tema.

7) ¿Cómo va a transferir y difundir los resultados?

Usando medios de difusión como son el internet, emitiendo un informe a nivel general en lo que se debería mejorar en distintos ámbitos de evaluación.

8) ¿Qué efectos e impactos podría tener las nuevas tecnologías o los nuevos conocimientos en el grupo objetivo?

Efectos positivos porque en base a un estudio de vulnerabilidades se puede tomar conciencia, e implementar nuevas mejoras en base a errores encontrados.

ANALISIS DE VULNERABILIDADES EN MEJORES ANTIVIRUS DEL 2012 A NIVEL CORPORATIVO.

Encuesta Realizada A La Empresa

"COORDINACION ZONAL 6 MIESS AZUAY."

Nombre: OSWALDO DURAN.
Cargo: TECNICO EN DEP. SISTEMAS.

1. ¿En su empresa se usa antivirus corporativo?
   - [x] SI
   - [ ] NO

Seleccione de la lista

- [ ] Webroot: Secure Aywhere Endpoint Protection 8.0
- [ ] Microsoft: Forefront Endpoint Protection 2010
- [ ] Sophos: Endpoint Security and Control 10.0
- [ ] F-Secure: Client Security 9.31
- [ ] Symantec: Endpoint Protection 12.1
- [x] Kaspersky: EndPoint Security 8.1
- [ ] Ninguno de los anteriores/otros.

Porque Por la protección y seguridad que brinda a los ordenadores, además es ligero en cuanto a recursos que ocupa en el S.O.

2. ¿Antes de adquirir su antivirus que parámetros analiza?
   - [ ] Costo
   - [x] Nivel de Protección
   - [x] Nivel de Reparación en el Sistema Operativo
   - [x] Carga en el Sistema operativo (Que no ralentice los equipos)
   - [x] De acuerdo a necesidades es decir, empresarial o usuario Final

3. ¿En su empresa se usa algún complemento adicional para maximizar la seguridad a parte del software antivirus?
   - [x] SI
   - [ ] NO

Enumere Software Symantec para respaldo incremental de información.

4. ¿Han sufrido ataques o infiltración de software malicioso?

Si.

5. ¿Está satisfecho con su antivirus corporativo actual?
   - [x] SI
   - [ ] NO

ANALISIS DE VULNERABILIDADES EN MEJORES ANTIVIRUS DEL 2012 A NIVEL CORPORATIVO.

Encuesta Realizada A La Empresa

"Motor Almer"

Nombre: Dayana Cardenas.
Cargo: Programador en Motor Almer.

1. ¿En su empresa se usa antivirus corporativo?
   - ☐ SI
   - ☒ NO

Seleccione de la lista

- ☐ Webroot: Secure Aywhere Endpoint Protection 8.0
- ☐ Microsoft: Forefront Endpoint Protection 2010
- ☐ Sophos: Endpoint Security and Control 10.0
- ☐ F-Secure: Client Security 9.31
- ☐ Symantec: Endpoint Protection 12.1
- ☐ Kaspersky: EndPoint Security 8.1
- ☐ Ninguno de los anteriores/otros.

Porque no usamos por costos, pero estamos yendo a optar por la adquisición de Kes pershy, actualmente se usa avast.

2. ¿Antes de adquirir su antivirus que parámetros analiza?
   - ☒ Costo
   - ☒ Nivel de Protección
   - ☒ Nivel de Reparación en el Sistema Operativo
   - ☒ Carga en el Sistema operativo (Que no ralentice los equipos)
   - ☐ De acuerdo a necesidades es decir, empresarial o usuario Final

3. ¿En su empresa se usa algún complemento adicional para maximizar la seguridad a parte del software antivirus?
   - ☐ SI
   - ☒ NO

Enumere _____

4. ¿Han sufrido ataques o infiltración de software malicioso?

Si

5. ¿Está satisfecho con su antivirus corporativo actual?

- ☐ SI
- ☒ NO

ANALISIS DE VULNERABILIDADES EN MEJORES ANTIVIRUS DEL 2012 A NIVEL CORPORATIVO.

Encuesta Realizada A La Empresa

"Constructora Chacra Asociados"

Nombre: Ing. Patricio Chacra.
Cargo: Director General.

1. ¿En su empresa se usa antivirus corporativo?
- ☐ SI
- ☒ NO

Seleccione de la lista
- ☐ Webroot: Secure Aywhere Endpoint Protection 8.0
- ☐ Microsoft: Forefront Endpoint Protection 2010
- ☐ Sophos: Endpoint Security and Control 10.0
- ☐ F-Secure: Client Security 9.31
- ☐ Symantec: Endpoint Protection 12.1
- ☐ Kaspersky: EndPoint Security 8.1
- ☐ Ninguno de los anteriores/otros.

Porque Por falta de asesoría y no conozco por cual optar porque no soy experto en ese tema.

2. ¿Antes de adquirir su antivirus que parámetros analiza?
- ☐ Costo
- ☒ Nivel de Protección
- ☒ Nivel de Reparación en el Sistema Operativo
- ☒ Carga en el Sistema operativo (Que no ralentice los equipos)
- ☐ De acuerdo a necesidades es decir, empresarial o usuario Final

3. ¿En su empresa se usa algún complemento adicional para maximizar la seguridad a parte del software antivirus?
- ☐ SI
- ☒ NO

Enumere

4. ¿Han sufrido ataques o infiltración de software malicioso?

Si, he tenido que hacer formatear algunas veces

5. ¿Está satisfecho con su antivirus corporativo actual?

- ☐ SI
- ☒ NO

ANALISIS DE VULNERABILIDADES EN MEJORES ANTIVIRUS DEL 2012 A NIVEL CORPORATIVO.

Encuesta Realizada A La Empresa

"Ceramica Rialto."

Nombre: René Córdova.
Cargo: Director Dep. Sistemas.

1. ¿En su empresa se usa antivirus corporativo?
   - [X] SI
   - [ ] NO

Seleccione de la lista
- [ ] Webroot: Secure Aywhere Endpoint Protection 8.0
- [ ] Microsoft: Forefront Endpoint Protection 2010
- [ ] Sophos: Endpoint Security and Control 10.0
- [ ] F-Secure: Client Security 9.31
- [X] Symantec: Endpoint Protection 12.1
- [ ] Kaspersky: EndPoint Security 8.1
- [ ] Ninguno de los anteriores/otros.

Porque Brinda completa protección, tiene varios módulos y fácil de usar.

2. ¿Antes de adquirir su antivirus que parámetros analiza?
   - [X] Costo
   - [X] Nivel de Protección
   - [X] Nivel de Reparación en el Sistema Operativo
   - [X] Carga en el Sistema operativo (Que no ralentice los equipos)
   - [X] De acuerdo a necesidades es decir, empresarial o usuario Final

3. ¿En su empresa se usa algún complemento adicional para maximizar la seguridad a parte del software antivirus?
   - [ ] SI
   - [X] NO

Enumere

4. ¿Han sufrido ataques o infiltración de software malicioso?

Si.

5. ¿Está satisfecho con su antivirus corporativo actual?

- [X] SI
- [X] NO

ANALISIS DE VULNERABILIDADES EN MEJORES ANTIVIRUS DEL 2012 A NIVEL CORPORATIVO.

Encuesta Realizada A La Empresa

"EL HIERRO"

Nombre: Fabian Bermeo Perez
Cargo: Web Developer "EL HIERRO"

1. ¿En su empresa se usa antivirus corporativo?
   - ☐ SI
   - ☒ NO

Seleccione de la lista
- ☐ Webroot: Secure Aywhere Endpoint Protection 8.0
- ☐ Microsoft: Forefront Endpoint Protection 2010
- ☐ Sophos: Endpoint Security and Control 10.0
- ☐ F-Secure: Client Security 9.31
- ☐ Symantec: Endpoint Protection 12.1
- ☐ Kaspersky: EndPoint Security 8.1
- ☐ Ninguno de los anteriores/otros.

Porque Usamos ESET SMART SECURITY 5.

2. ¿Antes de adquirir su antivirus que parámetros analiza?
   - ☒ Costo
   - ☒ Nivel de Protección
   - ☒ Nivel de Reparación en el Sistema Operativo
   - ☒ Carga en el Sistema operativo (Que no ralentice los equipos)
   - ☐ De acuerdo a necesidades es decir, empresarial o usuario Final

3. ¿En su empresa se usa algún complemento adicional para maximizar la seguridad a parte del software antivirus?
   - ☐ SI
   - ☒ NO

Enumere

4. ¿Han sufrido ataques o infiltración de software malicioso?

Si.

5. ¿Está satisfecho con su antivirus corporativo actual?
   - ☒ SI
   - ☐ NO

ANALISIS DE VULNERABILIDADES EN MEJORES ANTIVIRUS DEL 2012 A NIVEL CORPORATIVO.

Encuesta Realizada A La Empresa

"BC COMPU."

Nombre: Ing. Nelson Barrera.
Cargo: Gerente

1. ¿En su empresa se usa antivirus corporativo?
- ☐ SI
- ☒ NO

Seleccione de la lista
- ☐ Webroot: Secure Aywhere Endpoint Protection 8.0
- ☐ Microsoft: Forefront Endpoint Protection 2010
- ☐ Sophos: Endpoint Security and Control 10.0
- ☐ F-Secure: Client Security 9.31
- ☐ Symantec: Endpoint Protection 12.1
- ☐ Kaspersky: EndPoint Security 8.1
- ☐ Ninguno de los anteriores/otros.

Porque con la sesion de NOD SMART SECURITY no hemos tenido ningun inconveniente y estamos satisfechos.

2. ¿Antes de adquirir su antivirus que parámetros analiza?
- ☒ Costo
- ☒ Nivel de Protección
- ☒ Nivel de Reparación en el Sistema Operativo
- ☒ Carga en el Sistema operativo (Que no ralentice los equipos)
- ☒ De acuerdo a necesidades es decir, empresarial o usuario Final

3. ¿En su empresa se usa algún complemento adicional para maximizar la seguridad a parte del software antivirus?
- ☐ SI
- ☒ NO

Enumere

4. ¿Han sufrido ataques o infiltración de software malicioso?

Si.

5. ¿Está satisfecho con su antivirus corporativo actual?
- ☒ SI
- ☐ NO

ANALISIS DE VULNERABILIDADES EN MEJORES ANTIVIRUS DEL 2012 A NIVEL CORPORATIVO.

Encuesta Realizada A La Empresa

"ACSAM Consultoría Cía. LTDA."

Nombre: Luis Mendez Garay
Cargo: Encargado de Dept. de Sistemas

1. ¿En su empresa se usa antivirus corporativo?
   - [X] SI
   - [ ] NO

Seleccione de la lista
- [ ] Webroot: Secure Aywhere Endpoint Protection 8.0
- [ ] Microsoft: Forefront Endpoint Protection 2010
- [ ] Sophos: Endpoint Security and Control 10.0
- [ ] F-Secure: Client Security 9.31
- [X] Symantec: Endpoint Protection 12.1
- [ ] Kaspersky: EndPoint Security 8.1
- [ ] Ninguno de los anteriores/otros.

Porque Protección y copias de archivos y S.O, copias incrementales

2. ¿Antes de adquirir su antivirus que parámetros analiza?
   - [X] Costo
   - [X] Nivel de Protección
   - [X] Nivel de Reparación en el Sistema Operativo
   - [X] Carga en el Sistema operativo (Que no ralentice los equipos)
   - [X] De acuerdo a necesidades es decir, empresarial o usuario Final

3. ¿En su empresa se usa algún complemento adicional para maximizar la seguridad a parte del software antivirus?
   - [ ] SI
   - [X] NO

Enumere

4. ¿Han sufrido ataques o infiltración de software malicioso?

Si

5. ¿Está satisfecho con su antivirus corporativo actual?
   - [X] SI
   - [ ] NO

ANALISIS DE VULNERABILIDADES EN MEJORES ANTIVIRUS DEL 2012 A NIVEL CORPORATIVO.

Encuesta Realizada A La Empresa

"ACSAM Consultores C.A. LTDA"

Nombre: Luis Antonio Matos Garay.
Cargo: Encargado de Departamento de Sistemas.

1. ¿En su empresa se usa antivirus corporativo?
   - [x] SI
   - [ ] NO

Seleccione de la lista
- [ ] Webroot: Secure Aywhere Endpoint Protection 8.0
- [ ] Microsoft: Forefront Endpoint Protection 2010
- [ ] Sophos: Endpoint Security and Control 10.0
- [ ] F-Secure: Client Security 9.31
- [x] Symantec: Endpoint Protection 12.1
- [ ] Kaspersky: EndPoint Security 8.1
- [ ] Ninguno de los anteriores/otros.

Porque Por la protección que brinda y permite hacer copias de seguridad y el Sistema Operativo y instalarlo.

2. ¿Antes de adquirir su antivirus que parámetros analiza?
   - [x] Costo
   - [x] Nivel de Protección
   - [x] Nivel de Reparación en el Sistema Operativo
   - [x] Carga en el Sistema operativo (Que no ralentice los equipos)
   - [x] De acuerdo a necesidades es decir, empresarial o usuario Final

3. ¿En su empresa se usa algún complemento adicional para maximizar la seguridad a parte del software antivirus?
   - [ ] SI
   - [x] NO

Enumere _____

4. ¿Han sufrido ataques o infiltración de software malicioso?
   Si

5. ¿Está satisfecho con su antivirus corporativo actual?
   - [x] SI
   - [ ] NO

ANALISIS DE VULNERABILIDADES EN MEJORES ANTIVIRUS DEL 2012 A NIVEL CORPORATIVO.

Encuesta Realizada A La Empresa

"Graficamp"

Nombre: Jose Miguel Gonzales
Cargo: Gerente.

1. ¿En su empresa se usa antivirus corporativo?
   - ☐ SI
   - ☒ NO

Seleccione de la lista

- ☐ Webroot: Secure Aywhere Endpoint Protection 8.0
- ☐ Microsoft: Forefront Endpoint Protection 2010
- ☐ Sophos: Endpoint Security and Control 10.0
- ☐ F-Secure: Client Security 9.31
- ☐ Symantec: Endpoint Protection 12.1
- ☐ Kaspersky: EndPoint Security 8.1
- ☐ Ninguno de los anteriores/otros.

Porque Asesoría e información de costos de antivirus empresariales.

2. ¿Antes de adquirir su antivirus que parámetros analiza?
   - ☒ Costo
   - ☒ Nivel de Protección
   - ☒ Nivel de Reparación en el Sistema Operativo
   - ☒ Carga en el Sistema operativo (Que no ralentice los equipos)
   - ☐ De acuerdo a necesidades es decir, empresarial o usuario Final

3. ¿En su empresa se usa algún complemento adicional para maximizar la seguridad a parte del software antivirus?
   - ☐ SI
   - ☒ NO

Enumere Ninguno.

4. ¿Han sufrido ataques o infiltración de software malicioso?

Si.

5. ¿Está satisfecho con su antivirus corporativo actual?

- ☐ SI
- ☒ NO