UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

Tema:

"ANÁLISIS HEURÍSTICO DE MALWARE APLICADO A LA DETECCIÓN DE DOCUMENTOS PDF MALICIOSOS EN EL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPALIDAD DE AMBATO".

Trabajo de Graduación. Modalidad: Seminario De Graduación "Seguridad Informática", presentado previo a la obtención del título de Ingeniero en Sistemas Computacionales e Informáticos.

Subnivel de investigación: Seguridad Informática

AUTOR: Ana Lucia Morocho Toaza.

TUTOR: Ing. Msc. Alberto Arellano A.

Ambato – Ecuador
Abril - 2013

APROBACIÓN DEL TUTOR

En mi calidad de tutor del trabajo de investigación sobre el tema: **"ANÁLISIS HEURÍSTICO DE MALWARE APLICADO A LA DETECCIÓN DE DOCUMENTOS PDF MALICIOSOS EN EL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPALIDAD DE AMBATO"**, de la señorita Ana Lucia Morocho Toaza, estudiante de la carrera de Ingeniería en Sistemas, Electrónica e industrial, de la Universidad Técnica de Ambato, considero que el informe investigativo reúne los requisitos suficientes para que continúe con los tramites y consiguiente aprobación de conformidad el Art. 16 del Capítulo II, del Reglamento de Graduación para obtener el Título Terminal de Tercer Nivel de la Universidad Técnica de Ambato.

Ambato, Abril 2013

EL TUTOR

Ing. Msc. Alberto Arellano A.

AUTORÍA

El presente trabajo de investigación titulado: **ANÁLISIS HEURÍSTICO DE MALWARE APLICADO A LA DETECCIÓN DE DOCUMENTOS PDF MALICIOSOS EN EL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPALIDAD DE AMBATO** Es absolutamente original, auténtico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, Abril 2013

EL AUTOR

Ana Morocho

CC: 1803601408

APROBACIÓN DE LA COMISIÓN CALIFICADORA

La comisión calificadora del presente trabajo la conformada por los señores docentes Ing. Vicente Morales E Ing. Galo López, reviso y aprobó el Informe Final del trabajo de graduación Titulado **"ANÁLISIS HEURÍSTICO DE MALWARE APLICADO A LA DETECCIÓN DE DOCUMENTOS PDF MALICIOSOS EN EL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPALIDAD DE AMBATO"**, presentado por la señorita Ana Lucía Morocho Toaza de acuerdo al Art. 18 del Reglamento de Graduación para Obtener el Título Terminal de Tercer Nivel de la Universidad Técnica de Ambato.

_____

Ing. Mg. Edison Homero Álvarez Mayorga

PRESIDENTE DEL TRIBUNAL

_____ _____

Ing. Vicente Morales

DOCENTE CALIFICADOR

Ing. Galo López

DOCENTE CALIFICADOR

DEDICATORIA

Dedico esta tesis a Dios, a mis padres por apoyarme siempre en todo momento, a mis hermanas que fueron mis amigas incondicionales y siempre estuvieron alentándome a terminar mi carrera y a mis amigas por estar a mi lado en los momentos más difíciles.

Ana Lucía Morocho Toaza

AGRADECIMIENTO

En primer lugar agradezco a Dios por darme fuerzas para salir adelante y no desfallecer en el camino.

A la facultad de Ingeniería en Sistemas Electrónica e Industrial de la Universidad Técnica de Ambato por darme la oportunidad de formarme como profesional, a todos y cada uno de los docentes que forman parte de la Facultad de Sistemas.

Al ingeniero Alberto Arellano que en calidad de tutor supo guiarme y brindarme su colaboración y conocimientos para la culminación de esta investigación.

Al gobierno Autónomo Descentralizado Municipal de Ambato por haberme abierto las puertas y puesto su confianza en mí.

Ana Lucía Morocho Toaza

ÍNDICE GENERAL

Pág.

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

RESUMEN EJECUTIVO

El tema del presente trabajo investigativo es análisis heurístico de malware aplicado a la detección de documentos pdf maliciosos en el gobierno autónomo descentralizado municipalidad de Ambato.

Los archivos PDF al ser el formato más utilizado por las personas, se convierten en una amenaza importante, ya que son aprovechados por los atacantes para la introducción de código malicioso, por lo que se requiere de mecanismos de detección que sean eficaces y robustos.

El objetivo principal del Gobierno Autónomo Descentralizado Municipalidad de Ambato es brindar atención a sus contribuyentes con servicios de calidad, para esto debe realizar todas sus actividades con mayor eficacia tratando de esta manera asegurar en lo posible la información procesada día a día.

A continuación se presenta el resumen por capítulos de toda la investigación realizada.

Capítulo I: denominado "EL PROBLEMA", se identifica el problema a investigar, se plantea la justificación y los objetivos.

Capítulo II: denominado "MARCO TEÓRICO", se presentan los antecedentes investigativos, la fundamentación legal, hipótesis y el señalamiento de las variables.

Capítulo III: denominado "METODOLOGÍA", se determina la metodología de investigación a utilizar, el enfoque, la modalidad básica de la investigación, el tipo de investigación, la población y muestra.

Capítulo IV: denominado "ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS", comprende el análisis e interpretación de resultados.

En el capítulo V: denominado "CONCLUSIONES Y RECOMENDACIONES", se presenta las conclusiones y recomendaciones en base los resultados obtenidos en la entrevista realizada al personal encargado del departamento de sistemas.

Capítulo VI: denominado "PROPUESTA", se presenta el desarrollo de la propuesta ante el problema planteado.

Anexos: contienen formato de cuestionarios, manuales de administración, usuario e instalación.

INTRODUCCIÓN

El Análisis Heurístico de Malware consiste en dar respuestas en aquellas situaciones en donde los métodos reactivos no pueden darla, la capacidad de detectar un archivo malicioso aunque una muestra de éste no haya llegado al laboratorio antivirus.

El objetivo principal del Análisis Heurístico de Malware es obtener un informe donde se detalla el funcionamiento de la tecnología del software antivirus, dando respuestas en aquellas situaciones en donde los métodos reactivos no pueden darla, detectando un archivo malicioso desconocido para los antivirus.

Por este motivo es de vital importancia realizar el Análisis Heurístico de Malware para dar a conocer las nuevas formas de contagio a través de documentos pdf maliciosos en el Gobierno Autónomo Descentralizado Municipal de Ambato, por tal razón se expone a continuación una investigación que nos permitirá conocer la forma en que un documento pdf puede ser contagiado de código malicioso y los daños que se pueden producir al ejecutarse dicho archivo, con esto se logrará evitar el contagio de dicho malware, recomendando algunos software antivirus o por lo menos minimizar los riesgos de contagio dando a conocer la forma de contagio y las medidas de prevención que deberían ser utilizadas en el Gobierno Autónomo Descentralizado Municipal de Ambato logrando brindar unos servicios seguros y de calidad.

CAPITULO I

1. EL PROBLEMA

1.1. Tema

Análisis heurístico de malware aplicado a la detección de documentos PDF maliciosos en el Gobierno Autónomo Descentralizado Municipalidad de Ambato.

1.2. Planteamiento del Problema

1.2.1. Contextualización

El formato PDF se ha convertido en uno de los formatos de archivos portables más utilizados, lo que ha provocado que los atacantes de virus conviertan el formato PDF en un vector principal de malware descubriendo y explotando sus vulnerabilidades, por lo cual Adobe Reader ha sido una de las aplicaciones mas atacadas en el último año ya que el código malicioso se encuentra incrustado y se ejecuta en el momento q se abre un archivo PDF, además los intrusos han desarrollados nuevos artilugios para engañar a los usuarios haciendo que abran documentos PDF o algún mensaje de correos electrónicos que vienen cargados con malware, el engaño consiste en enviar correos electrónicos con supuestos documentos escaneados desde impresoras o escáneres de oficina que luego son enviados por algún compañero de trabajo, lo cual ha logrado engañar a muchos usuarios.

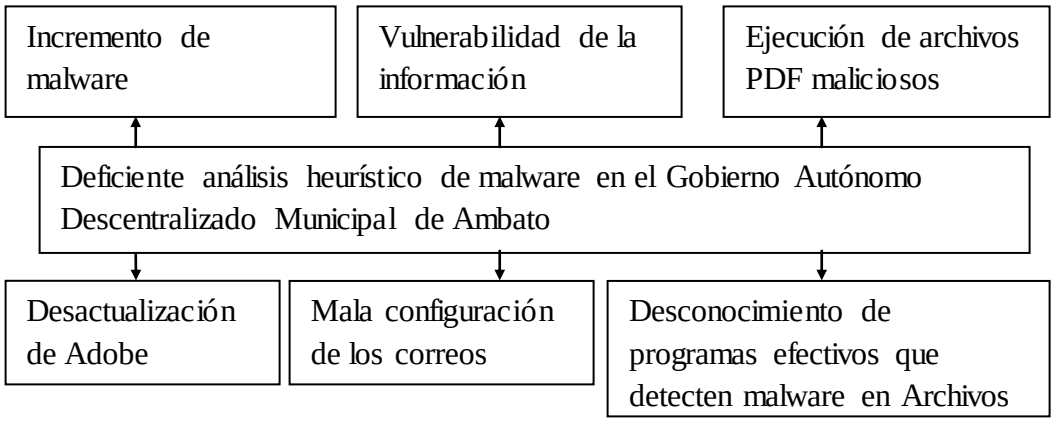
Últimamente ha habido muchos casos de pishing, robos de contraseñas y cuentas bancarias además de que con el internet todo el mundo está expuesto a ser contagiado con virus al navegar por diferentes páginas, al descargarse un archivo o bajar cualquier tipo de información, etc. A nivel de la provincia ha habido muchas casos de personas que han sido víctimas de diferentes ataques y esto se debe de cierta forma al

desconocimiento de los tipos de ataques existentes, además de que muchos de los computadores de los usuarios son sumamente vulnerables, provocando un mayor daño. El desconocimiento de las personas de técnicas que ayudan a eliminar código malicioso o a su vez minimizar el daño es cada vez más grande por existir demasiadas formas de contagio de malware y porque no existe un software cien por ciento seguro y capaz de detectar todo tipo de código malicioso.

El Gobierno Autónomo Descentralizado Municipalidad de Ambato afronta el problema relacionado con el deficiente análisis heurístico de malware debido a que el personal tiene un libre acceso a Internet y se han encontrado expuestos a diferentes tipos de contagios de virus, siendo los más comunes los ataques utilizando el correo electrónico, la mayoría del personal han recibido correos no deseados los cuales contienen links a paginas infectadas de virus, o a su vez algún archivo portable como el formato PDF, que al no ser examinado a través de un software antivirus, se expone a que la máquina se contagie de algún código malicioso en el momento que se ejecuta el archivo.

1.2.2. Árbol del Problema

Efectos



Causas

Figura 1. 1 Árbol del Problema

1.2.3. Análisis Crítico

El problema presentado en el Área de Sistemas en el Gobierno Autónomo Descentralizado Municipalidad de Ambato se produce principalmente por la desactualización del programa Adobe Reader, puesto que es el formato de archivo portable más utilizado para enviar o recibir información es el formato PDF y se debe tomar en cuenta que este programa es constantemente actualizado y parchado adquiriendo nuevas características y seguridades como por ejemplo una de las últimos cambios que se hicieron son la caja de arena y el aislamiento lo cual impiden o minimizan los riesgos de contagio de los computadores con malware.

La mala configuración de los correos electrónicos provoca que existan vulnerabilidades de la información, al no tomar en cuenta los requerimientos de la empresa y de los empleados de la misma, permitiendo que las organizaciones, empresas o personas de fuera envíen correos masivos no deseados a las cuentas de correo de los usuarios lo cual incrementa las formas de contagio de código malicioso en los computadores de los funcionarios.

El desconocimiento de programas efectivos que detecten malware en Archivos provoca la ejecución de PDF maliciosos ya que no ser correctamente analizados por un software antivirus adecuado antes de ser ejecutados se corre el riesgo de que se ejecute algún tipo de código malicioso, el desconocimiento por parte de los usuarios de nuevas técnicas de análisis de virus para ciertos formatos de archivos los cuales ayudarían a minimizar los riesgos de contagio pueden ocasionar en sin fin de daños o perdidas para la empresa.

1.2.4. Prognosis

De continuar con esta situación la Institución Pública a futuro tendría pérdidas de la información, oh a su vez la información podría ser conocida por personas no autorizadas las cuales podrían darle una mala utilización, lo cual llagaría a causar

desprestigio, sin tomar en cuenta que los intrusos podrían causar daños en archivos importantes de la empresa lo que provocaría pérdidas económicas entre otras cosas, por lo cual se hace necesaria la aplicación de técnicas de seguridad para prevenir una nueva forma de instrucción de virus a través de archivos PDF en el Gobierno Autónomo Descentralizado Municipalidad de Ambato.

1.2.5. Formulación del Problema.

¿Cómo el deficiente análisis heurístico de malware incide en el contagio a través de documentos PDF maliciosos en los computadores de los funcionarios en el Gobierno Autónomo Descentralizado Municipalidad de Ambato en el periodo 2010?

Preguntas Directrices

¿Cuáles son las mejores técnicas para el análisis heurístico de malware?
¿Qué ambiente seria el adecuado para la realización de pruebas utilizando correos electrónicos para el envió de documentos PDF maliciosos?

¿Cómo desarrollar una guía metodológica de análisis heurístico de malware que satisfaga las necesidades de los funcionarios y permita la detección de documentos PDF maliciosos en el Gobierno Autónomo Descentralizado Municipalidad de Ambato?

1.2.6. Delimitación del Problema

Campo: Informática.

Área: Seguridad Informática.

Aspecto: Análisis heurístico de malware.

Delimitación Espacial: La presente investigación se llevará a cabo en el Gobierno Autónomo Descentralizado Municipalidad de Ambato.

Delimitación Temporal: El problema será investigado, en el periodo comprendido entre el 2011- 2012

1.3. Justificación

En la actualidad no existen muchas personas interesadas en el estudio de la seguridad informática, así que es un campo que no ha sido explotado, especialmente en el Ecuador y en la ciudad de Ambato por lo que además se podrían abrirme muchos caminos en el campo laboral.

En Internet se puede encontrar una gran cantidad de información sobre el tema especificado, facilitando la investigación y brindando toda clase de información posible sobre ataques, programas robustos y eficientes incluyendo los más recientes ataques y la forma como fueron ejecutados entre otras cosas. Al ser un tema novedoso puede ser aplicado en cualquier empresa grande o a su vez en una entidad pública ya que se menciono con anterioridad la seguridad de la información es de gran interés para todos.

El estudio de la introducción de virus en archivos PDF va de la mano con la seguridad informática y es un campo que aun no ha sido explotado en su totalidad y un tema en el cual todo el mundo se encuentra interesado para mantener la información más segura ya sea eliminando o minimizando los riesgos de contagio de virus.

Los beneficios serían muchos ya que puede ser aplicado en cualquier parte sin ningún problema como por ejemplo instituciones bancarias, instituciones públicas o privadas, o institutos como escuelas, colegios, universidades entre otros.

En cuanto a los recursos y la factibilidad los gastos no serán grandes ya que no se necesitarán expertos en el tema y la tecnología con la que se cuenta es la adecuada, evitando así los gastos innecesarios en el Gobierno Autónomo Descentralizado Municipalidad de Ambato en donde va a ser aplicado nuestro tema.

1.4 Objetivos

1.4.1. Objetivo General

Determinar el análisis heurístico de malware para que no permita el acceso de documentos PDF maliciosos en el Gobierno Autónomo Descentralizado Municipalidad de Ambato.

1.4.2. Objetivos Específicos

- Diagnosticar las técnicas de análisis heurístico de malware.
- Analizar un ambiente de pruebas utilizando correos electrónicos para el envió de documentos PDF maliciosos.
- Proponer una guía metodológica del análisis heurístico de malware considerando las necesidades que permita la detección de documentos PDF maliciosos en el Gobierno Autónomo Descentralizado Municipalidad de Ambato.

CAPITULO II

2. MARCO TEORICO

2.1. Antecedentes Investigativos:

Jesús Manuel Puetate Espinoza, estudio de los protocolos de seguridad del servicio de correo electrónico para implementar un web mail en el HCPCH, Riobamba Ecuador 2009, biblioteca virtual ESPOCH.

La seguridad en la computación y la utilización de correos electrónicos para el intercambio de información en el trabajo diarios entre personas. Y es similar en el objetivo general del estudio de protocolos de seguridad del servicio de correo electrónico, mientras que en el tema a desarrollarse es un análisis heurístico de malware para encontrar la mejor técnica y tomando en cuenta que los objetivos específicos tienen un orden similar a lo que se va a realizar.

Fernández De Córdova, David Moncayo, Análisis, diseño e implementación de una solución anti spam para la Empresa Ecua online, Sangolquí / ESPE / 2009, biblioteca virtual ESPE.

Al igual que el tema que se está tratando aquí habla sobre los diferentes tipos de virus y un análisis con el que se determinará la mejor solución además de que la forma de contagio es a través de correos electrónicos, lo cual tiene una semejanza ya que en este tema una forma de contagio es el envío de documentos maliciosos utilizando correos electrónicos.

2.2. Fundamentación Legal

Constitución del estado

Sección tercera
Comunicación e Información

Art. 19.- La ley regulará la prevalencia de contenidos con fines informativos, educativos y culturales en la programación de los medios de comunicación, y fomentará la creación de espacios para la difusión de la producción nacional independiente. Se prohíbe la emisión de publicidad que induzca a la violencia, la discriminación, el racismo, la toxicomanía, el sexismo, la intolerancia religiosa o política y toda aquella que atente contra los derechos.

Art. 20.- El Estado garantizará la cláusula de conciencia a toda persona, y el secreto profesional y la reserva de la fuente a quienes informen, emitan sus opiniones a través de los medios u otras formas de comunicación, o laboren en cualquier actividad de comunicación.

Capítulo octavo
Derechos de protección

Art. 82.- El derecho a la seguridad jurídica se fundamenta en el respeto ala Constitución y en la existencia de normas jurídicas previas, claras, públicas y aplicadas por las autoridades competentes.

Sección octava
Ciencia, tecnología, innovación y saberes ancestrales

Art. 385.- El sistema nacional de ciencia, tecnología, innovación y saberes ancestrales, en el marco del respeto al ambiente, la naturaleza, la vida, las culturas y la soberanía, tendrá como finalidad:

1. Generar, adaptar y difundir conocimientos científicos y tecnológicos.
2. Recuperar, fortalecer y potenciar los saberes ancestrales.
3. Desarrollar tecnologías e innovaciones que impulsen la producción nacional, eleven la eficiencia y productividad, mejoren la calidad de vida y contribuyan a la realización del buen vivir.174

Art. 386.- El sistema comprenderá programas, políticas, recursos, acciones, e incorporará a instituciones del Estado, universidades y escuelas politécnicas, institutos de investigación públicos y particulares, empresas públicas y privadas, organismos no gubernamentales y personas naturales o jurídicas, en tanto realizan actividades de investigación, desarrollo tecnológico, innovación y aquellas ligadas a los saberes ancestrales.

El Estado, a través del organismo competente, coordinará el sistema, establecerá los objetivos y políticas, de conformidad con el Plan Nacional de Desarrollo, con la participación de los actores que lo conforman.

Art. 387.- Será responsabilidad del Estado:

1. Facilitar e impulsar la incorporación a la sociedad del conocimiento para alcanzar los objetivos del régimen de desarrollo.
2. Promover la generación y producción de conocimiento, fomentar la investigación científica y tecnológica, y potenciar los saberes ancestrales, para así contribuir a la realización del buen vivir, al sumakkawsay.
3. Asegurar la difusión y el acceso a los conocimientos científicos y tecnológicos, el usufructo de sus descubrimientos y hallazgos en el marco de lo establecido en la Constitución y la Ley.
4. Garantizar la libertad de creación e investigación en el marco del respeto a la ética, la naturaleza, el ambiente, y el rescate de los conocimientos ancestrales.

5. Reconocer la condición de investigador de acuerdo con la Ley.

Art. 388.- El Estado destinará los recursos necesarios para la investigación científica, el desarrollo tecnológico, la innovación, la formación científica, la recuperación y desarrollo de saberes ancestrales y la difusión del conocimiento. Un porcentaje de estos recursos se destinará a financiar proyectos mediante fondos concursables. Las organizaciones que reciban fondos públicos estarán sujetas a la rendición de cuentas y al control estatal respectivo.

2.3. Categorías Fundamentales

Variable Independiente: Análisis heurístico de malware

Variable Dependiente: Documentos PDF Maliciosos

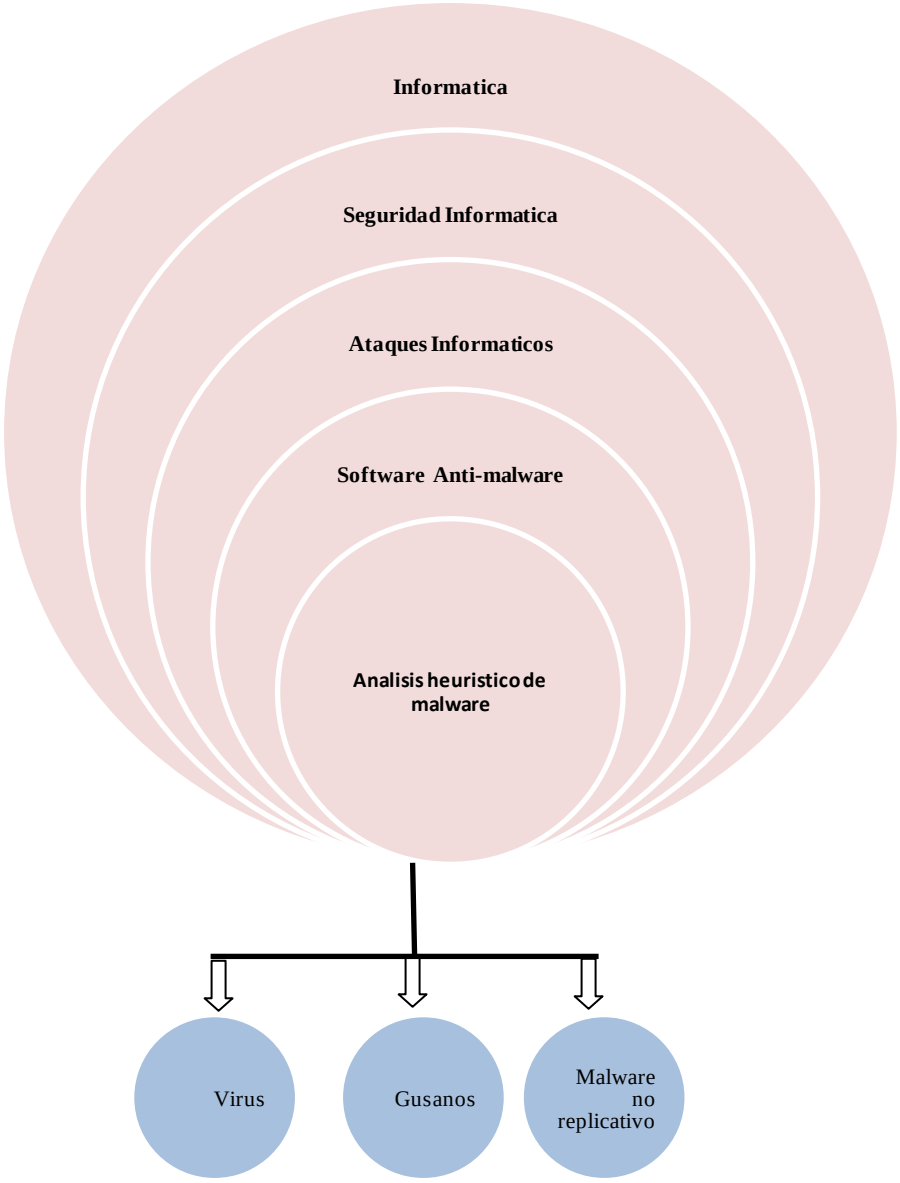


Figura 2. 1Variable Independiente

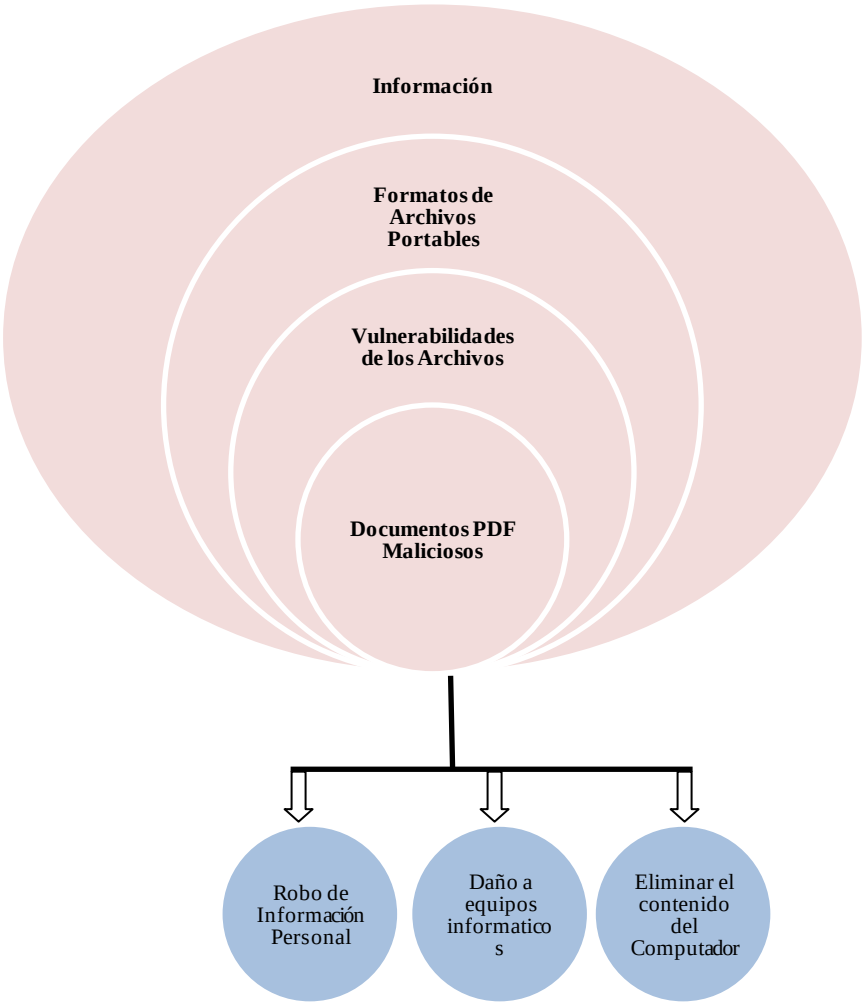


Figura 2. 2Variable Dependiente

2.3.1. Fundamentación teórica variable independiente

Informática

Se considera lo dicho por LANZILLOTTA, Analía (Internet; 12/02/2005,05/10/2011, 16:09) que la informática es la ciencia que tiene como objetivo estudiar el tratamiento automático de la información a través de la computadora. Y también se toma en cuenta la definición del Dr. MARQUÈSGRAELLS, Pere (Internet; 08/08/10,05/10/2011,16:34) en donde

menciona que es la ciencia que busca la máxima eficiencia y economía en el tratamiento de la información mediante la utilización de unas máquinas automáticas concretas, los ordenadores. Por otro lado TORRES, Juan LLORIS, Antonio PRIETO, Alberto (2004, Pág. 1) también es importante ya que menciona que "Informática es una palabra de origen francés formada por la contracción de dos vocablos INFORmación y autoMÁTICA. La Real Academia Española de la lengua define la informática como el conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores."

La informática es una ciencia cuyo objetivo es estudiar el tratamiento autónomo de la información, buscando la máxima efectividad y economía por medio de computadores.

Seguridad Informática

Se ha encontrado una definición importante en Revista Red, La comunidad de expertos en redes (Internet; 11/2002, 28/10/2011, 13:55) en donde expresa que la seguridad puede entenderse como aquellas reglas técnicas y/o actividades destinadas a prevenir, proteger y resguardar lo que es considerado como susceptible de robo, pérdida o daño, ya sea de manera personal, grupal o empresarial. Además se debe tomar en cuenta la definición de ALEGSA - Santa Fe, Argentina (Internet; 1998 – 2011, 28/10/2011, 14:50) "La seguridad informática es una disciplina que se relaciona a diversas técnicas, aplicaciones y dispositivos encargados de asegurar la integridad y privacidad de la información de un sistema informático y sus usuarios." También es importante la versión de BORGHELLO, Cristian (Internet; 2000-2009, 28/10/2011, 13:05) La Seguridad Física, el activo más importante que se posee es la **información**, y por lo tanto deben existir técnicas, más allá de la seguridad física, que la aseguren. Estas técnicas las brinda la Seguridad Lógica. La **Seguridad Lógica** consiste en la "aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo."

Es una disciplina que se relaciona a diversas técnicas, aplicaciones y dispositivos, garantizando que los recursos informáticos no estén dañados o alternados por circunstancias o factores externos de tal forma que prevenga, proteja y resguarde la información, para lo cual se debe tomar en cuenta la seguridad física y lógica.

Ataques Informáticos

EnMIERES, Jorge (Internet; enero-2009, 06/11/2011, 22:51) menciona que Un ataque informático consiste en aprovechar alguna debilidad o falla (vulnerabilidad) en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente informático. Por otra parte SANDRA (Internet; 01/07/2007,20:24, 06/11/2011, 22:51) expresa que se puede definir como ataques, todas aquellas acciones que suponen una violación de la seguridad de nuestro sistema, confidencialidad, integridad o disponibilidad.

Son acciones que violan la seguridad de la información, un individuo aprovecha las vulnerabilidades ya sea en el software, en el hardware e incluso en las personas que forman parte de un ambiente informático con el fin de obtener un beneficio.

Software anti-malware

La definición encontrada ANONIMO (Panda Security)(Internet; 2011, 07/11/2011, 0:30) expresa que "Se llama **"Malware"** a todo archivo con contenido de carácter malicioso para un equipo informático. Esto no se limita a los virus, pues existen otros muchos archivos capaces de causar daños importantes en un ordenador o en una red informática." Lo cual coincide con BORTNIK, Sebastián (Internet; 23/05/2010,12:07, 07/11/2011, 0:59) Un antivirus es un software que posee la función de detectar códigos maliciosos. Aunque su nombre está relacionado con los virus informáticos, en la actualidad estos programas son soluciones antimalware que poseen protección contra gusanos, troyanos, rootkit, spyware y otros elementos dañinos; es decir, todo tipo de códigos maliciosos.

El software anti-malware, evita la infiltración en el sistema y el daño, proporcionando protección en tiempo real contra la instalación de malware en una computadora y detectando y eliminando malware que ya ha sido instalado en una computadora, poseyendo protección contra gusanos, troyanos, rootkit, spyware y otros elementos dañinos; es decir, todo tipo de códigos maliciosos.

Análisis heurístico de malware

HARLEY, David Security Author, Consultant Andrew Lee, ChiefResearchOfficer de ESET (Internet: 27/03/2007, 11:03, 28/10/2011, 20:37) dice "Es un informe que detalla cómo es que funciona la tecnología de los software antivirus. Se destaca el funcionamiento del análisis heurístico, marcando las particularidades de esta tecnología para la detección de las últimas amenazas informáticas desconocidas." Lo cual tiene similitud con BORTNIK, Sebastián, Analista en Seguridad de ESET para Latinoamérica (Internet: 23/05/2010, 12:07, 28/10/2011, 21:00). El objetivo esencial de los algoritmos heurísticos es dar respuestas en aquellas situaciones en donde los métodos reactivos no pueden darla: la capacidad de detectar un archivo malicioso aunque una muestra de éste no haya llegado al laboratorio antivirus. Al igual que FREIRE, José Luis(Internet; 25/06/2000-2008, 29/10/2011, 8:44) quien opina que el análisis heurístico consiste en un sistema de "detección genérica" de códigos maliciosos, es decir, un modo de localizar la presencia de un virus aun cuando no existe vacuna para éste y es, por lo tanto, desconocido para el software antivirus.

Es una forma de buscar la solución de un problema mediante métodos no rigurosos como el método de cadenas, chequeo de integridad, algoritmos, desencriptador genérico, etc. A través de los cuales se puede obtener un informe donde se detalla el funcionamiento de la tecnología del software antivirus, dando respuestas en aquellas situaciones en donde los métodos reactivos no pueden darla, detectando un archivo malicioso desconocido para los antivirus.

Virus

ANONIMO (Internet; 1999-2011, 07/11/2011, 1:42) define "Un **virus informático** es un programa o software que se auto ejecuta y se propaga insertando copias de sí mismo en otro programa o documento. Un virus informático se adjunta a un programa o archivo de forma que pueda propagarse, infectando los ordenadores a medida que viaja de un ordenador a otro." Con una definición similar ANONIMO (Internet; 26/09/2005, 07/11/2011, 1:48) "Un virus informático es un programa que puede infectar a otros programas, modificándolos de tal manera que causen daño en el acto (borrar o dañar archivos) o afectar su rendimiento o seguridad." Con lo cual RIVERO, Marcelo (Internet; 13/01/2011, 07/11/2011, 2:01) está de acuerdo "Los Virus Informáticos son sencillamente programas maliciosos **(malware)** que "infectan" a otros archivos del sistema con la intención de modificarlo o dañarlo."

Es un programa malicioso que se propaga insertando copias en programas y archivos dañándolos o afectando ya sea su rendimiento o seguridad.

Gusanos

ANONIMO (Internet; 1999-2011, 07/11/2011, 1:42) "Los gusanos informáticos se propagan de ordenador a ordenador, pero a diferencia de un virus, tiene la **capacidad a propagarse sin la ayuda de una persona**. Un gusano informático se aprovecha de un archivo o de características de transporte de tu sistema, para viajar. " De la misma forma ANONIMO (Panda Security) (Internet; 2013, 2/03/2013, 21:10) define que "Un gusanose copian y se envían masivamente desde un ordenador infectado a todos los miembros de la lista de direcciones." Con lo cual ANONIMO (Panda Security)(Internet; 2011, 07/11/2011, 2:37) está de acuerdo con la siguiente definición "Los Gusanos Informáticos son programas que realizan copias de sí mismos, alojándolas en diferentes ubicaciones del ordenador". El objetivo de este malware suele ser colapsar los ordenadores y las redes informáticas, impidiendo así el trabajo a los usuarios. A diferencia de los virus, los gusanos no infectan archivos."

Son programas que residen en la memoria y se duplican así mismo, se propagan de computador en computador sin ayuda de una persona, aprovechándose de un archivo o de características de transporte del sistema para viajar.

Malware no replicativo

Se considera la definición de HARLEY, David Security Author and Consultant LEE, Andrew ChiefResearchOfficer de ESET (Internet: 27/03/2007, 07/11/2011, 3:20) En la cual deduce de las definiciones anteriores que si un programa malicioso no se replica, no puede ser ni virus ni gusano. Pero eso no significa que el software antivirus no pueda detectarlos o que no sean dañinos. Ya que el malware no replicativo al no replicarse como los virus o gusanos no quiere decir que no puede ser detectado o que no pueda causar algún daño, algunos de los malware no replicativo son intendeds, archivos basura, programas relacionados con virus y programas de testeo legítimos, y uno de los más conocidos es el troyano.

2.3.2. Fundamentación teórica variable dependiente

Información

Se toma en cuenta la versión de CHIAVENATO, Idalberto (2006, Pág. 110) "es un conjunto de datos con un significado, o sea, que reduce la incertidumbre o que aumenta el conocimiento de algo. En verdad, la información es un mensaje con significado en un determinado contexto, disponible para uso inmediato y que proporciona orientación a las acciones por el hecho de reducir el margen de incertidumbre con respecto a nuestras decisiones" Al igual que FERRELL O. C. HIRT, Geoffrey (2004, Pág. 121) "comprende los datos y conocimientos que se usan en la toma de decisiones." Mientras que CZINKOTA, Michael y KOTABE, Masaaki (2001, Pág. 115) nos dice que "consiste en datos seleccionados y ordenados con un propósito específico."

Es un conjunto de datos con un significado en un determinado contexto que se usa en la toma de decisiones con un propósito específico.

Formatos de archivos portables

Para esta definición de han toma en cuenta algunas de las definiciones de los formatos de archivos como la de Carlos López (Docente Ciencias Exactas y Naturales) y Mónica Agudelo (Ingeniera de Sistemas)de la UNIVERSIDAD DE ANTIOQUIA (Internet; 02/03/2013, 21:022) en donde define "Los archivos se pueden dividir en dos grandes grupos: los ejecutables y los no ejecutables o archivos de datos. La diferencia fundamental entre ellos es que los primeros funcionan por si mismos y los segundos almacenan información para ser utilizada con ayuda de algún programa.

Dentro de los archivos de datos se pueden crear grupos, especialmente por la temática o clase de información que almacenen. Por ejemplo: texto, vídeo, audio, gráficos, información comprimida... entre otros". De igual forma ANONIMO (Internet; 1999-2011, 07/11/2011, 4:11) expresa que el pdf captura información del formato de varias aplicaciones, haciendo posible que aparezcan en el monitor de la persona que lo recibe o en la impresora exactamente como fueron creados. Por otro lado es importante considerar a MARÍA JESÚS LAMARCA LAPUENTE (Internet; 05/11/2011, 02/03/2013, 21:40) en la cual considera otro formato de archivo importante como "**pdf** Identifica archivos cuyo contenido está en formato PDF. Este formato debe su nombre al acrónimo del inglés *Portable DocumentFormat* y permite transferir documentos como folletos, trípticos y en general, aquellos que contengan diseño gráfico y utilicen fuentes tipográficas especiales, con la seguridad de que se verán en la forma adecuada, sin importar el tipo de equipo que se utilice. Este formato fue creado por Adobe Systems, Inc, pero existen otros programas no propietarios que generan este tipo de archivos."

Entre los formatos de archivos portables más utilizados tenemos el PDF y PNG que nos permiten y facilitan la creación de documentos con todo tipo de datos e información como imágenes, tablas, etc.

Vulnerabilidades de los formatos de archivos

ANONIMO (Panda Security) (Internet; 2011, 04/11/2011, 4:31) considera que las vulnerabilidades son "Fallos o huecos de seguridad detectados en algún programa o sistema informático, que los virus utilizan para propagarse e infectar." Mientras que BOSCH, Ángel (Internet; 2000-2003, 04/11/2011, 4:44) opine que esta vulnerabilidad consiste en que hay un error en el tratamiento de este tipo de ficheros, que permite la ejecución arbitraria de código en las máquinas vulnerables. Esto puede conseguirse mediante verdaderas imágenes PNG malformadas que, al ser procesadas por alguno de los productos afectados, puede provocar la falla del equipo. También menciona RUIZ, Ángela (Internet; 04/01/2007, 04/11/2011, 4:48) que Múltiples vulnerabilidades han sido identificadas en esta aplicación, las cuáles pueden ser explotadas por atacantes remotos para provocar denegación de servicio (que el programa deje de responder), o para ejecutar scripts de comandos (JavaScript), lo que permitiría tomar el control completo del equipo que ejecute las versiones vulnerables de este programa.

Las vulnerabilidades pueden ser fallos en programas o sistemas informáticos lo que permite que los atacantes de alguna forma introduzcan código malicioso en los archivos de forma que al abrir el archivo el código malicioso incrustado se ejecute, causando algún daño en el computador.

Documentos PDF Maliciosos

Se considera la opinión de NONES, Javier (Internet; 18/02/2011, 04/11/2011, 20:05) quien ha manifestado que casi todos los ataques se producen mediante el servicio de correo electrónico. Los hackers actualmente crean y envían mails que pretenden ser

de un contacto de confianza refiriéndose a temas rutinarios. Por último adjuntan malware que les concede acceso sin restricciones para robar datos e información sensible de los computadores infectados. Mientras que JAIRO(Internet; 03/03/2011, 04/11/2011, 20:025) comenta que los archivos PDF son incluso más peligrosos que los .EXE porque es mucho más fácil ocultar contenido malicioso en archivos PDF y gozan de cierta popularidad y de relativa confiabilidad. Una investigación de LARKIN, Erik (Internet; 05/01/2010, 04/11/2011, 21:35) menciona que "PC World México te recomienda tener especial precaución si recibes en estos días un correo no deseado con un archivo en formato PDF. Los recientes informes indican que los hackers están aprovechando una vulnerabilidad de este tipo de ficheros para perpetrar ataques.

Los atacantes crean y envían documentos PDF maliciosos mediante el servicio de correo electrónico, adjuntando malware o a su vez pueden tener incrustado en el código java script código malicioso el cual se ejecuta en el momento en que se abren un archivo que les concede acceso sin restricción para robar datos e información sensible del computador.

Robo de información personal

MIERES, Jorge, BORGHELLO, Cristian (Internet; 26/06/2008, 07/11/2011, 10:00) deduce que las metodologías actuales para robar información confidencial son muchas y mutan continuamente en el tiempo, por lo que estar informados sobre ellas se ha vuelto fundamental. Al igual que ANONIMO (Internet; septiembre/2011, 07/11/2011, 10:11) quien menciona que el robo de identidad se produce cuando alguien usa su nombre, su número de Seguro Social o alguna otra información de índole personal, financiera o médica sin su permiso, para cometer un fraude u otros delitos. En lo cual coincide GARRIDO, Solange (Internet; 06/02//2010,11:04, 07/11/2011, 10:21) expresando que r**obar dinero nunca ha sido más fácil gracias a**

internet, estos crímenes no dejan de crecer por las facilidades que da internet de actuar a distancia y sin dejar rastro.

La mayoría de las personas comparten información valiosa, ya sea en redes sociales, cuentas de correo, etc. Lo cual permite que los hackers o intrusos obtengan información valiosa haciendo mal uso de la misma, además muchas veces la introducción de código malicioso al computador provoca que el atacante obtenga información valiosa.

Daños a equipos informáticos

RECOVERY LABS EMPRESA ESPAÑOLA (Internet; 2012, 02/03/2013, 22:46) menciona que el delito informático como: "los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos". Coincidiendo con MANSON, Marcelo (Internet; 25/01/2007,17:50, 07/11/2011, 10:38) el cual menciona que dado el carácter transnacional de los delitos cometidos mediante el uso de las computadoras, es conveniente establecer tratados de extradición o acuerdos de ayuda mutua entre los países.

El daño en los equipos informáticos puede darse por muchas razones como por ejemplo: su mala utilización, falta de mantenimiento cada cierto periodo, pero uno de los daños más importantes son los causados por la introducción de código malicioso provocando daños irreparables al equipo tanto de software como hardware.

Eliminar el contenido del computador

Se ah tomado en cuenta el comentario de MENDOZA, Alfredo (Internet; Noviembre/2004, 07/11/2011, 11:33). Un virus informático puede estar oculto en cualquier sitio, cuando un usuario ejecuta algún archivo con extensión .exe que es portador de un algún virus todas las instrucciones son leídas por la computadora y procesadas por ésta hasta que el virus es alojado en algún punto del disco duro o en la

memoria del sistema. Mientras que ANONIMO (Internet; febrero/2008, 07/11/2011, 12:04) expresa que dependiendo del tipo de malware se podría perder toda la información contenida en las unidades de disco infectadas (incluidas las unidades de red). Y que se podría además perder la estructura de cada una de las unidades de disco (por lo menos de la principal), mediante el formateo de éstas. Estos daños son muy difícilmente reparables y algunos de ellos irreparables.

Dependiendo del tipo de virus ejecutado, puede afectar gravemente al computador provocando pérdidas de información y/o archivos que se encuentren en las unidades de disco infectadas, estos daños podrían ser muy difíciles de reparar o irreparables.

2.4. Hipótesis

El análisis heurístico de malware influirá en la disminución de la introducción de virus a través de los documentos PDF maliciosos en los computadores de los funcionarios del Gobierno Autónomo Descentralizado Municipalidad de Ambato.

2.5. Señalamiento de variables

Variable Independiente X: Análisis heurístico de malware.
Variable Dependiente Y: Documentos PDF maliciosos.

CAPITULO III

3. MARCO METODOLOGICO

3.1. Enfoque

El presente trabajo investigativo tomara un enfoque Cuali - Cuantitativo por las siguientes consideraciones:
Siempre se considerara el entorno del trabajo de los funcionarios en el Municipio de Ambato y se respetaran sus principios, culturas y opiniones de cada uno de ellos, además abra un respeto mutuo entre los compañeros de trabajo y no se forzara a realizar más trabajo de lo necesario siempre y cuando los funcionarios estén de acuerdo. La aplicación de la solución se realizara explícitamente dentro de Municipio de Ambato. Con el análisis heurístico de malware se definirá una norma a seguir para llevar a cabo los objetivos planteados.

3.2. Modalidades básicas de la Investigación

La presente investigación tiene las siguientes modalidades:

Modalidad Bibliográfica o documentada: Se ha considerado esta medidas ya que se han utilizado, diccionarios virtuales, libros, tesis de grado, internet, bibliotecas.

Modalidad Experimental: Se ha considerado la relación de la variable independiente, análisis heurístico de malware y su influencia y relación en la variable dependiente documentos PDF maliciosos para considerar sus causas y sus efectos.

Modalidad de Campo: Se ha considerado esta modalidad ya que el investigador ira a recoger la información primaria directamente de los involucrados a través de una encuesta.

3.3. Tipos de Investigación

Se ha realizado la investigación exploratoria, ya que permitió plantear el problema de la investigación "El insuficiente análisis heurístico de malware incide en el contagio a través de documentos pdf maliciosos en los computadores de los funcionarios en el Gobierno Autónomo Descentralizado Municipalidad de Ambato." Como de la misma manera ayudo a plantear la hipótesis "El análisis heurístico de malware influirá en la disminución de la introducción de virus a través de los documentos PDF maliciosos en los computadores de los funcionarios en el Gobierno Autónomo Descentralizado Municipalidad de Ambato."

Se ha considerado la investigación descriptiva, porque permitió analizar el problema en sus partes como delimitar el tiempo y el espacio construyendo el análisis crítico, la contextualización y los antecedentes investigativos.

Por otro lado se ha tomado la Investigación correlacional, ya que ha permitido medir la compatibilidad de la variable dependiente documentos maliciosos con la variable independiente análisis heurístico de malware.

3.4. Población y Muestra

3.4.1. Población

La población que se va a considerar para la presente investigación son los funcionarios del Gobierno Autónomo Descentralizado Municipalidad de Ambato mismos que se estima alcanzan un número de 550.

3.4.2. Muestra

Del total de la población se tomara un grupo para aplicar las encuestas, utilizando la fórmula de la muestra.

Cálculo de la muestra:

$$N = \frac{PQN}{(N-1)E^2/K^2 + PQ}$$

$$N = \frac{0{,}25(550)}{(550 - 1)0{,}1^2/2^2 + 0{,}25}$$

$$N = \frac{137}{(449)0{,}1^2/4 + 0{,}25}$$

$$N = \frac{137}{4{,}49/4 + 0{,}25}$$

$$N = \frac{137}{1.1225 + 0{,}25}$$

$$N = \frac{137}{1.3725}$$

N= 99.81

N=100

3.5. Operacionalización de variables.

Variable independiente: Análisis heurístico de malware.

Concepto	**Categorías**	**Indicadores**	**Ítems**	**Técnicas e Instrumentos**
Es una forma de buscar la solución de un problema mediante métodos no rigurosos como el método de cadenas, chequeo de integridad, algoritmos, desencriptador genérico, etc. A través de los cuales se puede obtener un informe donde se detalla el funcionamiento de la tecnología del software	Métodos Método de cadenas Chequeo de integridad Algoritmos	• Técnicas • Si • No • Si • No • Ordenamiento Búsqueda •	¿Tiene conocimiento de algunas técnicas que prevengan el contagio de virus a través de documentos PDF maliciosos? ¿Conoce el método de cadenas y como funciona en la detección de código malicioso? ¿Tiene alguna idea de la funcionalidad del chequeo de integridad en el análisis heurístico, que hace o cómo funciona? ¿En el municipio de Ambato por alguna razón se ha utilizado ya sea los algoritmos de ordenamiento o búsqueda?	Encuestas a través de cuestionarios a los funcionarios del Municipio.

antivirus, dando respuestas en aquellas situaciones en donde los métodos reactivos no pueden darla, detectando un archivo PDF malicioso desconocido para los antivirus.	Desencriptador genérico Software antivirus Métodos reactivos	• Técnicas • Si • No • Si • No	¿El desencriptador genérico es una técnica que ayuda al análisis heurístico de malware, tiene algún conocimiento sobre esta técnica? ¿Qué software antivirus tiene instalado en su computador, y cuan eficiente cree usted que es? ¿Tiene algún conocimiento sobre los métodos reactivos para la detección de código malicioso, que hace o como funciona?	

Variable Dependiente: Detección de documentos PDF maliciosos.

Concepto	**Categorías**	**Indicadores**	**Ítems**	**Técnicas y Instrumento**
Los atacantes crean y envían documentos maliciosos mediante el servicio de correo electrónico, adjuntando malware o a su vez pueden tener incrustado en el código java script código malicioso, el cual se ejecuta en el momento en que se abre un archivo que les concede acceso sin restricción para robar	Atacantes Documentos maliciosos Correo electrónico	• Hackers • Crackers • Word • Excel • Power point • Adobe • Correo POP Web mail o Correo web	¿Durante todo el tiempo que se encuentra trabajando en el Municipio de Ambato alguna vez ha sido víctima de algún tipo de ataque ya sea por Hackers, Crackers o algún otro tipo de ataque? ¿Sabía usted que al abrir un documento, como Word, Excel, PowerPoint, Adobe, entre otros, Corre el riesgo de que su computador se infecte de algún tipo de código malicioso? ¿Ah recibido a través del correo electrónico algún tipo de documentos, información basura o links a direcciones extrañas?	Encuestas a través de cuestionarios a los funcionarios del Municipio.

datos e información sensible del computador.	Malware	• Virus • Gusanos • Malware no replicativo	¿Su computador se ha visto afectado por virus, gusanos, o información basura, tiene usted conocimiento del daño que puede causarle?	
	Java script	• Si • No	¿Sabía usted que un archivo al contener código Java Script es más vulnerables a contagiarse de malware, cuáles cree que sean las razones?	
	Información	• Datos • Imágenes • Videos	¿Cuán segura se encuentra la información , datos, imágenes, videos, etc. En el Municipio de Ambato, y qué medidas se han tomado para hacerlo?	
	Computador	• De escritorio • Portátiles	¿Qué tipo de computador utiliza para su trabajo, de escritorio, portátiles?	

3.6. Recolección y análisis de la Información

Secundaria	**Primaria**
Se recolecta de estudios realizados anteriormente	Se recolecta directamente del contacto con los funcionarios en el Gobierno Autónomo Descentralizado del Ilustre Municipio de Ambato.
Se encuentra registrada en documentos y material impreso: libros, informes técnicos, tesis de grado, etc.	
Las fuentes de información son: bibliotecas de la facultad, internet, repositorios de tesis.	

Técnicas de Investigación

Bibliográficas	De Campo
El análisis de documentos (lectura científica)	
El fichaje	
	La Encuesta

Recolección de la información

Preguntas	Explicación
1. ¿Preguntas?	Recolectar información primaria para comprobar y contrarrestar con la hipótesis.
2. ¿A qué personas o sujeto?	La información será tomada de los funcionarios en el Gobierno Autónomo Descentralizado del Ilustre Municipio de Ambato.
3. ¿Sobre qué aspectos?	VI: Análisis heurístico de malware VD: Documentos PDF Maliciosos

4. ¿Quién?	La Investigadora
5. ¿Cuándo?	De acuerdo al cronograma establecido
6. ¿Lugar de recolección de información?	Gobierno Autónomo Descentralizado del Ilustre Municipio de Ambato.
7. ¿Cuántas veces?	Una sola vez
8. ¿Qué técnica de recolección?	Encuesta
9. ¿Con que?	Cuestionario
10. ¿En qué situación?	Situación normal y cotidiana

3.7. Procesamiento y Análisis de la Información

Revisión y codificación de la información

Categorización y tabulación de la información

Tabulación manual

Tabulación computarizada programa SPSS

Análisis de los datos

La interpretación de los datos se lo hará en gráficos cuadros para analizarlos e interpretarlos.

Interpretación de los resultados

1. Describir los resultados y analizar la hipótesis en relación con los resultados obtenidos para verificarla o rechazarla.

2. Estudiar cada uno de los resultados por separado.

3. Redactar una síntesis general de los resultados.

CAPITULO IV

4. ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

4.1. Análisis de la necesidad

El Gobierno Autónomo Descentralizado Municipal de Ambato al ser una institución gubernamental tiene la obligación de mantener la información segura, es decir se deben cumplir los requerimientos de seguridad informática mencionados anteriormente en el capítulo II.

Entonces existe la necesidad de realizar un análisis heurístico de malware dentro de la Municipalidad de Ambato para dar posibles soluciones y así salvaguardar la información que día a día es transmitida por la red.

4.2. Análisis de los resultados

Para determinar la necesidad se realizó encuestas aplicadas a los funcionarios del Gobierno Autónomo Descentralizado Municipal de Ambato el cual está conformado por 550 funcionarios de los cuales se trabajaran únicamente con 100 que son el resultado de la muestra aplicada anteriormente.

Una vez aplicada la encuesta se obtuvieron como resultado los siguientes datos.

1. ¿Tiene conocimiento de algunas técnicas que prevengan el contagio de virus a través de documentos PDF maliciosos?

N°	Ítems	Frecuencia	%
1	Si	29	29
2	No	71	71
Total		100	100%

Tabla 1 : Tabulación de la entrevista - pregunta 1

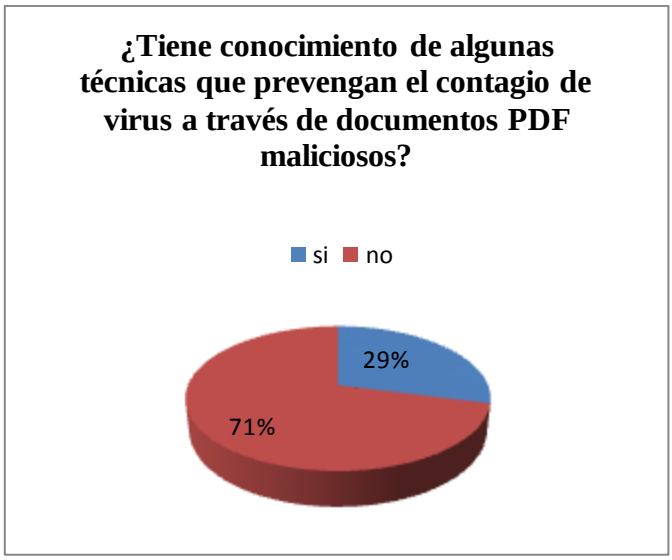


Figura 4. 1: Tabulación de la entrevista - pregunta 1

Análisis Cuantitativo: De las 100 personas 29 encuestados que representan el 29 % indican que si tienen conocimiento de algunas técnicas que prevengan el contagio de virus a través de documentos PDF maliciosos mientras que 71 encuestados que representan el 71 % indican que no tienen conocimiento de algunas técnicas que prevengan el contagio de virus a través de documentos PDF maliciosos.

Análisis Cualitativo: Por lo tanto se demuestra que en la institución la mayoría de los funcionarios no tiene conocimientos de algún software que prevenga el contagio de virus a través de documentos PDF maliciosos, por lo que va a ser necesario que se dé a conocer el funcionamiento de algunos software o herramientas para que posterior mente puedan ser implementados de ser necesario.

2. ¿Conoce el método de cadenas y como funciona en la detección de código malicioso?

N°	Ítems	Frecuencia	%
1	si	29	29
2	no	71	71
Total		100	100%

Tabla 2: Tabulación de la entrevista - pregunta 2

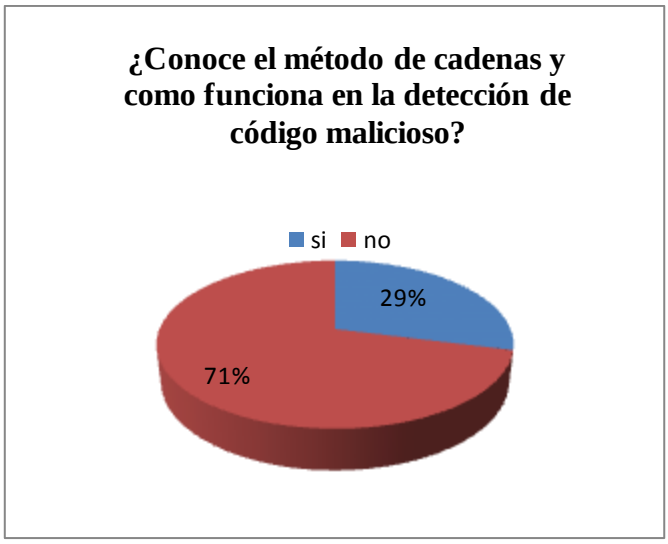


Figura 4. 2: Tabulación de la entrevista - pregunta 2

Análisis Cuantitativo: De las 100 personas 29 encuestados que representan el 29 % indican que si conoce el método de cadenas y como funciona en la detección de código malicioso mientras que 71 encuestados que representan el 71 % indican que no conoce el método de cadenas y como funciona en la detección de código malicioso.

Análisis Cualitativo: En la Municipalidad de Ambato existe un gran desconocimiento por parte de los funcionarios sobre el funcionamiento del software antivirus que se utiliza actualmente.

3. ¿Tiene alguna idea de la funcionalidad del chequeo de integridad en el análisis heurístico, que hace o cómo funciona?

N°	Ítems	Frecuencia	%
1	si	14	14
2	no	86	86
Total		100	100%

Tabla 3: Tabulación de la entrevista - pregunta 3

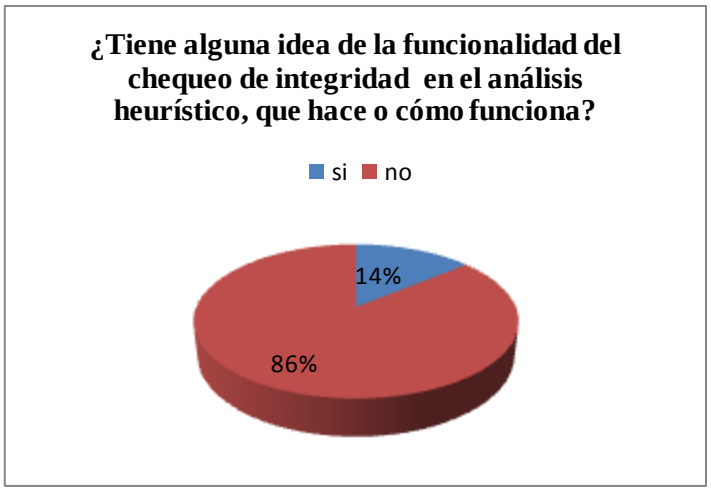


Figura 4. 3: Tabulación de la entrevista - pregunta 3

Análisis Cuantitativo: De las 100 personas 14 encuestados que representan el 14 % indican que si conoce la funcionalidad del chequeo de integridad en el análisis heurístico mientras que 86 encuestados que representan el 86 % indican que no conoce la funcionalidad del chequeo de integridad en el análisis heurístico.

Análisis Cualitativo: El chequeo de integridad es un tema innovador y desconocido para las personas que trabajan en la Municipalidad de Ambato, las personas que tienen un leve conocimiento son los que trabajan en el área de sistemas.

4. ¿En el municipio de Ambato por alguna razón se ha utilizado los algoritmos de ordenamiento o de búsqueda?

N°	Ítems	Frecuencia	%
1	si	3	3
2	no	14	14
3	desconoce	83	83
Total		100	100%

Tabla 4: Tabulación de la entrevista - pregunta 4

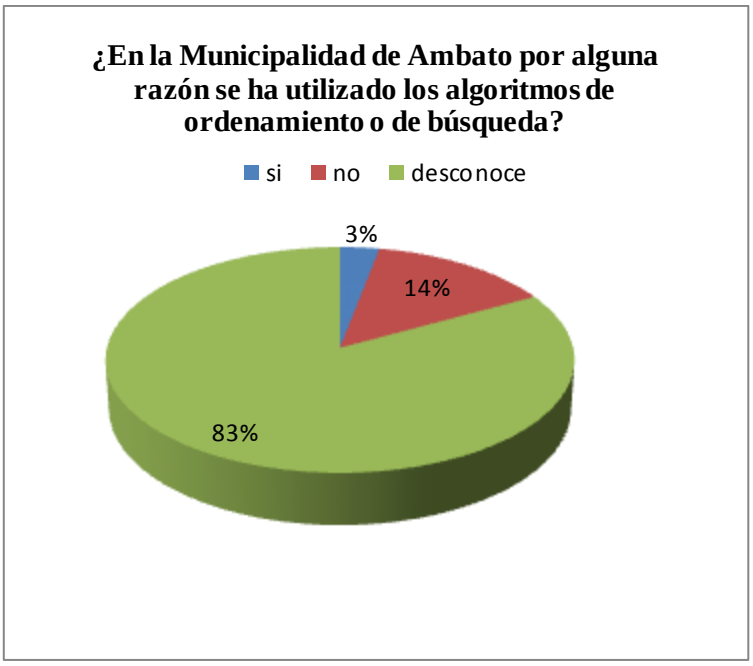


Figura 4. 4: Tabulación de la entrevista - pregunta 4

Análisis Cuantitativo: De las 100 personas 3 encuestados que representan el 3 % indican que en la Municipalidad de Ambato se ha utilizado los algoritmos de ordenamiento o de búsqueda mientras que 14 encuestado que representan el 14 % indican que en el municipio de Ambato no se ha utilizado los algoritmos de ordenamiento o de búsqueda, y 83 encuestados que representan el 83 % indican que desconocen si en la Municipalidad de Ambato por alguna razón se ha utilizado los algoritmos de ordenamiento o de búsqueda.

Análisis Cualitativo: Existe un gran desconocimiento del algoritmo de ordenamiento o búsqueda y su función en un software antivirus, debido a la desactualización de la tecnología, ya que esta cambia constantemente.

5. ¿El desencriptador genérico es una técnica que ayuda al análisis heurístico de malware, tiene algún conocimiento sobre esta técnica?

N°	Ítems	Frecuencia	%
1	si	0	0
2	no	100	100
Total		100	100%

Tabla 5: Tabulación de la entrevista - pregunta 5

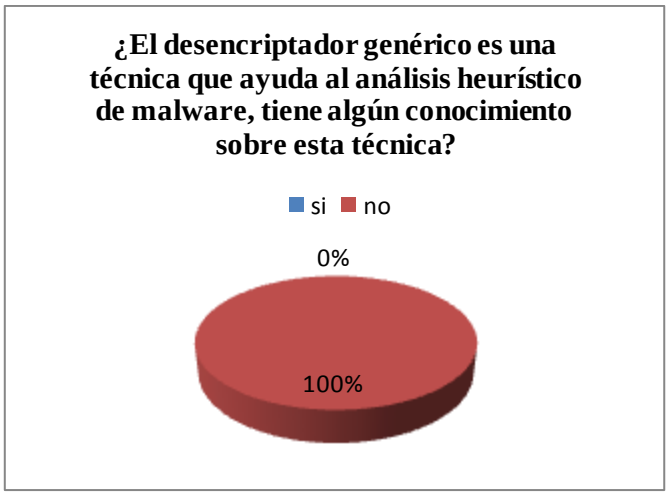


Figura 4. 5: Tabulación de la entrevista - pregunta 5

Análisis Cuantitativo: De las 100 personas 0 encuestados que representan el 0 % indican que si tiene algún conocimiento sobre la técnica del desencriptador genérico que ayuda al análisis heurístico de malware, mientras que 100 encuestados que representan el 100 % indican que no tienen conocimiento sobre la técnica del desencriptador genérico que ayuda al análisis heurístico de malware.

Análisis Cualitativo: El análisis heurístico de malware es un tema innovador y desconocido por parte de los funcionarios de la Municipalidad de Ambato.

6. ¿Qué software antivirus tiene instalado en su computador?

N°	Ítems	Frecuencia	Valores	%
1	AVG	0	0	0
2	AVIRA	0	0	0
3	NOD 32	57	60	57
4	KARPERSKY	43	50	43
Total		100	110	100%

Tabla 6: Tabulación de la entrevista - pregunta 6

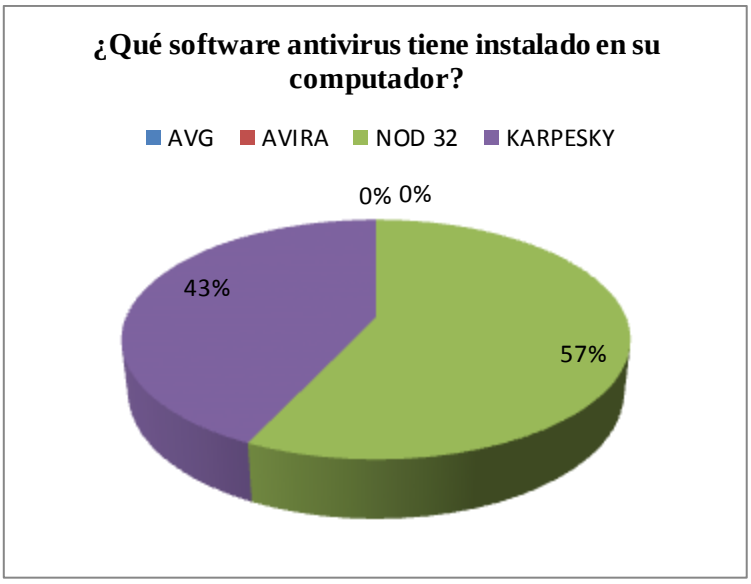


Figura 4. 6: Tabulación de la entrevista - pregunta 6

Análisis Cuantitativo: De las 100 personas 57 encuestados que representan el 57 % indican que el software antivirus que tienen instalado en su computador es el NOD 32 mientras, existen 3 personas de las 57 han indicado que también tienen instalado Karpesky, es decir trabajan con dos software antivirus, mientras que 43 encuestados que representan el 43 % indican que el software antivirus que tienen instalado en su computador es Karpesky, existen 7 personas de las 43 encuestadas quienes han indicado que también tienen instalado NOD 32, estos valores lo podemos ver reflejado en la columna de la tabla con el nombre de valores.

Análisis Cualitativo: En las computadoras de los funcionarios existe una gran seguridad ya que tienen software anti virus con licencia y para reforzar la seguridad en algunos casos se encuentran instalados dos antivirus, los cuales son constantemente actualizados.

7. ¿Tiene algún conocimiento sobre los métodos reactivos para la detección de código malicioso, que hace o cómo funciona?

N°	Ítems	Frecuencia	%
1	Si	14	14
2	No	86	86
Total		100	100%

Tabla 7: Tabulación de la entrevista - pregunta 7

Figura 4. 7: Tabulación de la entrevista - pregunta 7

Análisis Cuantitativo: De las 100 personas 14 encuestado que representan el 14 % indican que si tiene algún conocimiento sobre los métodos reactivos para la detección de código malicioso mientras que 86 encuestados que representan el 86 % indican que no tienen ningún conocimiento sobre los métodos reactivos para la detección de código malicioso.

Análisis Cualitativo: Los funcionarios de la Municipalidad no tienes conocimientos de los métodos reactivos y su funcionamiento en la detección de código malicioso.

8. ¿Durante todo el tiempo que se encuentra trabajando en el Municipio de Ambato alguna vez ha sido víctima de algún tipo de ataque?

N°	Ítems	Frecuencia	%
1	Hackers	14	14
2	Crackers	14	14
3	Lammers	29	29
4	Ninguno	43	43
Total		100	100%

Tabla 8: Tabulación de la entrevista - pregunta 8

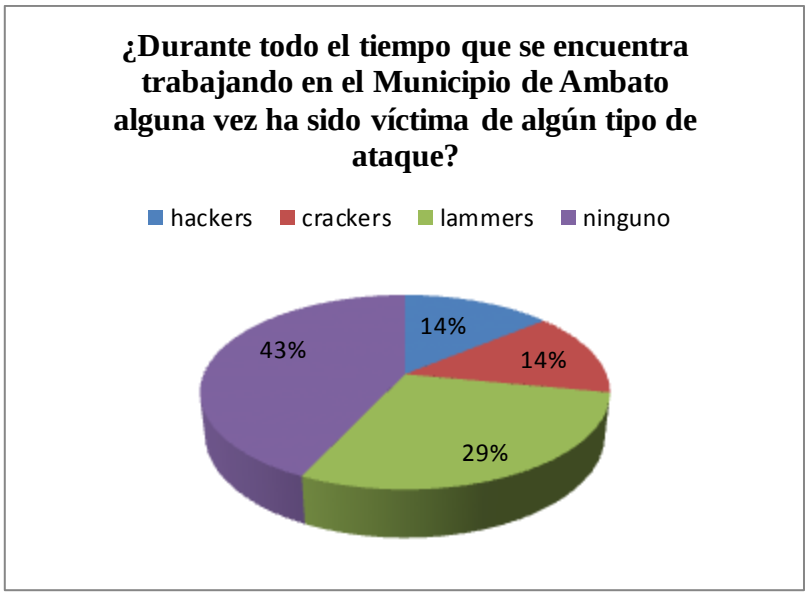


Figura 4. 8: Tabulación de la entrevista - pregunta 8

Análisis Cuantitativo: De las 100 personas 14 encuestados que representan el 14 % indica ha sido víctima de hackers mientras que 14 encuestados que representa el 14 % indica ha sido víctima de crackers, además 29 encuestados que representan el 29 % indican que han sido víctima de lammers mientras que hay 43 encuestados que representan el 43% que indican que no han sido víctimas de ningún tipo de ataque.

Análisis Cualitativo: A pesar de las seguridades y la utilización de un software antivirus en las computadoras de los funcionarios, estos han sido víctimas de algunos ataques. Es decir se encuentran vulnerables a los nuevos ataques que van apareciendo constantemente.

9. ¿Sabía usted que al abrir un documento, como Word, Excel, PowerPoint, Adobe, corre el riesgo de que su computador se infecte de algún tipo de código malicioso?

N°	Ítems	Frecuencia	%
1	si	86	86
2	no	14	14
Total		100	100%

Tabla 9: Tabulación de la entrevista - pregunta 9

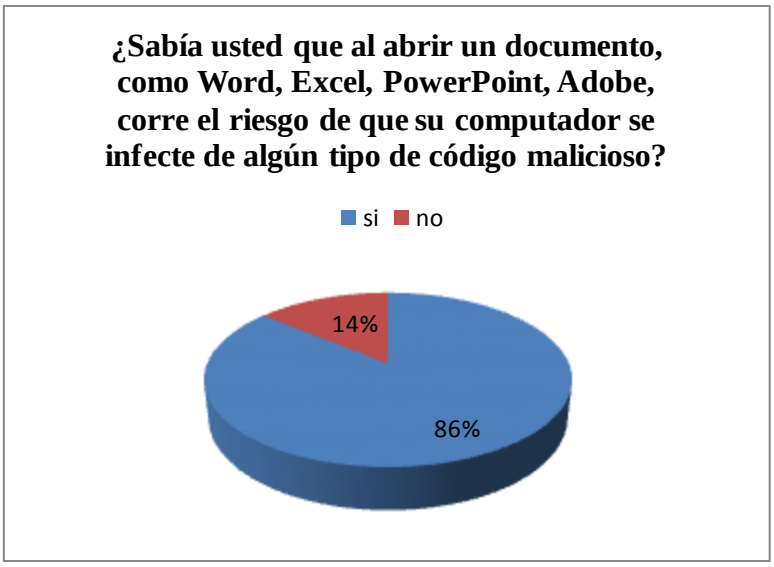


Figura 4. 9: Tabulación de la entrevista - pregunta 9

Análisis Cuantitativo: De las 100 personas 86 encuestados que representan el 86 % indican que tienen conocimiento que al abrir un documento, como Word, Excel, PowerPoint, Adobe, corre el riesgo de que su computador se infecte de algún tipo de código malicioso mientras que 14 encuestados que representan el 14 % indica que no tienen conocimiento que al abrir un documento, como Word, Excel, PowerPoint, Adobe, corre el riesgo de que su computador se infecte de algún tipo de código malicioso.

Análisis Cualitativo: Sería conveniente dar a conocer de qué forma son infectados los archivos pdf ya que existe algo de conocimiento sobre el tema mencionado, y con un poco mas de información se podrían aclarar las ideas que se tiene y a su vez podrían tomar medidas de precaución ante este tipo de ataques.

10. ¿Ah recibido a través del correo electrónico algún tipo de documentos, información basura o links a direcciones extrañas?

N°	Ítems	Frecuencia	%
1	si	100	100
2	no	0	0
Total		100	100%

Tabla 10: Tabulación de la entrevista - pregunta 10

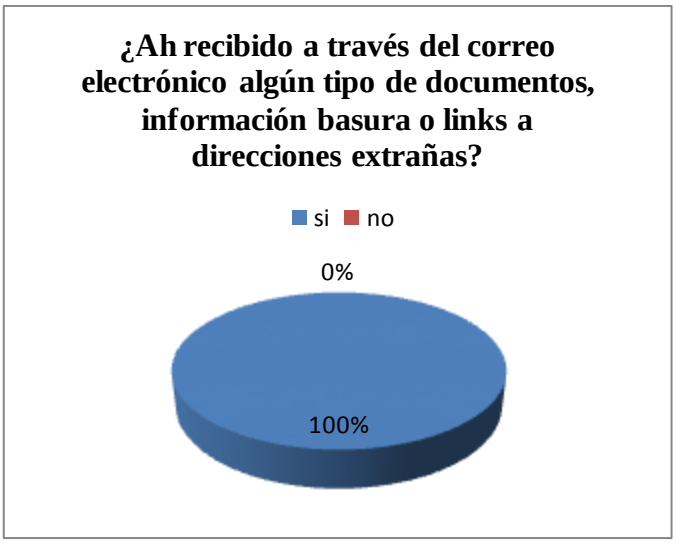


Figura 4. 10: Tabulación de la entrevista - pregunta 10

Análisis Cuantitativo: De las 100 personas los 100 encuestados que representan el 100 % indican que si han recibido a través del correo electrónico algún tipo de documentos, información basura o links a direcciones extrañas.

Análisis Cualitativo: El correo electrónico es la herramienta principal que se utiliza en la municipalidad por el cual se encuentran expuestos los computadores para el contagio de malware.

11. ¿Su computador se ha visto afectado, porque tipo de amenaza?

N°	Ítems	Frecuencia	%
1	Virus	29	29
2	Gusanos	29	29
3	Información basura	42	42
Total		100	100%

Tabla 11: Tabulación de la entrevista - pregunta 11

Figura 4. 11: Tabulación de la entrevista - pregunta 11

Análisis Cuantitativo: De las 100 personas 29 encuestados que representan el 29 % indican que sus computadores se han infectado por virus mientras que 29 encuestados que representan el 29 % indican que sus computadores se han infectado por gusanos y 42 encuestados que representan el 42 % indican que sus computadores han sido infectados por información basura.

Análisis Cualitativo: Por los antecedentes los computadores de los funcionarios han sido infectados constantemente, aunque los daños no han sido lamentables son considerables y sería conveniente prevenirlos o evitar en su totalidad si fuera posible.

12. ¿Sabía usted que un documento al contener código Java Script es más vulnerables a contagiarse de malware?

N°	Ítems	Frecuencia	%
1	si	29	29
2	no	71	71
Total		100	100%

Tabla 12: Tabulación de la entrevista - pregunta 12

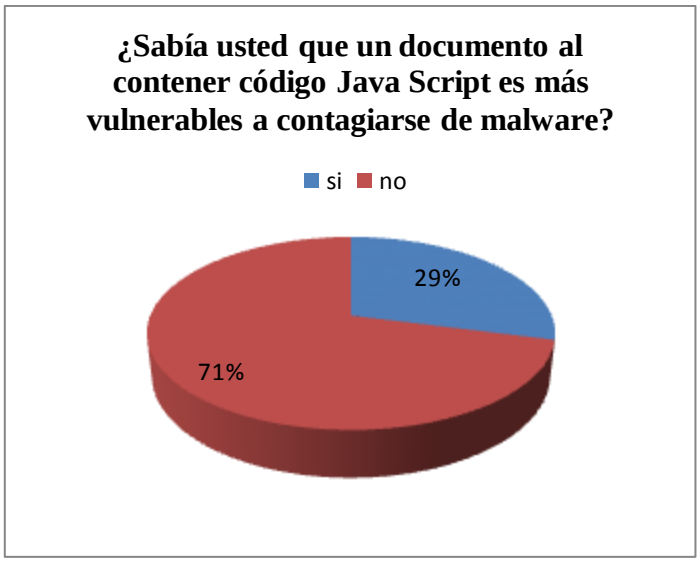


Figura 4. 12: Tabulación de la entrevista - pregunta 12

Análisis Cuantitativo: De las 100 personas 29 encuestados que representan el 29 % indican que si saben que un archivo al contener código Java Script es más vulnerable a contagiarse de malware mientras que 71 encuestados que representan el 71 % indican que no sabían que un archivo al contener código Java Script es más vulnerable a contagiarse de malware.

Análisis Cualitativo: Los documentos PDF pueden estar compuestos de código Java Script de lo cual no están conscientes la mayoría de los funcionarios, por lo que existe mayor riesgo de contagio de algún tipo de código malicioso.

13. ¿Cuán segura se encuentra la información, datos, imágenes, videos, etc. en el Municipio de Ambato?

N°	Ítems	Frecuencia	%
1	Excelente	14	14
2	Muy Buena	57	57
3	Buena	29	29
4	Regular	0	0
Total		100	100%

Tabla 13: Tabulación de la entrevista - pregunta 13

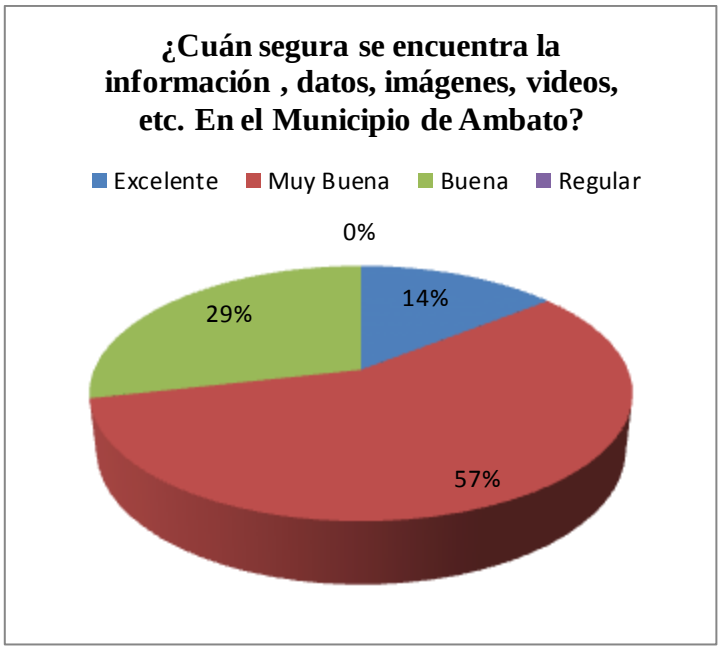


Figura 4. 13: Tabulación de la entrevista - pregunta 13

Análisis Cuantitativo: De las 100 personas 14 encuestados que representa el 14 % indica la protección de la información en el Municipio es excelente mientras que 57 encuestados que representan el 57 % indican que la protección de la información en el municipio es muy buena y 29 encuestados que representan el 29 % indican que la protección de la información en el municipio es buena.

Análisis Cualitativo: La información del municipio debe ser la principal prioridad pero con las nuevas amenazas esto no ha sido posible en su totalidad.

14. ¿Qué tipo de computador utiliza para su trabajo?

N°	Ítems	Frecuencia	%
1	Escritorio	86	86
2	Portátil	14	14
Total		100	100%

Tabla 14: Tabulación de la entrevista - pregunta 14

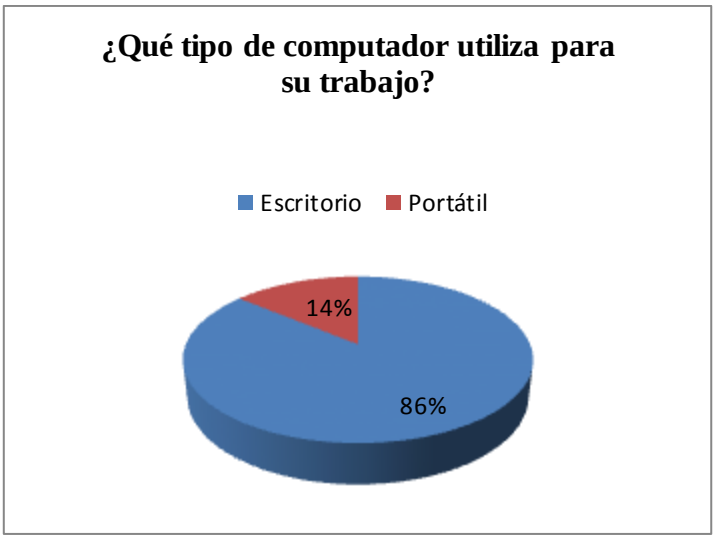


Figura 4. 14: Tabulación de la entrevista - pregunta 14

Análisis Cuantitativo: De las 100 personas 86 encuestados que representa el 86 % indica el tipo de computador utiliza para su trabajo es de escritorio mientras que 14 encuestados que representan el 14 % indican que el tipo de computador utiliza para su trabajo es una portátil.

Análisis Cualitativo: Al estar las computadoras en red existe una mayor probabilidad de contagio.

Interpretación total entrevista

De acuerdo a las versiones que ha manifestado los funcionarios encargados de diferentes áreas en el Gobierno Autónomo Descentralizado Municipal de Ambato, en la institución la mayoría no tiene conocimientos de algún software que prevenga el contagio de virus a través de documentos PDF maliciosos, y existe un gran desconocimiento por parte de los funcionarios de la Municipalidad de Ambato sobre el funcionamiento del software antivirus que se utiliza. Los métodos como el chequeo de integridad, el algoritmo de ordenamiento o búsqueda, los métodos reactivos y el análisis heurístico en si es un tema innovador y poco conocido por las personas que trabajan en las diferentes áreas de la municipalidad.

Las computadoras de los funcionarios son seguras y tienen software antivirus con licencia y para reforzar la seguridad en algunos casos se encuentran instalados dos software antivirus, pero a pesar de las seguridades y el software antivirus las computadoras de los funcionarios han sido víctimas de algunos ataques, siendo el correo electrónico una de las herramientas principales que se utiliza en la municipalidad por la cual se encuentran expuestos los computadores para el contagio de malware.

Por los antecedentes se puede concluir que los computadores de los funcionarios han sido infectados constantemente ya que al estar las computadoras en red existe una mayor probabilidad de contagio, y aunque los daños no han sido lamentables son considerables y sería conveniente prevenirlos o evitarlos en su totalidad si fuera posible ya que la información del municipio debe ser la principal prioridad por lo que sería conveniente dar a conocer de qué forma son infectados los archivos pdf, puesto que existe algo de conocimiento sobre el tema como por ejemplo que los documentos PDF pueden estar compuestos de código Java Script, de lo cual no están conscientes la mayoría de los funcionarios, por lo que existe mayor riesgo de contagio por algún tipo de código malicioso.

CAPÍTULO V

5. CONCLUSIONES Y RECOMENDACIONES

El presente capítulo comprende las conclusiones y recomendaciones fundamentadas en los resultados presentados y analizados, conforme a los objetivos de estudio.

5.1. CONCLUSIONES

- Más del 50 % de los funcionarios del Gobierno Autónomo Descentralizado Municipalidad de Ambato desconoces sobre el funcionamiento de técnicas o métodos que ayuden a la detección de malware, al igual que la función que estos cumplen dentro de cualquier software antivirus.
- Los computadores de los funcionarios del Gobierno Autónomo Descentralizado Municipalidad de Ambato no se encuentran 100 % protegidos, existe una pequeña cantidad que sólo depende de un software antivirus para que el computador no sea contagiado de algún tipo de malware.
- La información de los computadores de los funcionarios del Gobierno Autónomo Descentralizado Municipalidad de Ambato puede ser vulnerada por personas que no necesariamente sea expertos en la materia.
- Todos los funcionarios del gobierno autónomo descentralizado municipalidad de Ambato han sido víctimas de diferentes tipos de ataques y están propensos a que las introducciones de malware sean reincidentes.
- Las razones por las que los funcionarios siguen siendo víctimas de ataques y contagio de malware es que no tienen un amplio conocimiento sobre las nuevas formas de contagio como puede ser abrir un documento, Word, Excel, PowerPoint, Adobe, por lo que corren el riesgo de que los computadores se infecten de algún tipo de malware.

5.2. RECOMENDACIONES

- Realizar capacitaciones cada cierto periodo de tiempo para dar a conocer el general la importancia de resguardar la información y cómo hacerlo, ente otras cosas.
- Instalar en los computadores de los funcionarios del Gobierno Autónomo Descentralizado Municipalidad de Ambato más de un software antivirus eficiente, siempre y cuando sean compatibles.
- Incorporar políticas y procedimientos para que la información un pueda ser fácilmente vulnerada, en especial por los mismos funcionarios del Gobierno Autónomo Descentralizado Municipalidad de Ambato.
- Incrementar el nivel de seguridad especialmente en los servidores de correo y las páginas sociales.
- Contar con un análisis heurístico de malware aplicado a la detección de documentos PDF maliciosos en el Gobierno Autónomo Descentralizado Municipalidad de Ambato.

Preguntas Discriminantes

8.- ¿Durante todo el tiempo que se encuentra trabajando en el Municipio de Ambato alguna vez ha sido víctima de algún tipo de ataque?

Los funcionarios del Gobierno Autónomo Descentralizado Municipal del Ambato manifiesta que a pesar de las seguridades y el software anti virus las computadoras han sido víctimas de algunos ataques y se encuentran vulnerables a los nuevos ataques que van apareciendo con los avances tecnológicos.

9.- ¿Sabía usted que al abrir un documento, como Word, Excel, PowerPoint, Adobe, corre el riesgo de que su computador se infecte de algún tipo de código malicioso?

Los entrevistados indican que en el Gobierno Autónomo Descentralizado Municipal del Ambato existe algo de conocimiento sobre el tema mencionado, pero no lo suficiente como para poder tomar medidas así que sería conveniente dar a conocer de qué forma son infectados los archivos PDF.

Comentario

Se han tomado en cuenta las dos preguntas discriminantes, la número 8 y la número 9 de la encuesta aplicada, ya que de los resultados arrojados, nos dice que como en cualquier empresa la información no es 100 % segura y que a pesar de las medidas de seguridad que se han tomado durante todo este tiempo la información aún sigue siendo vulnerada y que todos los funcionarios del Gobierno Autónomo Descentralizado Municipalidad de Ambato han sido víctimas de diferentes tipos de ataques los cuales pueden llegar a causar serios daños en la Municipalidad. Además hay que tomar en cuenta que una de las razones por la cuales los funcionarios siguen siendo víctimas es que no tienen un amplio conocimiento sobre las nuevas formas de contagio como que al abrir un documento, como Word, Excel, PowerPoint, Adobe, corre el riesgo de que su computador se infecte de algún tipo de código malicioso, entre otros.

CAPITULO VI

6. PROPUESTA

6.1. Datos Informativos

- **Titulo**

Análisis heurístico de malware aplicado a la detección de documentos PDF maliciosos en el Gobierno Autónomo Descentralizado Municipalidad de Ambato.

- **Institución ejecutora**

Gobierno Autónomo Descentralizado Municipalidad de Ambato

- **Director de tesis**

Ing. Msc. Alberto Arellano

- **Beneficiario**

Funcionarios del Gobierno Autónomo Descentralizado Municipalidad de Ambato

- **Ubicación**

Bolívar y Castillo

- **Tiempo estimado para la ejecución**

Fecha de inicio: Enero 2012

Fecha de finalización: Diciembre 2012

- **Equipo técnico responsable**

➢ Investigadora: Ana Morocho

6.2. Antecedentes de la Propuesta

Los funcionarios del Gobierno Autónomo Descentralizado Municipalidad de Ambato desconocen sobre el funcionamiento de técnicas o métodos que ayuden a la detección de malware. Por lo que los computadores no se encuentran 100 % protegidos, además de que existe una pequeña cantidad que solo depende de un software antivirus para que el computador no sea contagiado de algún tipo de malware. La información puede ser vulnerada por personas que no necesariamente sea expertos en la materia y hay que tomar en cuenta que todos los funcionarios han sido víctimas de diferentes tipos de ataques y están propensos a que las introducciones de malware sean reincidentes. Las razones por las que los funcionarios siguen siendo víctimas de ataques y contagio de malware es que no tienen un amplio conocimiento sobre las nuevas formas de contagio como abrir un documento por lo que corren el riesgo de que los computadores se infecten de algún tipo de malware.

La realización de capacitaciones cada cierto periodo de tiempo para dar a conocer en general la importancia de resguardar la información y cómo hacerlo, ente otras cosas podría ser una forma de prevención además de instalar en los computadores de los funcionarios del Gobierno Autónomo Descentralizado Municipalidad De Ambato más de un software antivirus eficiente e incorporar políticas y procedimientos para que la información no pueda ser fácilmente vulnerada, en especial por los mismos funcionarios. También se debería incrementar el nivel de seguridad especialmente en los servidores de correo y las páginas sociales y por último se sugeriría contar con un análisis heurístico de malware aplicado a la detección de documentos PDF maliciosos en el Gobierno Autónomo Descentralizado Municipalidad de Ambato.

6.3. Justificación

El análisis heurístico de malware es una investigación necesaria para Gobierno Autónomo Descentralizado Municipalidad de Ambato. Los aportes que se hace con respecto a una información más segura para los funcionariosse resumen en estas 5 funciones:

- **Se dará a conocer una nueva forma de contagio de malware**

Lo que se logrará es dar a conocer a los funcionarios son las nuevas formas de contagio que han aparecido y como es su funcionamiento al igual que se especificará como afecta el contagio a través de documentos PDF maliciosos a los computadores, ya que el formato de archivo pdf es el que más se utiliza para guardar la información.

- **Evitará la introducción de malware**

Con la información adquirida, los funcionarios evitarán correr riesgos de contagios y tomarán sus propias medidas de seguridad de acuerdo a su labor de trabajo.

- **Protegerá la información**

Se tomarán medidas de seguridad las cuales si el personal autorizado y encargado de la parte de sistemas está de acuerdo, se implementará en el lugar y tiempo en el cual consideren pertinente.

- **Incrementará de seguridad**

Se incrementarán las políticas de seguridad, reglas y se tomarán las medidas de seguridad necesarias entre otras cosas, las cuales impedirán o minimizarán el contagio de algún tipo de malware en los computadores de los funcionarios.

- **Minimizará los riesgos de contagio de malware**

Con el desarrollo de la guía para prevención de contagio de algún tipo de malware y las recomendaciones respectivas se minimizará los riesgos de contagio en los computadores de los funcionarios del Gobierno Autónomo Descentralizado Municipalidad de Ambato.

6.4. Objetivos

6.4.1. Objetivo General

Aplicar el análisis heurístico de malware a través de la aplicación de técnicas para determinar el grado de efectividad en la detección de documentos PDF maliciosos en el Gobierno Autónomo Descentralizado Municipalidad de Ambato.

6.4.2. Objetivos específicos

- Investigar la introducción de virus en los documentos PDF maliciosos.

- Realizar el estudio del análisis heurístico de malware.
- Determinar el mejor software para la detección de documentos PDF maliciosos.
- Realizar las pruebas respectivas para conocer el funcionamiento del análisis heurístico de malware creando un ambiente de simulación.

6.5. Análisis de factibilidad

Según el tipo de propuesta se debe tener en cuenta ciertos aspectos de viabilidad:

Política: Es política de la empresa el permitir realizar cualquier mejora que traiga beneficios a la misma, siempre y cuando se encuentre supervisado por el personal autorizado, el cual brindará ayuda para la realización de cambios en caso de ser necesario.

Socio cultural: Se dará un buen manejo de la información y además se garantiza que será muy bien manejada y con la discreción que se requiere, ya que sólo se dará a conocer al personal autorizado.

Equidad de género: En este aspecto el desarrollo del proyecto de investigación no tendrá ninguna influencia ni preferencia hacia ningún género ya que será estrictamente profesional.

Tecnológico: La Municipalidad de Ambato brindará todos los recursos necesarios para el desarrollo de la tesis en cuanto a software y hardware, tomando en cuenta que el tema a desarrollarse no exige tantos recursos para su correcto desarrollo.

Ambiental: La tesis a realizarse no afectará ni influirá en ningún aspecto en cuanto al medio ambiente se refiere.

Económico-financiera: Para el desarrollo de la investigación no se requerirá de grandes inversiones ya que es estrictamente investigativo y bastara con los recursos con los que hasta el momento dispone la empresa.

Legal: Dentro de las leyes no existe ningún impedimento para la realización del proyecto de investigación por lo que el proyecto no tendría ningún inconveniente en cuanto a la ley se refiere.

6.6. Fundamentación Científico Técnica

6.6.1. Análisis heurístico de malware

6.6.1.1. Definición

HARLEY, David Security Author, Consultant Andrew Lee, ChiefResearchOfficer de ESET(Internet: 27/03/2007, 11:03, 28/10/2011, 20:37) dice "Es un informe que detalla cómo es que funciona la tecnología de los software antivirus. Se destaca el funcionamiento del análisis heurístico, marcando las particularidades de esta tecnología para la detección de las últimas amenazas informáticas desconocidas." Lo cual tiene similitud con BORTNIK, Sebastián, Analista en Seguridad de ESET para Latinoamérica(Internet: 23/05/2010, 12:07, 28/10/2011, 21:00)El objetivo esencial de los algoritmos heurísticos es dar respuestas en aquellas situaciones en donde los métodos reactivos no pueden darla: la capacidad de detectar un archivo malicioso aunque una muestra de éste no haya llegado al laboratorio antivirus. Al igual que FREIRE, José Luis(Internet; 25/06/2000-2008, 29/10/2011, 8:44) quien opina que el análisis heurístico consiste en un sistema de "detección genérica" de códigos maliciosos, es decir, un modo de localizar la presencia de un virus aun cuando no existe vacuna para éste y es, por lo tanto, desconocido para el software antivirus.

6.6.1.2. Heurística

6.6.1.2.1. Definición

BORTNIK, Sebastián, Analista en Seguridad de ESET para Latinoamérica (Internet: 23/05/2010, 12:07, 28/10/2011, 21:00) La etimología de la palabra heurística proviene del griego "heurísko", uno de cuyos significados es encontrar

La Real Academia Española la define como “técnica de la indagación y del descubrimiento”. “

También otorga una segunda definición: “En algunas ciencias, manera de buscar la solución de un problema mediante métodos no rigurosos, como por tanteo, reglas empíricas, etc.”.

Esta última definición es la que mejor se aplica a la utilización de heurística en tecnologías antivirus.

Por lo general la programación heurística es considerada como una de las aplicaciones de la inteligencia artificial y como herramienta para la resolución de problemas. Tal como es utilizada en sistemas expertos, la heurística se construye bajo reglas extraídas de la experiencia, y las respuestas generadas por tal sistema mejoran en la medida en que “aprende” a través del uso y aumenta su base de conocimiento.

La heurística siempre es aplicada cuando no puedan satisfacerse demandas de completitud que permitan obtener una solución por métodos más específicos (por ejemplo la creación de una firma para un malware determinado).

A manera de ejemplo, puede suponerse que un responsable de Recursos Humanos desea contratar un graduado de cierta carrera y se conecta con la universidad. La institución le ofrece un listado de 300alumnos que se graduaron en los últimos años y él debe seleccionar a uno para su contratación. Su capacidad para realizar entrevistas es de 20 personas, por lo que debe tomar una decisión que le permita encontrar al candidato indicado. Una decisión heurística podría ser que se seleccione a los 20alumnos con mejor promedio, lo cual probablemente le permita acercarse a los mejores candidatos. Sin embargo, lo ideal para el responsable de Recursos Humanos sería entrevistar a todos, ya que es probable que haya excelentes candidatos con promedios inferiores. Sin embargo, ante una limitación de completitud, las decisiones heurísticas permiten acercarse al resultado ideal.

Si los alumnos fueran 20, sería posible entrevistar a todos, y elegir sin lugar a dudas el que mejor haya pasado la entrevista. Sin embargo, en este caso es imposible entrevistar a los 300 alumnos y es por ello que se aplican métodos heurísticos.

De igual forma, con las tecnologías reactivas es imposible cubrir la protección necesaria para las condiciones actuales de evolución de amenazas, ya que es no es

posible contar con todos los códigos maliciosos que circulan por Internet, y tampoco se puede disminuir los tiempos de creación de firmas lo suficiente para asegurar protección total al usuario.

Ante estas imposibilidades la aplicación de heurística en tecnologías antivirus ofrece cobertura y protección inteligente ante códigos maliciosos.

6.6.1.2.2. Tipos de heurística

BORTNIK, Sebastián, Analista en Seguridad de ESET para Latinoamérica (Internet: 23/05/2010, 12:07, 28/10/2011, 21:00) Los algoritmos heurísticos, como su pluralidad lo indica, son distintas metodologías de análisis proactivo de amenazas. Se definen a continuación las tres variantes más comunes que son utilizadas en este tipo de análisis:

• Heurística genérica: se analiza cuán similar es un objeto a otro, que ya se conoce como malicioso.

Si un archivo es lo suficientemente similar a un código malicioso previamente identificado, este será detectado como "una variante de…".

• Heurística pasiva: ese explora el archivo tratando de determinar qué es lo que el programa intentará hacer. Si se observan acciones sospechosas, éste se detecta como malicioso.

• Heurística activa: se trata de crear un entorno seguro y ejecutar el código de forma tal que se pueda conocer cuál es el comportamiento del código. Otros nombres para la misma técnica son

"sandbox", "virtualización" o "emulación".

Asimismo, los algoritmos de detección proactiva de amenazas contienen instrucciones que le permiten sortear diversos mecanismos que poseen los códigos maliciosos para ocultar su comportamiento, especialmente el empaquetamiento y el cifrado.

6.6.1.3. Software Anti- Malware

6.6.1.3.1. Definición

La definición de ANONIMO (Panda Security)(Internet; 2011, 07/11/2011, 0:30) expresa que "Se llama **"Malware"** a todo archivo con contenido de carácter malicioso para un equipo informático. Esto no se limita a los virus, pues existen otros muchos archivos capaces de causar daños importantes en un ordenador o en una red informática." Lo cual coincide con BORTNIK, Sebastián (Internet; 23/05/2010,12:07, 07/11/2011, 0:59) Un antivirus es un software que posee la función de detectar códigos maliciosos. Aunque su nombre está relacionado con los virus informáticos, en la actualidad estos programas son soluciones antimalware que poseen protección contra gusanos, troyanos, rootkit, spyware y otros elementos dañinos; es decir, todo tipo de códigos maliciosos.

El software anti-malware, evita la infiltración en el sistema y el daño, proporcionando protección en tiempo real contra la instalación de malware en una computadora y detectando y eliminando malware que ya ha sido instalado en una computadora, poseyendo protección contra gusanos, troyanos, rootkit, spyware y otros elementos dañinos; es decir, todo tipo de códigos maliciosos.

6.6.1.3.2. Funcionamiento

BORTNIK, Sebastián, Analista en Seguridad de ESET para Latinoamérica (Internet: 23/05/2010, 12:07, 28/10/2011, 21:00) Un antivirus es un software que posee la función de detectar códigos maliciosos. Aunque su nombre está relacionado con los virus informáticos, en la actualidad estos programas son soluciones antimalware que poseen protección contra gusanos, troyanos, rootkit, spyware y otros elementos dañinos; es decir, todo tipo de códigos maliciosos.

Además, un antivirus tiene como función identificar una amenaza. Esto se refiere a la capacidad de la aplicación no sólo de detectar un malware, sino también de describir de qué amenaza se trata, tanto por su tipo (virus, troyano, gusano, etc.) como su nombre (por ejemplo Conficker, QHost, Nuwar, etc.).

Finalmente, una vez detectada e identificada cierta amenaza, un antivirus debe prevenir o eliminar la misma del sistema. En el primer caso se trata de un código malicioso que es detectado al momento de intentar infectar un sistema, por lo tanto el

antivirus bloqueará su acceso y prevendrá la infección. En el otro caso, cuando se descubre el malware en un sistema que ya está infectado, el antivirus debe eliminar (o desinfectar) la amenaza.

Sin embargo, tal como se describe en este sencillo proceso de funcionamiento de un antivirus, el primer paso es la detección de un código malicioso. Para este fin el antivirus analiza los archivos (puede ser entiempo real o a petición del usuario) en búsqueda de malware. En su visión simplificada, el antivirus examina cada archivo respondiendo a la pregunta: ¿es un código malicioso?

En esta parte se verá como el software antivirus ha evolucionado y los sistemas de detección empleados para identificar si un archivo es o no una amenaza, complementando los clásicos procedimientos de detección reactivos, basados en firmas, con nuevas técnicas de detección proactivas, basadas en heurística. Estas últimas permiten a los antivirus detectar malware nuevo o desconocido.

Detección reactiva: base de firmas

Desde sus orígenes los antivirus cuentan con un método de detección basado en firmas (también llamadas vacunas). Este emplea una base de datos generada por el fabricante que permite determinar al software si un archivo es o no una amenaza. El sistema es sencillo: se coteja cada archivo a analizar con la base de datos y, si existe coincidencia (es decir, existe en la base una firma que se corresponde con el archivo), se identifica el archivo como código malicioso.

El proceso de generación de firmas se compone de los siguientes pasos:

1. Aparece un nuevo código malicioso
2. El laboratorio de la empresa antivirus recibe una muestra de ese código
3. Se crea la firma para el nuevo código malicioso
4. El usuario actualiza el producto con la nueva base de firmas y comienza a detectar el malware

Figura 6. 1: Proceso de generación de firmas.

Recién a partir del último paso, el sistema estará protegido contra esta amenaza. Aquí radica la importancia de tener actualizado el antivirus: si la firma ya ha sido creada por el fabricante, pero no ha sido descargada en el sistema del usuario, el mismo no estará protegido contra esa amenaza en particular.

Además de la necesidad de mantener actualizada la base de datos, este método posee otras dos desventajas:

• El programa no puede detectar malware que no se encuentre en la base de datos

• El sistema debe contar con una firma por cada variante de un mismo código malicioso

La demora necesaria para generar una firma es variable, y depende del tiempo que tarde el malware en ser descubierto por el laboratorio, de las características del código malicioso y de la dificultad para generar la firma. De una u otra forma, se puede considerar que la demora puede oscilar entre las 2 y las 10 horas; aunque existen casos y excepciones que se escapan de este rango en ambos límites.

En conclusión, la detección por firmas es un método de protección reactivo: primero se debe conocer el malware para que luego sea detectado.

Sin embargo, debido a la alta velocidad de propagación de nuevos códigos maliciosos, y la gran cantidad de nuevas variantes que aparecen día a día, este método se volvió, con el pasar de los años, lento e insuficiente

Un antivirus que utilice sólo métodos reactivos de detección estará protegiendo a sus usuarios sólo de aquellos códigos maliciosos que han sido incorporados a la base de datos, dejando siempre desprotegido al usuario frente a todas las variantes que sean desconocidas por el laboratorio del fabricante, o que aún no posean una firma.

Detección proactiva: heurística antivirus

Para dar solución a esta problemática aparecen los métodos de detección proactivos basados en heurística, como complemento de la detección basada en firmas. Esto quiere decir que la detección proactiva es un agregado a la detección por firmas y para una óptima protección son necesarios ambos métodos, tal como trabajan las soluciones antimalware en la actualidad.

El objetivo esencial de los algoritmos heurísticos es dar respuestas en aquellas situaciones en donde los métodos reactivos no pueden darla: la capacidad de detectar un archivo malicioso aunque una muestra de éste no haya llegado al laboratorio antivirus, y que aún no se posea la firma correspondiente.

Funcionamiento

Los algoritmos heurísticos son la base de la mayor parte de métodos de detección de malware proactivos.

El análisis heurístico posee un comportamiento basado en reglas para diagnosticar si un archivo es potencialmente ofensivo. El motor analítico trabaja a través de su base de reglas, comparando el contenido del archivo con criterios que indican un posible malware, y se asigna cierto puntaje cuando se localiza una semejanza. Si el puntaje iguala o supera un umbral determinado, el archivo es señalado como amenaza y procesado de acuerdo con ello.

De igual modo que un analista de malware intentaría determinar, trabajando en el laboratorio, la peligrosidad de un determinado programa, analizando sus acciones y características (por ejemplo: modifica el registro, se carga al inicio de sesión, elimina

archivos, etc.), el análisis heurístico realiza el mismo proceso de toma de decisiones inteligentes, actuando como un investigador virtual de malware.

Existen diferentes métodos heurísticos que utilizan distintas reglas para determinar si un archivo es o no un código malicioso. Asimismo, un algoritmo de este tipo posee diferentes niveles de rigurosidad para determinar si un archivo es o no dañino. A mayor rigurosidad, mayor es la probabilidad de que se cometa un error en la detección, así como también mayor es la carga de procesamiento al momento del análisis.

A continuación se les dará un ejemplo en el caso de los productos de ESET, que se le permite al usuario seleccionar los métodos de detección y configurarlos según sus requerimientos:

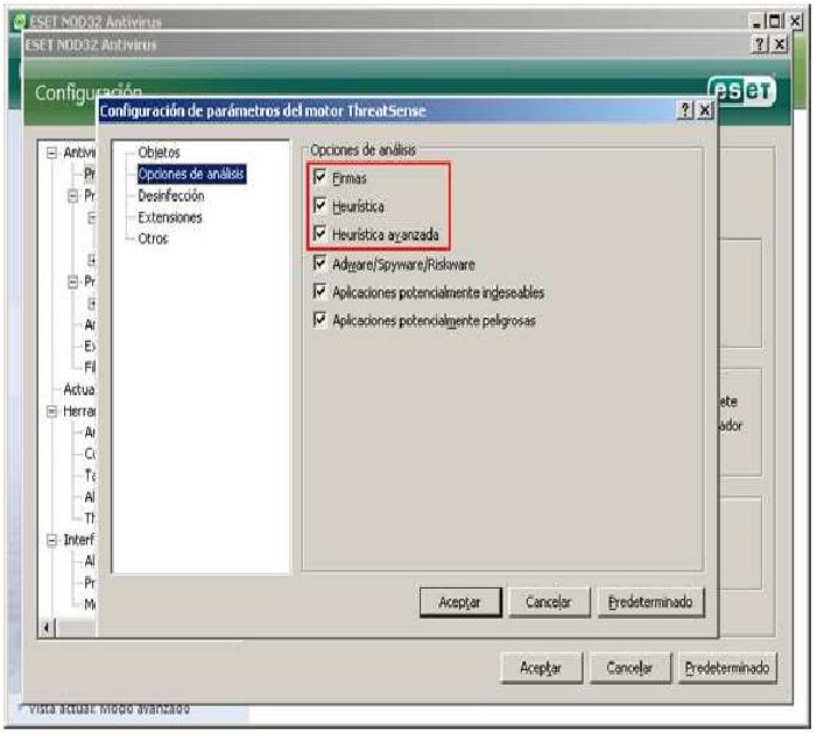


Figura 6. 2: Configuración de detección en ESETNOD 32 Antivirus 4

Mientras que la identificación de una amenaza realizada por medio de una detección reactiva basada en firmas posee la previa legitimación de una persona del laboratorio, la detección proactiva a través de métodos heurísticos no incluye la intervención humana, y en la detección posee un suficiente grado de certeza al respecto como para

afirmar que un archivo es una amenaza. A pesar de esta aparente "desventaja", los algoritmos heurísticos ofrecen protección donde la exploración por firmas no puede darla.

Aunque la detección proactiva no depende de la actualización de la base de firmas, sí debe mantenerse actualizado el programa antivirus, a fin de contar con los últimos algoritmos de detección heurística.

PROPUESTA, cumplimiento del segundo Objetivo Específico

En parte superior se puede observar que se realizado un minucioso estudio sobre el análisis heurístico de malware, con esto se ha logrado conocer el funcionamiento interior de los software antivirus, por lo que se concluye que el segundo objetivo específico de la propuesta se ha cumplido con éxito.

6.6.1.3.3. TIPOS

6.6.1.3.3.1. Metasploit

ANONIMO (Internet: 28/03/2007, 12:09, 15/01/2012, 22:45)Es un proyecto de código abierto desarrollado para la seguridad informática, el cual proporciona información sobre las vulnerabilidades en la seguridad, además de ayudar en tesis de penetración y en lo que tiene que ver con el desarrollo de firmas para sistemas de detección de intrusos.

Su sub proyecto más conocido es el Metasploit Framework, Es toda una plataforma pensada para el desarrollo de herramientas de seguridad. Se utiliza principalmente, para la realización de tesis de intrusión en redes o en servidores. Esto permite conocer las deficiencias de seguridad en estos sistemas y poder solucionarlos antes de que los descubran con intenciones algo más oscuras. Pero la plataforma no viene sola, sino que en el fichero a descargar se incluyen más de 150 exploits distintos, más de 100 payloads, es decir, viene preparada para funcionar desde el primer momento, además que nos ofrece la posibilidad de desarrollar nuestros propios módulos para ampliarlo.

Está escrito en Ruby y es multiplataforma, está disponible para Linux, BSD, Mac OS X y Windows con Cygwin, además de ser totalmente gratuito.

Metasploit, diseñada para facilitar el trabajo de infiltración, considerada como una de las aplicaciones más útiles para practicar hacking (después de notepad, nmap, y opera).

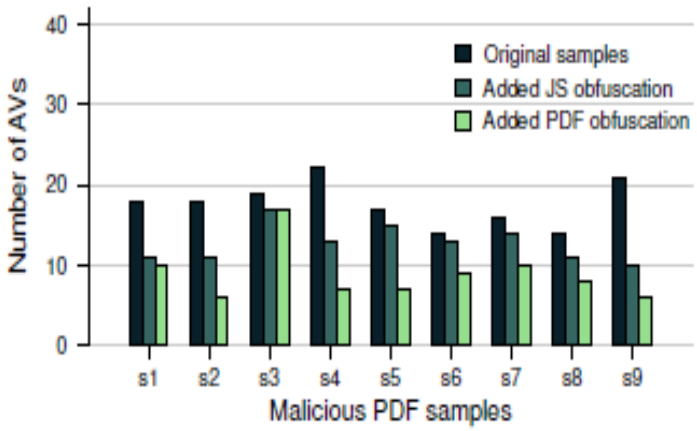


Figure 5: Number of virus scanners (out of 41) of VirusTotal that detected obfuscated versions of malicious PDF files generated using Metasploit.

Figura 6. 3: Detección de virus usando Metasploit

6.6.1.3.3.2. MDScan

ANONIMO (Internet: 28/03/2007, 12:09, 15/01/2012, 22:45)

Diseño e Implementación

La sola presencia de JavaScript en un archivo PDF no indica una mala intención, incluso si el código ha sido ofuscado. Además de obstaculizar el análisis del código malicioso, la ofuscación de código es usado legítimamente para la prevención de ingeniería inversa de las aplicaciones propietarias. MDScan analiza cualquier código embebido, el cual se ejecuta en un JavaScript intérprete. En la ejecución si algún tipo de código Shell se revela en el espacio de direcciones de la intérprete de JavaScript, el documento de entrada se marca como malicioso.

La digitalización de documentos en MDScan consta principalmente de 2 faces:

En la primera fase, MDScan analiza el archivo de entrada y reconstruye la estructura lógica del documento, extrayendo todos los objetos identificados los objetos que contengan el código JavaScript. En la segunda fase, cualquier código JavaScript que se encuentra en el documento, se ejecuta en un JavaScript interprete, el cual en tiempo de ejecución puede detectar la presencia de shellcode incorporado. El diseño de MDScan se presenta en la figura 2. Donde se describen sus principales características y detalles.

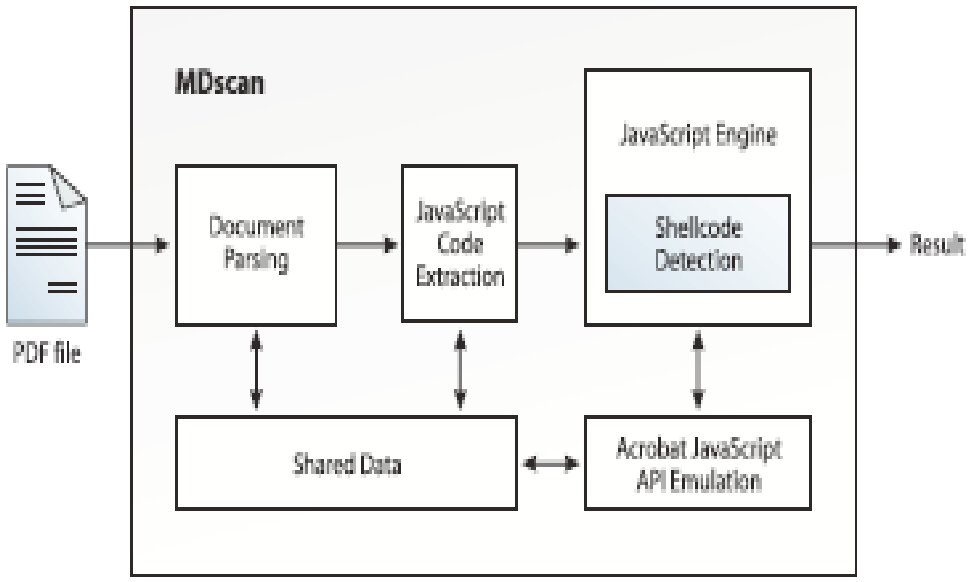


Figura 6. 4: Arquitectura de MDScan

Análisis del documento

MDScan analiza su estructura y extrae todos los objetos identificados, luego son organizados en una estructura jerárquica, la complejidad y las ambigüedades.

Análisis del Archivo

El análisis de archivos comienza con la extracción de todos los objetos encontrados en el cuerpo del documento, incluidos los objetos que han dejado deliberadamente fuera de la tabla de referencias cruzadas. Después de que todos los objetos han sido

identificados, el analizador de los ingresos se encuentra a un paso de normalización que neutraliza nuevas ofuscaciones, y extrae la información semántica sobre cada objeto identificado. En la práctica, los atacantes pueden combinar cualquier número de filtros para correr el código malicioso JavaScript incrustado.

Emulación de la API de JavaScript para Acrobat

Adobe Reader proporciona una extensa API que permite a los autores crear documentos de múltiples funciones con una amplia gama de funcionalidad. La API de JavaScript para Acrobat es accesible como un conjunto de extensiones de JavaScript que proporcionan documentos específicos objetos, propiedades y métodos. El código malicioso puede entonces recuperar sus piezas faltantes o acceder a los datos ocultos a través de la API de Acrobat, y continuar su ejecución.

JavaScript código de Extracción

Después de que todos los objetos extraídos se han analizado, tenemos que identificar los objetos que contienen código JavaScript, y la reconciliación, estructura de la imagen de código completo que se alimentará al motor JavaScript para su ejecución. De acuerdo con la especificación de PDF, los objetos que contienen el código JavaScript se señalan con la palabra clave / JS. El código se puede encontrar en el propio objeto, o en algún otro objeto relacionado con el objeto principal a través de una referencia indirecta (o una cadena de objetos vinculados indirectamente). En este punto, nuestro objetivo es recuperar sólo el código inicial de JavaScript que está configurado para ejecutarse automáticamente cuando el documento se abre.
En la mayoría de los casos, el orden correcto de los trozos de código se puede deducir del ordenamiento coherente de los objetos en el archivo PDF, y las cadenas de referencias indirectas. Sin embargo, también se utilizan algunas heurísticas adicionales para identificar las condiciones de uso antes de la declaración, y reordenar los fragmentos de código respectivo adecuadamente.

La ejecución de código y detección Shellcode

Después de haber extraído el código embebido, MDScan procede en la fase de análisis dinámico, en la que el código se ejecuta en un intérprete de JavaScript. En la mayoría de los archivos PDF maliciosos el objetivo del código JavaScript es poner en funcionamiento una vulnerabilidad capacidad en el visor de PDF, y desviar la ejecución normal el flujo de la shellcode incorporado. El código Shell se puede ocultar potencialmente utilizando múltiples capas de cifrado o transformaciones, como UTF-caracteres codificados, las cadenas de eval, tablas de asignación, u otros sistemas de medida complejo.

Limitaciones

El JavaScript para Acrobat API expone un amplio conjunto de funciones a través de numerosas llamadas a la API. Está claro que nuestro enfoque de emular la funcionalidad de la API de varias llamadas se encuentra en archivos PDF maliciosos no escala bien si el atacante empieza a utilizar una gama más amplia de llamadas a la API en su código.

La complejidad de la aplicación de algunas de las llamadas puede ser prohibitiva. Sin embargo, sería MDScan útil como un detector de primer nivel, y puede ser prorrogado para descargar el análisis de los archivos PDF que usan sin apoyo Llamadas a la API de un sistema de análisis como son Wepawet o CWSandbox. En la actualidad, MDScan sólo detecta archivos PDF maliciosos que muestran vulnerabilidad en el visor de PDF.

6.6.1.3.3.3. VIRUS TOTAL

SITIO WEB (Internet: 01/08/2010, 15/01/2012, 22:45)

Concepto

Es un servicio en internet en el cual podemos analizar archivos y URLs para saber si se encuentran o no infectados por código malicioso, facilitando de esta manera una

rápida detección de virus, troyanos, entre otros tipos de código malicioso. Además de ser reconocido como uno de los mejores en la categoría Sitios Web Seguros.

Características

• Libre, servicio Independiente.
• Corre múltiples archivos.
• Actualizaciones automáticas en tiempo real.
• Resultados detallados de cada motor antivirus.
• Corre múltiples sitios web.

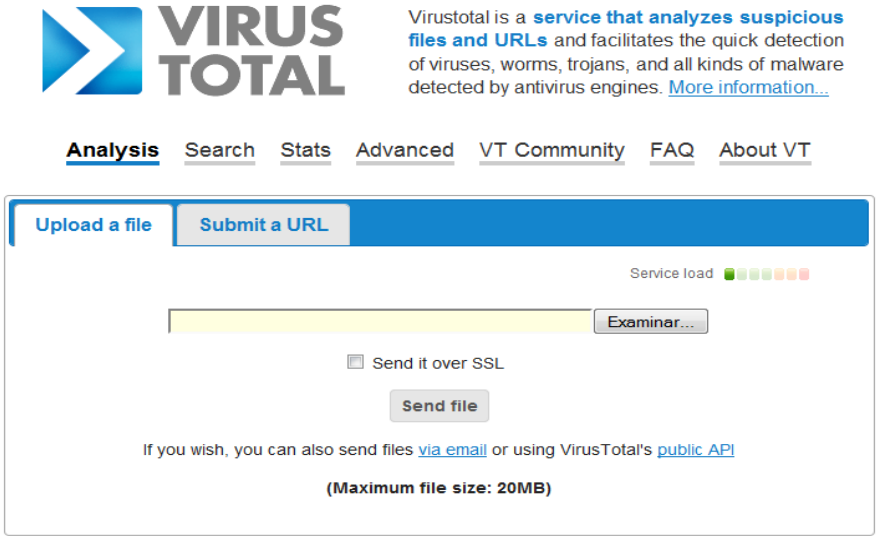


Figura 6. 5: Interfaz Servicio Virus Total

Opciones del Servicio Virus Total.

Análisis

En esta sección los usuarios pueden examinar archivos y URLs para la detección de código malicioso, únicamente subiendo el archivo o ingresando el URL y enviándolo a analizar.

Search

A pesar de ser la interfaz algo diferente aquí también se puede detectar código malicioso que se encuentran en las URLs.

States

Muestra la información de forma estadística y a su vez resumida, además de brindar información a los usuarios sobre la cantidad de documentos que se reciben, la forma en que son analizados, etc.

Advanced

Le permite enviar archivos vía email y recibir el resultado del escaneo en su cuenta de correo. El archivo es subido como un ataque de correo y el resultado puede ser recibido como un texto plano o XML. Los archivos enviados vía email tienen un periodo menor, por lo q el resultado del escaneo no siempre puede ser regresado inmediatamente.

¿Cómo empezar el proceso de escaneo vía email?

Los requerimientos son simples, usted solo necesita una cuenta de email valido y el archivo el cual se desee analizar.

Los pasos a seguir son los siguientes:

- Crear un nuevo mensaje con scan@virustotal.com como la dirección destino.
- Si usted desea revisar el resultado como texto plano, escribir SCAN en el archivo subject. Si desea recibir un XML adjunto con el resultado, escribir SCAN + XML en el subject file.
- Adjuntar el archivo que va ser escaneado. El archivo no debe exceder de los 20 MB en tamaño. Si el archivo adjuntado es largo, el sistema lo rechazara automáticamente.

4.3.5. VT Community

Muestra la información de la comunidad Virus Total, los últimos comentarios, los últimos miembros, los usuarios más activos, archivos mas recibidos, entre muchas cosas más.

6.6.1.3.3.4. SOPHOS ANTI-VIRUS

SOPHOS (Internet: 1997-2013, 04/01/2012, 20:23)

Sophos tiene una nueva función diseñada especialmente para ofrecer una mejor resolución Java Script, la cual tiene la capacidad de acortar y analizar JavaScript, emulación de Javascript el cual ofrece un mecanismo genérico para simplificar los contenidos del código, permitiendo al motor ver la carga útil del código para la detección genérica proactiva.

La diferencia entre Sophos y los demás programas antivirus es que las actuales tecnologías para desempaquetar confían en el reconocimiento de camuflajes específicos y en la escritura del código para manejar cada uno. Pero en la actualidad, este enfoque no progresa al mismo ritmo que el volumen de programas maliciosos. Los códigos pueden camuflarse, prácticamente, de infinitas maneras, y sabemos que los atacantes modifican sus técnicas con frecuencia. Se requiere una solución genérica para descubrirlos. Esto es lo que ofrece la emulación de JavaScript.

Con Sophos aumentará las tasas de detección de documentos PDF y contenido de código malicioso y se incrementara la protección proactiva contra nuevos ataques.

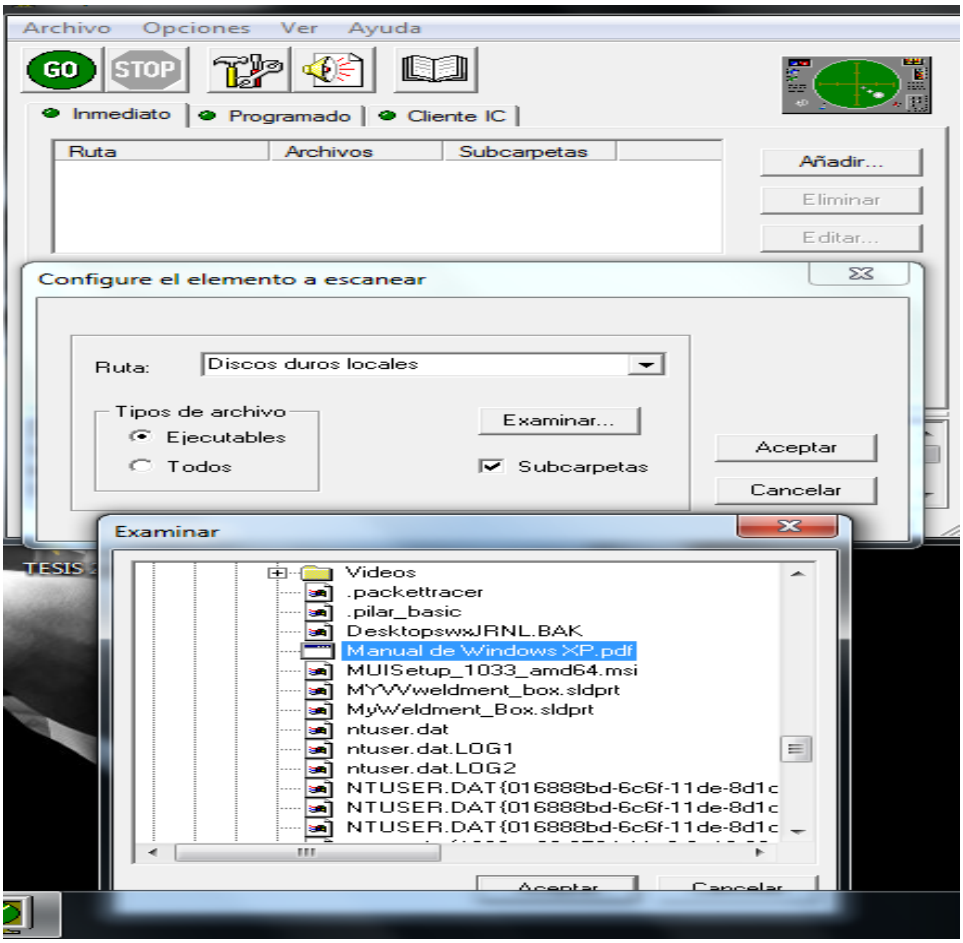


Figura 6. 6: Interfaz de Sophos Antivirus

Como se muestra en la figura 6. 6 la interfaz de Sophos Antivirus no es complicada, lo que se hace es: seleccionar lo que deseo escanear ya sea una unidad de disco, una flash memory, un directorio o carpeta y además existen las opciones de escanear los formatos de archivos que yo desee, como: pdf, HTML, etc. Es decir cualquier archivo especifico antes de ser ejecutado. El archivo que he seleccionado es un manual de formato pdf con el cual se realizará la prueba.

Si nos fijamos en la parte superior tenemos tres pestañas que son: Inmediato, Programado, y Cliente IC.

- En la primera pestaña es en la cual seleccionamos lo que se va escanear, recuerden que lo que se selecciono fue un archivo de formato PDF y para empezar el escaneo nos vamos a la opción archivo, escáner.

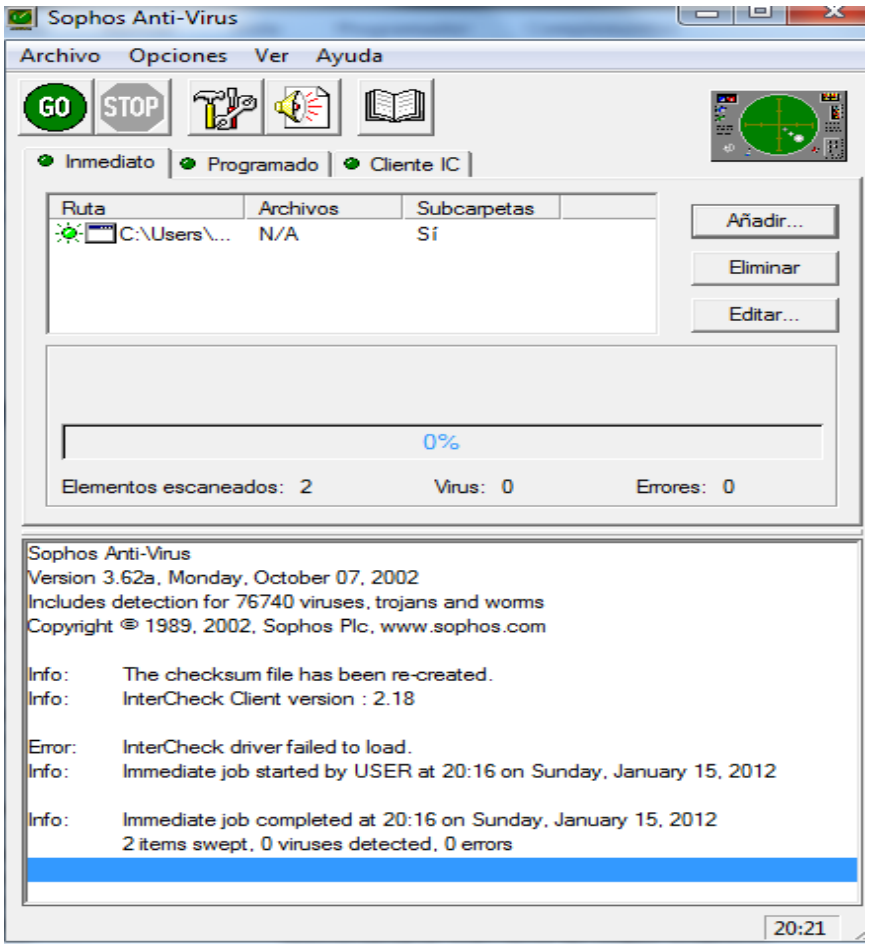


Figura 6. 7: Resultado del escaneo del archivo PDF

Si se observa en la figura podemos darnos cuenta que nos muestra la fecha y hora del escaneo en el que empezó y la fecha y hora en que finalizó, además de la cantidad de virus detectado y si existió algún tipo de error durante el proceso o no.

El resultado que se obtuvo fue que el archivo está libre de malware y el tiempo de demora fue de segundos.

- En la segunda pestaña opción Programado se puede añadir una tarea al software antivirus, en nuestro caso se llamará prueba y al hacer clic en aceptar aparecerá una nueva ventana en la cual podemos ver la lista de archivos

seleccionados anteriormente, si se desea se puede añadir más archivos, en la opción día/hora especificaremos que días queremos que se ejecute la tarea y la hora en la cual se realizara.

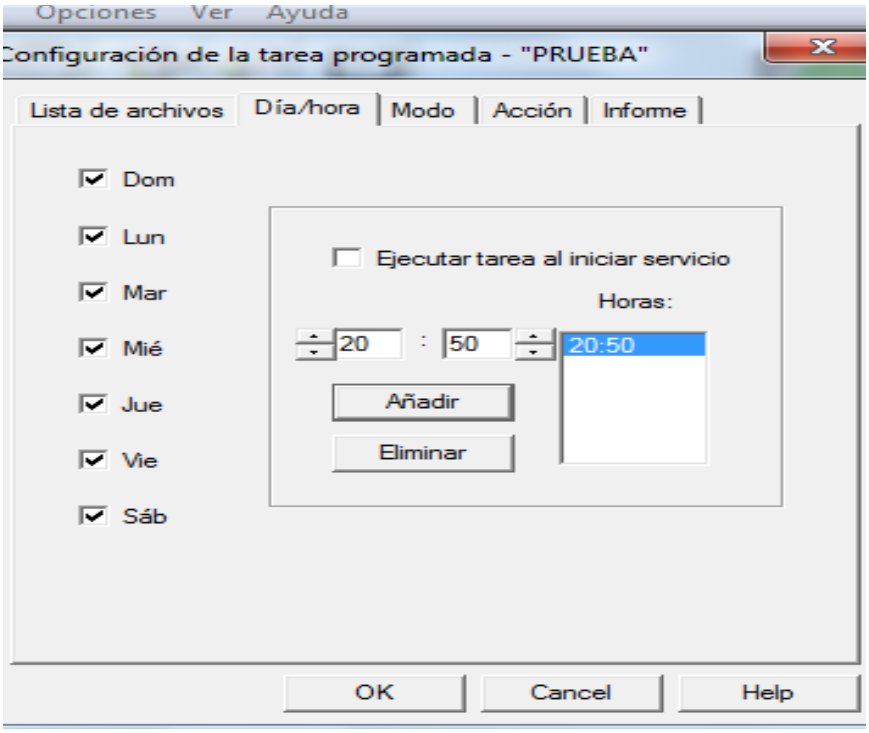


Figura 6. 8: Selección de la ejecución de la tarea.

La tarea PRUEBA se ejecutara todos los días a las 8:50. Se puede añadir un sinfín de tareas y determinarlas en diferentes horas, con eso se lograra mantener el equipo libre de malware y no tendrá que preocuparse por ejecutar el software cada día o cada hora, ya que tendrá la seguridad que las tareas se realizarán automáticamente.

Cabe mencionar que la versión de sophos utilizada es únicamente para el cliente, en caso de que se desee realizar para una empresa se debería instalar Sophos Endpoint Security, para lo cual se necesitaría un servidor como server 2003, server 2008, etc. Este programa se incorporará al servidor y se instalará como un servicio más del sistema operativo, por lo mismo la configuración será más complicado pero a la vez mejor y seguro, además que nos proporcionara un sinfín de opciones para su correcta utilización.

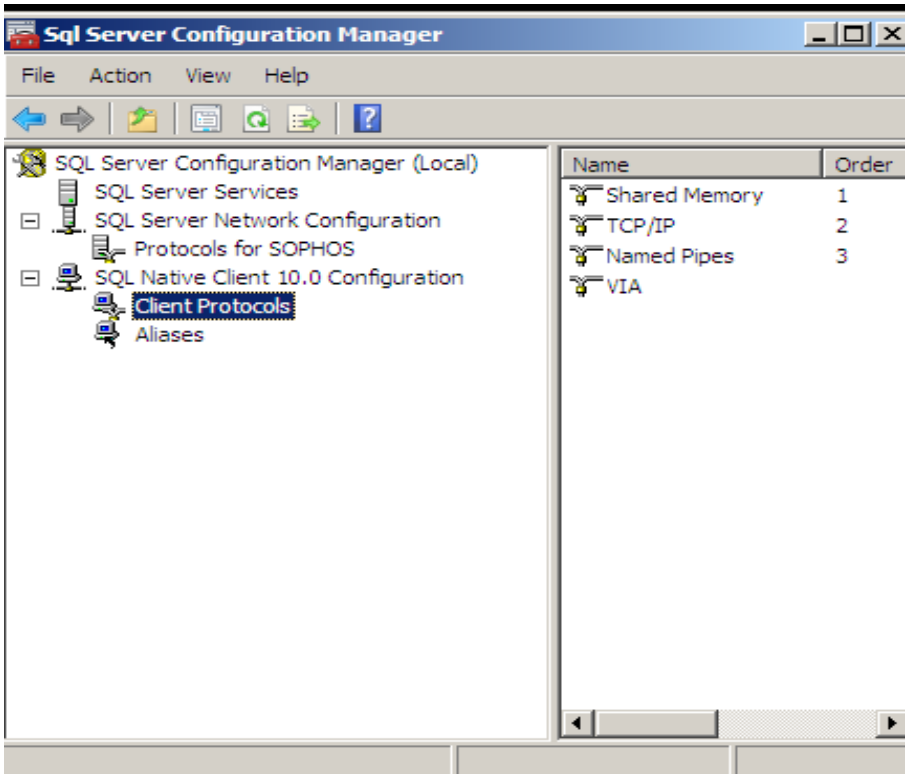


Figura 6. 9: Sql server para Sophos Endpoint Secirity.

Este programa se instalará junto con los demás componentes de Sophos Endpont Security, aquí se creará la base de datos para el manejo del Software Antimalware.

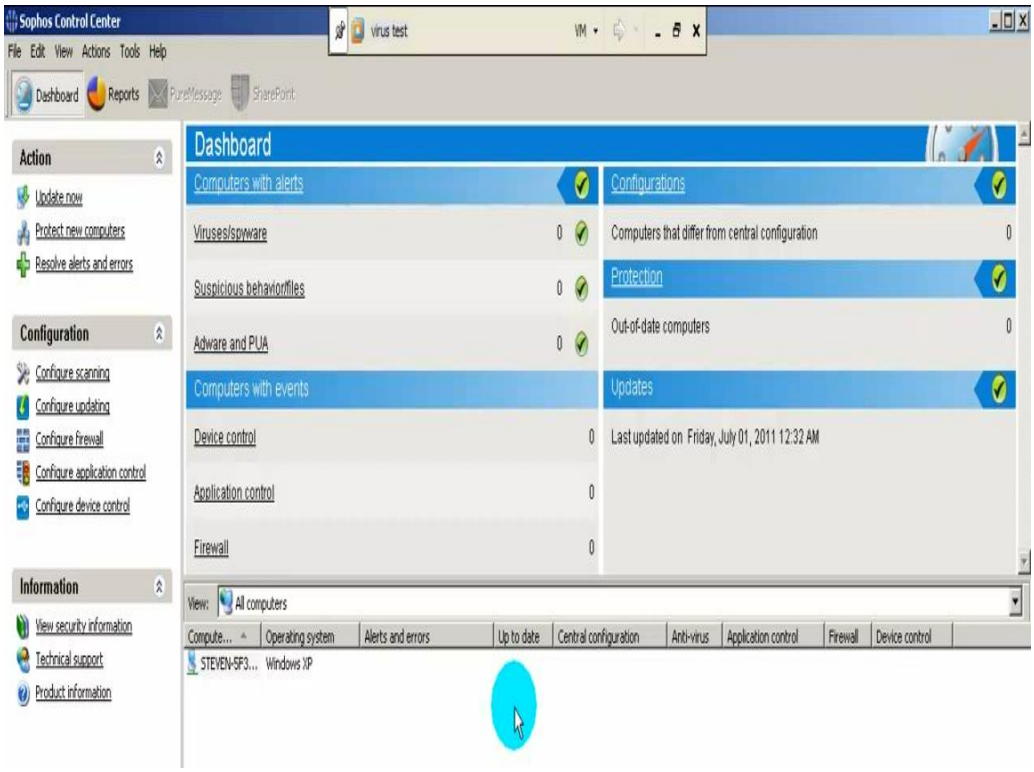


Figura 6. 10: Sophos Control Center

Para ver cómo funciona Sophos como servidor se lo instalo en Windows server 2008, para su descarga se tuvo que ir a la página oficial en la cual nos permite descargarnos una versión trial la cual tiene una vigencia de 30 días en los cuales puede ser utilizada normalmente y realizar las pruebas respectivas para conocer su funcionamiento y saber si en verdad conviene comprar la licencia o no. Al momento de descargarse le pedirá el correo y nombre y apellido, esto será necesario ya que nos dará además un usuario y una contraseña las cuales serán vitales en el momento de que ya esté instalado. Para la instalación anteriormente se deberá crear un usuario en el servidor ya que en la instalación le pedirá usuario y contraseña, el proceso para la instalación no es tan complicada simplemente se debe seleccionar muy bien lo que se va instalar y leer bien los requerimientos.

Al terminar la instalación pedirá el usuario y la contraseña que dan en el momento de descargarse el programa así que se debe guardar muy bien. Debido al tiempo y a la falta de conocimientos no se pudo realizar pruebas luego de la instalación de esta

versión de Sophos, pero cabe recalcar q al igual que la versión del cliente es sumamente eficiente y nos proporciona mucha más seguridad en comparación a otros programas antivirus que son creados para detectar únicamente ciertos virus y que al aparecer una nueva versión de virus no podría ser detectada, en cambio con Sophos esto no sucederá puesto que al ser genérico al igual que el malware, ira evolucionando y será capaz de detectar nuevas amenazas, obviamente tiene sus pos y sus contras pero es más recomendable que los demás.

Sophos Endpont Security es una versión reciente y no todo el mundo tiene conocimientos sobre su existencia, así que antes de aceptarlo o rechazarlo se debería investigar un poco más sobre su funcionamiento y sus pos y contras, pero algo adicional que quiero mencionar es que Sophos Endpont Security escanea en busca de virus, programas espía y programas publicitarios además de que es útil para el escaneo de equipos proporcionando ventajas como: fácil instalación sin necesidad de desinstalar los antivirus existentes y para el escaneo de redes implementando paquetes MSI y Active Directory, brindando informes completos además de que ejecuta y protege a Internet Explorer para que no procese los programas maliciosos en las solicitudes.

PROPUESTA, cumplimiento del tercer objetivo específico.

Después de conocer el funcionamiento de algunos tipos de software antivirus, se concluyó que la mejor opción es el servicio de internet Virus Total, ya que al mandar analizar un documento PDF malicioso o que contenga código javascript, muestra un análisis detallado en la cual indica que el documento fue analizado por varios software antivirus.

CUMPLIMIENTO DEL PRIMER OBJETIVO ESPECÍFICO

Diagnosticar las técnicas de análisis heurístico de malware.

Una vez que se que se ha dado a conocer el funcionamiento de la heurística en los software antivirus, y se ha explicado algunos tipos y como funcionan en cuanto a la detección de documentos PDF maliciosos, los funcionarios de la Municipalidad de Ambato tendrán ideas mas claras sobre lo que se esta tratando de explicar y podrán

considerar la instalación de alguno de los software antivirus en sus computadores, por lo que se puede concluir que se ha cumplido con el primer Objetivo Especifico mencionado en el Capitulo I de esta tesis.

6.7. DETECCION DE DOCUMENTOS PDF MALICIOSOS

Para la detección de documentos PDF maliciosos, en primer lugar hay que conocer cómo funciona Adobe Acrobat, ya que con eso se podrá crear el documento pdf malicioso o a su vez un documento pdf que contenga código java script el cual realice alguna acción, el cual será posteriormente escaneado con alguno de los software antivirus anteriormente mencionados.

6.7.1. Adobe Acrobat

FERRI-BENEDETTI, Fabrizio (Internet: 03/02/2011, 03/01/2012, 20:45)

Todo el mundo conoce Acrobat Reader, que es el lector de archivos PDF de Adobe pero lo que deben saber es que también existe un programa el cual permite modificar o crear un archivo pdf a partir de otros documento. Este programa se llama Adobe Acrobat x Pro que es el editor de PDF mas completo, el cual se destaca por su impresora virtual, un accesorio con el cual se podrá crear un PDF desde cualquier programa capaz de imprimir, y también genera un PDF a partir de lo que se escanee. Además permite modificar el texto, insertar comentarios y figuras, marcar objetos para su revisión, incrustar vídeos y proteger el PDF con firmas, certificados digitales y contraseñas que impidan la impresión o la edición del contenido.

Cambios recientes:

- Integración con Office 2010
- Personalización de carteras PDF
- Digitalización mejorada
- Herramientas rápidas
- Interfaz renovada

Adobe Acrobat X Pro soporta los siguientes formatos

PDF, EPS, HTML, JPG, JPF, DOC, XLS, PNG, PS, RTF, TXT, TIFF, XML

Ventajas:

- Creación y edición PDF de alta calidad
- Sistemas de protección mediante cifrado
- Incrustación de vídeos FLV y H.264
- Diseño de formularios dinámicos
- Integración con Acrobat.com y Office

6.7.1.1. Introducción

En estos últimos años una gran cantidad de personas se ha interesado en la investigación PDF con la esperanza de encontrar mejores maneras de detectar archivos PDF maliciosos, ya que el Formato de Documento Portátil (PDF) es uno de los formatos de archivo más utilizados. Últimamente los atacantes se han centrado más en atacar por el lado del cliente que del servidor, esta es una de las razones por las cuales los documentos PDF es un vector principal de la distribución de malware. Un aspecto clave del Formato PDF desde el lado de los atacantes es la complejidad del lector de múltiples funciones de Adobe para Windows, probablemente el espectador que más ampliamente ha utilizado formato PDF ha llegado al descubrimiento de muchas de las vulnerabilidades explotables.

Los principales ataques empiezan en los sitios web y en las descargas de documentación, los archivos PDF maliciosos pueden ser distribuidos por diferentes formas incluyendo los mensajes atreves del correo electrónico.

En efecto, los documentos PDF maliciosos pueden ser considerados como el renacimiento de los virus de macro los cuales afectaron a Microsoft Office y otras empresas de productividad en la década de los 90 hasta principios de los 2000. En aquel tiempo uno de los factores que llevaron a la extinción de los virus de macro las medidas de seguridad adicionales y las protecciones que se están aplicando gradualmente a las nuevas versiones de las versiones afectadas. De este modo, X Reader, la versión reciente de Adobe Reader, viene con seguridad y características tales como la caja de arena y el aislamiento, lo que significativamente reduce el

riesgo de comprometer el sistema completo. La detección de las amenazas PDF se mantendrán como una cuestión importante, puesto que las aplicaciones antivirus no ofrecen cobertura de detección adecuada, incluso aun cuando las amenazas son conocidas en archivos PDF, mientras que el uso de sencillas técnicas de ofuscación puede disminuir la tasa de detección, e incluso más.

6.7.1.2. Antecedentes

El formato PDF desarrollado por Adobe System, se ha convertido en el formato de archivo más utilizado para la distribución e impresión de documentos. Un archivo que se adhiere a la especificación de PDF consta de 4 secciones principales: una línea de cabecera con el número de versión de la especificación PDF, el cuerpo principal del documento, el cual consiste en objetos como texto, imágenes, fuentes, etc. Una tabla de referencias cruzadas con las compensaciones de los objetos dentro de los archivos incrustados, una tabla de referencias cruzadas con las compensaciones de los objetos dentro del archivo, y por último , una forma para un rápido acceso a la tabla de referencias cruzadas y otros objetos especiales.

Además de los datos estáticos, los objetos PDF también pueden contener código escrito en JavaScript. Esto permite a los autores de los documentos incorporar características avanzadas tales como la validación de formularios, contenidos multimedia, o incluso la comunicación con sistemas y aplicaciones externas. Desafortunadamente, los atacantes también pueden tomar ventaja de la versatilidad que ofrece JavaScript para la explotación de vulnerabilidades de ejecución de código arbitrario en la aplicación de la visualización del archivo PDF. A través de JavaScript el atacante puede lograr dos objetivos fundamentales: desencadenar la vulnerabilidad del código de poder, y desviar la ejecución de código de su elección.

Dependiendo de la vulnerabilidad, lo primero es lograr la llamada la vulnerable función API o de otra manera la creación de las condiciones necesarias. Luego atreves de alguna técnica de manipulación de memoria, el flujo de control se transfiere al código Shell incorporado, que lleva a cabo el paso final del ataque, por ejemplo, el vertido en el disco y luego lanzando un código ejecutable malicioso incrustado.

Además de explotar alguna vulnerabilidad en el visor de PDF, los atacantes han aprovechado las características avanzadas de PDF como el /Lanzamiento de opción, que se inicia automáticamente un incrustado ejecutable, o el URI/ y / Ir a las opciones, lo cual puede abrir los recursos externos constituidos en la misma máquina o en Internet, Aunque en ambos casos la primera aplicación para el usuario pide autorización, tales características son muy peligrosas y después de la exposición pública de sus implicaciones de seguridad que se mitigan rápidamente.

PROPUESTA, cumplimiento del primer Objetivo Específico

A través de la investigación se ha podido tener una idea clara sobre la introducción de virus en los documentos PDF maliciosos para lo cual se busco antecedentes sobre caso similares que ya fueron explicados en el literal 6.7.1.1 Introducción y 6.7.1.2 Antecedentes.

6.7.1.3. Funcionamiento

La aplicación adobe en su versión x pro, es una versión adobe mejorada considerablemente, en lo que es la manipulación y creación de los documentos en formato PDF. En esta versión se puede a partir de un documento creado en cualquier otro tipo de aplicación como Word, Excel, etc. Abrirlo y personalizarlo, además se puede añadir elementos de formulario, se puede combinar diferentes archivos para generar un solo documento PDF, se puede insertar elemento adicionales, también se puede añadir acciones para crear formularios de manera que desde esa versión se pueda optimizar el funcionamiento de los documentos PDF y se podrá mejorar considerablemente la calidad de los documentos PDF, así como su portabilidad.

Una vez que se ha ingresado adobe x pro nos muestra esta pantalla:

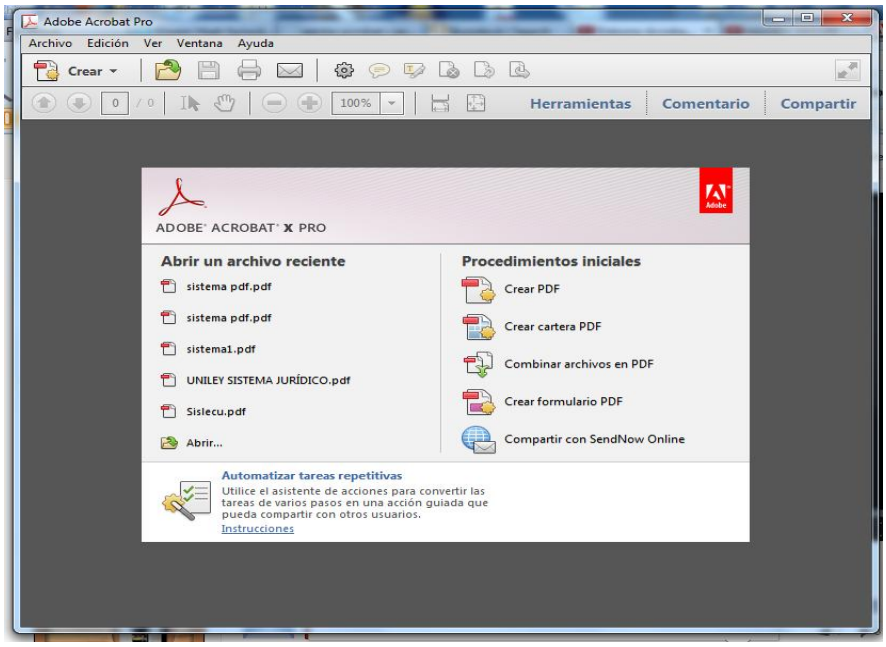


Figura 6. 11: Adobe Acrobat Pro (Ventana de inicio)

Aquí encontramos la opción procedimientos iniciales en donde nosotros podemos crea un PDF, una cartera de PDF, combinar varios archivos en un solo PDF, crear formularios es decir los documentos que podamos usar para que los usuarios lo llenen con lo que necesiten y finalmente tenemos la opción en la cual se puede compartir mediante las aplicaciones de adobe el documento que se va a crear.

La opción que vamos a escoger es Crear formulario PDF, ya que con la creación de formularios nos aparecerán las opciones que nos van a permitirán incrustar código javascript en el documento.

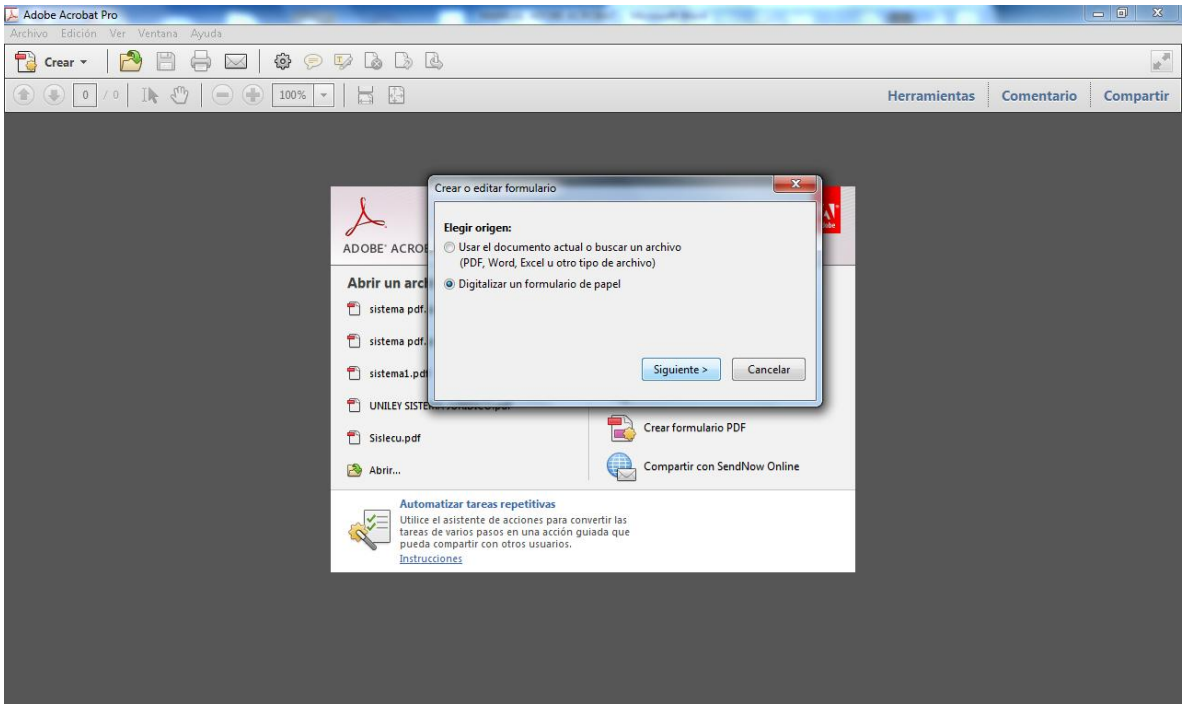


Figura 6. 12: Ventana de origen para la creación del Formulario

A continuación nos aparece una ventana con dos opciones:

La primera opción: nos permite partir de un documento creado anterior mente en formatos como PDF, Word, Excel u otro tipo de archivo, o a su vez nos permitirá partir de un documento en blanco.

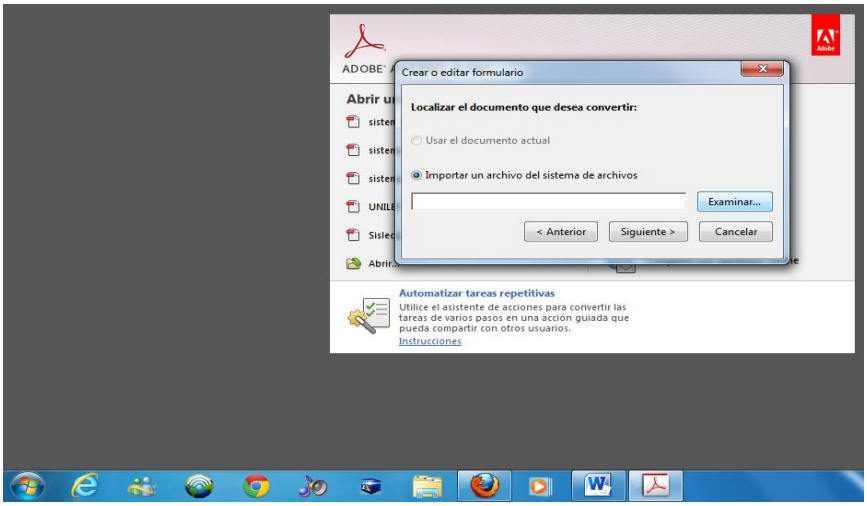


Figura 6. 13: Selección del Documento para convertirlo en PDF.

La segunda opción: también es de gran utilidad ya que nos permite hacer algún tipo de cambios a los documentos impresos, es decir podemos personalizarlos.

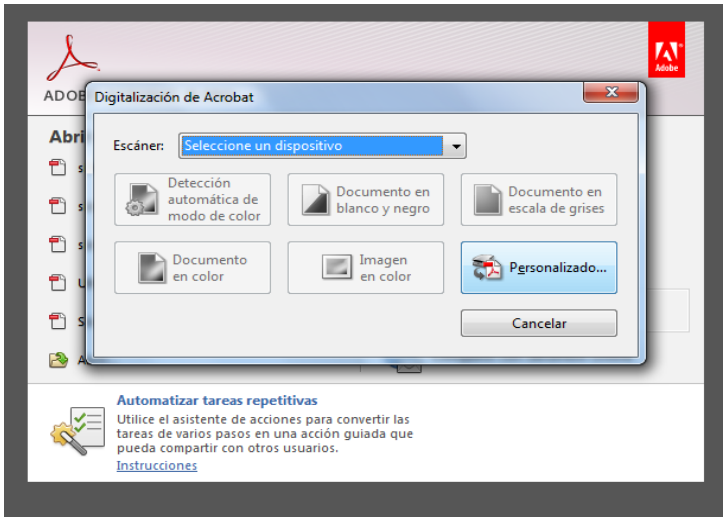


Figura 6. 14: Escaneo de un documento.

En la digitalización personalizada encontramos varias opciones básicas para la entrada del documento que va ha ser utilizado para la incrustación de formularios, como se muestra en la siguiente figura.

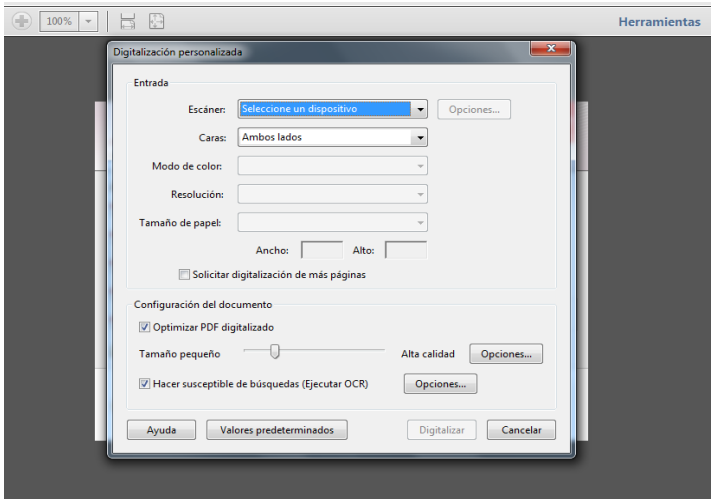


Figura 6. 15: Opciones del Documento escaneado.

Podemos observar que muchas de las opciones no se encuentran habilitadas lo cual se debe a que no contamos con un escáner para realizar la entrada del documento digitalizado.

Por facilidad se escogió la primera opción ya que se va a partir de un documento Word en blanco creado con anterioridad llamado prueba.

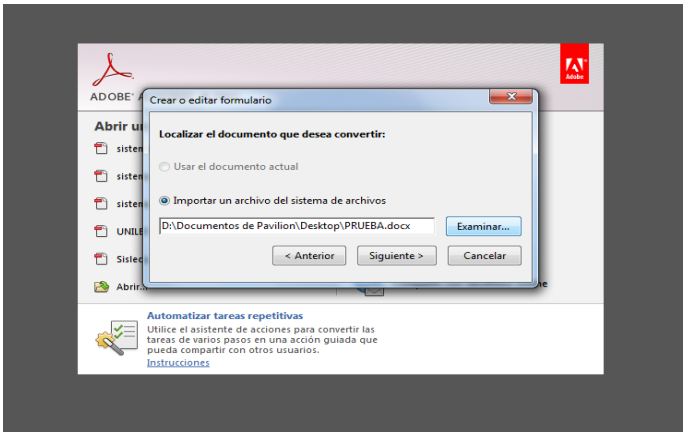


Figura 6. 16: Selección de un Documento creado.

Se escogio la opcion siguiente en donde se puede observar como el documento procede a ser cargado con un nuevo formato que es el de PDF.

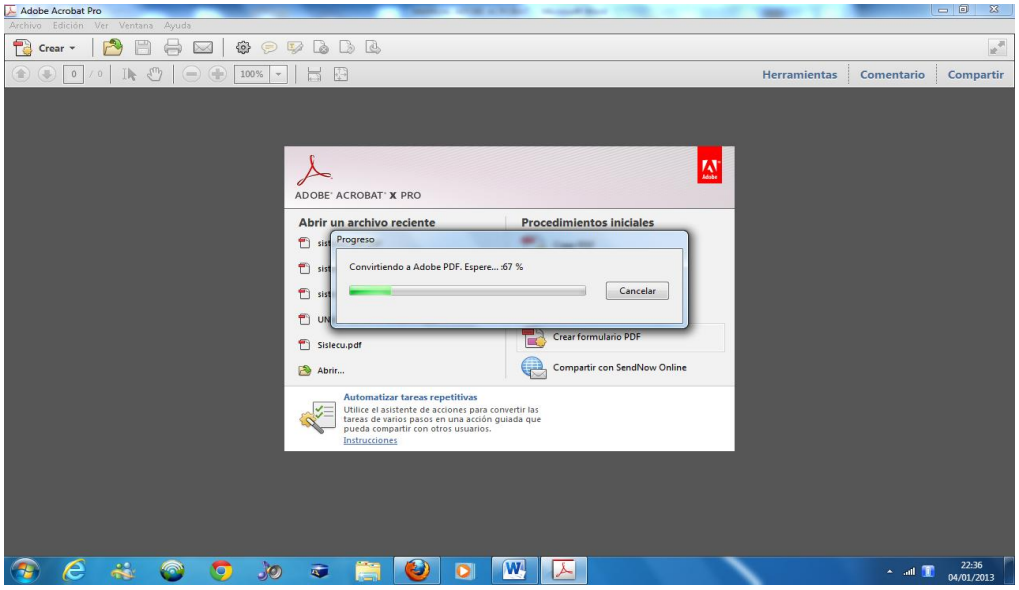


Figura 6. 17: El Documento seleccionado está siendo convertido en formato PDF.

A continuación se visualizó la siguiente pantalla:

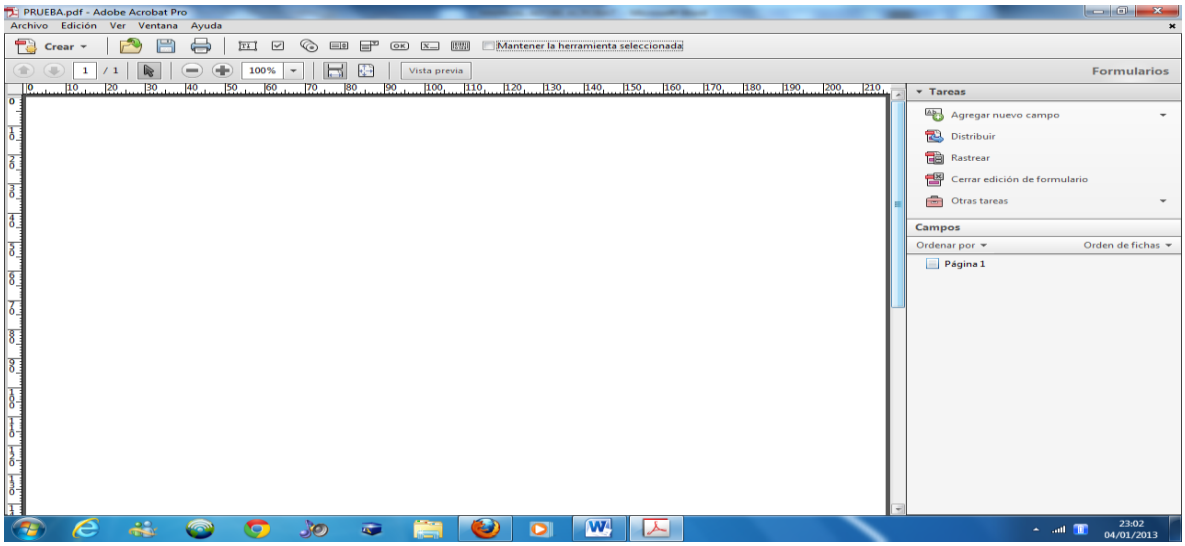


Figura 6. 18: Documento convertido en formulario..

Aquí encontramos todas las tareas que nos permiten crear formularios en los cuales se pude incrustar código JavaScript como son:

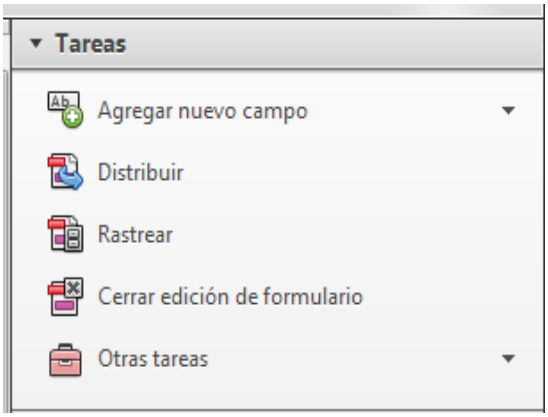


Figura 6. 19: Opciones de las tareas del Formulario.

Una vez que se decidida el tipo de información que desea recibir de los usuarios, hay que empezar asignar los elementos de formulario adecuados dependiendo de los distintos tipos de información.

- Si el usuario va a escribir datos de texto y datos numéricos, se diseña el formulario para utilizar campos de texto o cuadros de lista desplegable.

- Para ofrecer una sola elección entre varias opciones, puede usar botones de radio, un cuadro de lista o una lista desplegable.
- Para ofrecer un número limitado de opciones de las cuales el usuario puede seleccionar ninguna, una o varias, sería conveniente usar casillas de verificación, o a su vez un cuadro de lista en las cuales se pude definir sus propiedades de campo para que permita múltiples selecciones.
- Para acciones, como abrir un archivo, reproducir un sonido o un video, enviar datos del formulario, etc., se usan botones.
- Para aumentar la seguridad, existe un campo de firma digital que verifica la identidad del usuario.

También puede adaptar las propiedades de campos de formulario individuales para facilitar aún más la cumplimentación del formulario PDF.

- Agregar nuevo campo

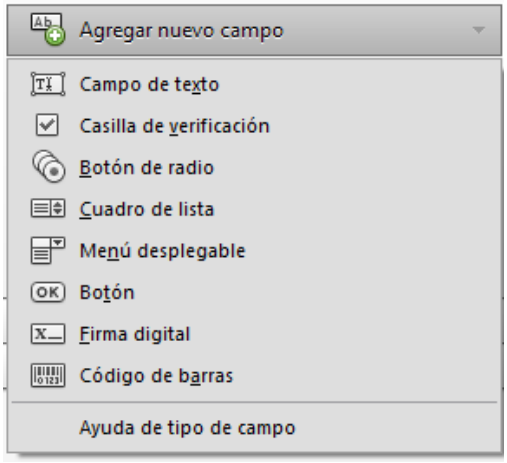


Figura 6. 20: Lista de los campos necesarios para crear el formulario.

✓ **Campo de texto**

Permiten que el usuario escriba texto (nombre, dirección, número de teléfono, etc.).

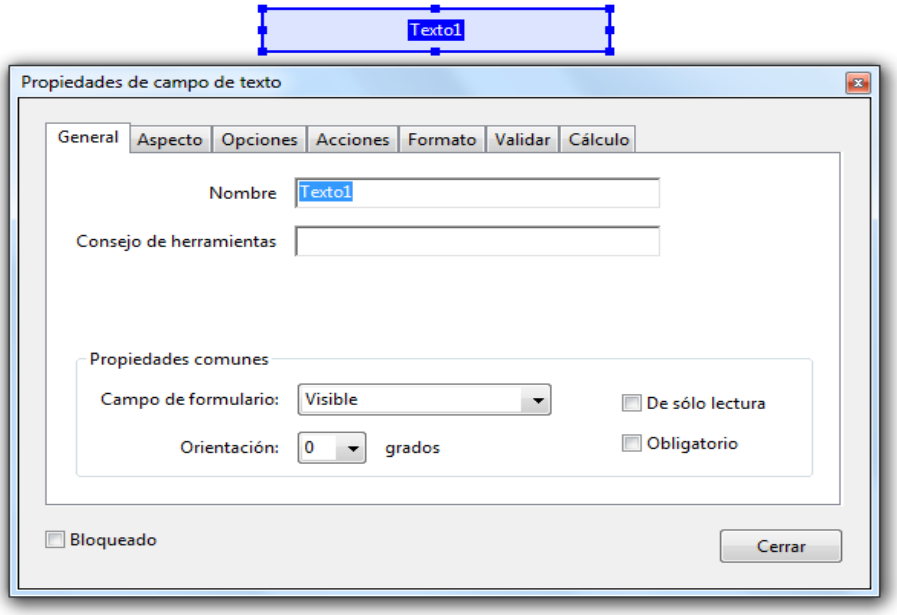


Figura 6. 21: Pestaña General de las Propiedades de campo de texto.

Al colocar el campo de texto en el formulario vamos a encontrar la opción de propiedades, en las cuales tenemos las siguientes pestañas: General, Aspecto, Opciones, Acciones, Formato, Validar, Calculo. En la pestaña general se puede agregar el nombre del campo, si quiere que sea visible o no al momento de utilizar el formulario, su orientación y si el campo es requerido o no.

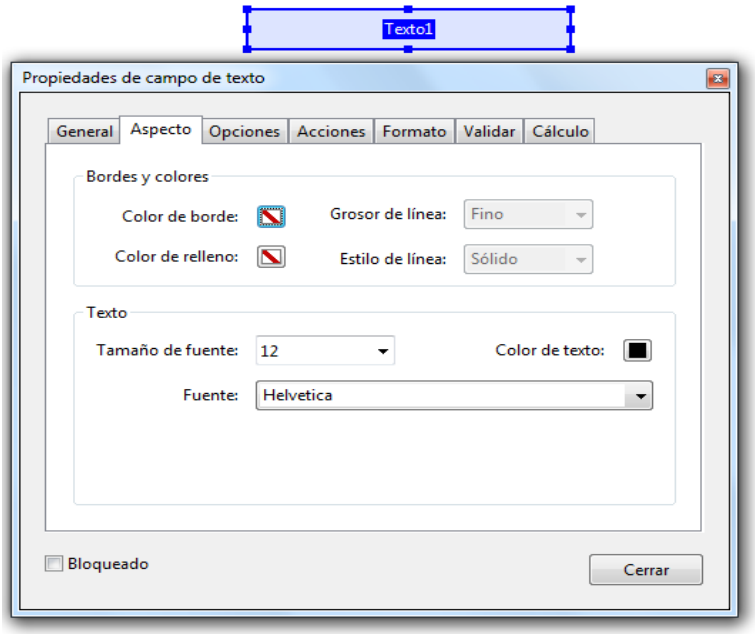


Figura 6. 22: Pestaña Aspecto de las Propiedades de campo de texto.

En la pestaña de Aspecto escogemos el color de borde, relleno, el grosor de la línea, el estilo y tamaño de fuente, además del color de texto y la fuente.

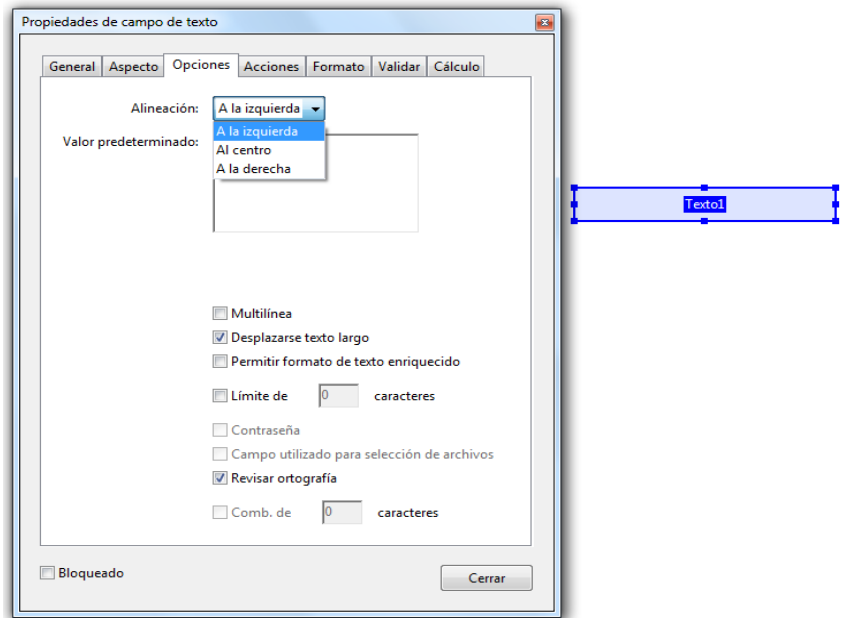


Figura 6. 23: Pestaña Opciones de las Propiedades de campo de texto.

En la pestaña de Opciones tenemos las opciones de alineación, Izquierda, Centro, Derecha, también existe una casilla en caso de que se necesite colocar un valor predeterminado o también podemos especificar el límite de caracteres que necesitemos.

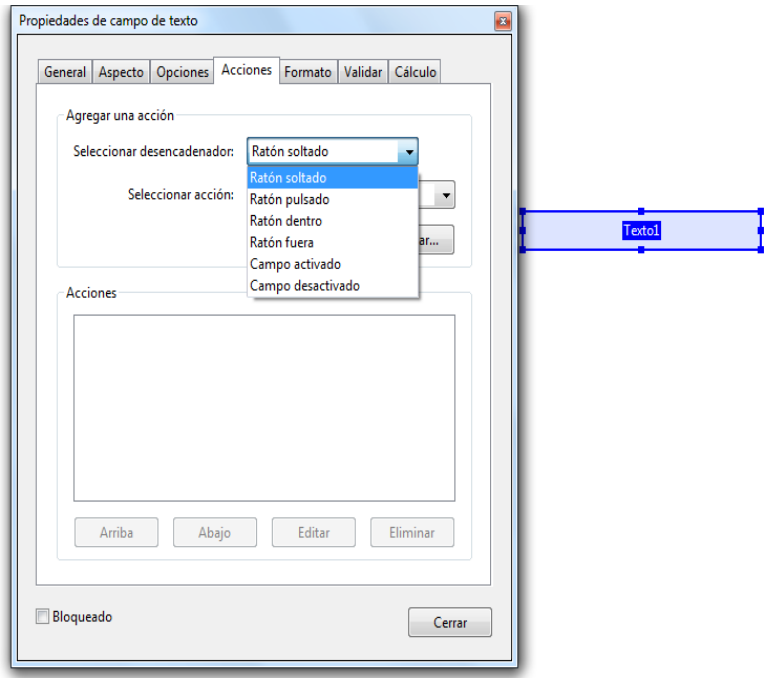


Figura 6. 24: Pestaña Acciones de las Propiedades de campo de texto.

En la pestaña de Acciones tenemos algunas opciones para el campo de texto, es decir nosotros podemos crear algún tipo de código cuando se ejecute alguna opción como por ejemplo al pulsar el ratón, al activar o desactivar el campo, etc. Al escoger cualquier acción de campo, en la parte inferior tenemos un cuadro en el cual se puede incrustar código JavaScript que realice algún tipo de acción, lo cual es muy útil dependiendo de la utilización posterior del formulario que se está creando.

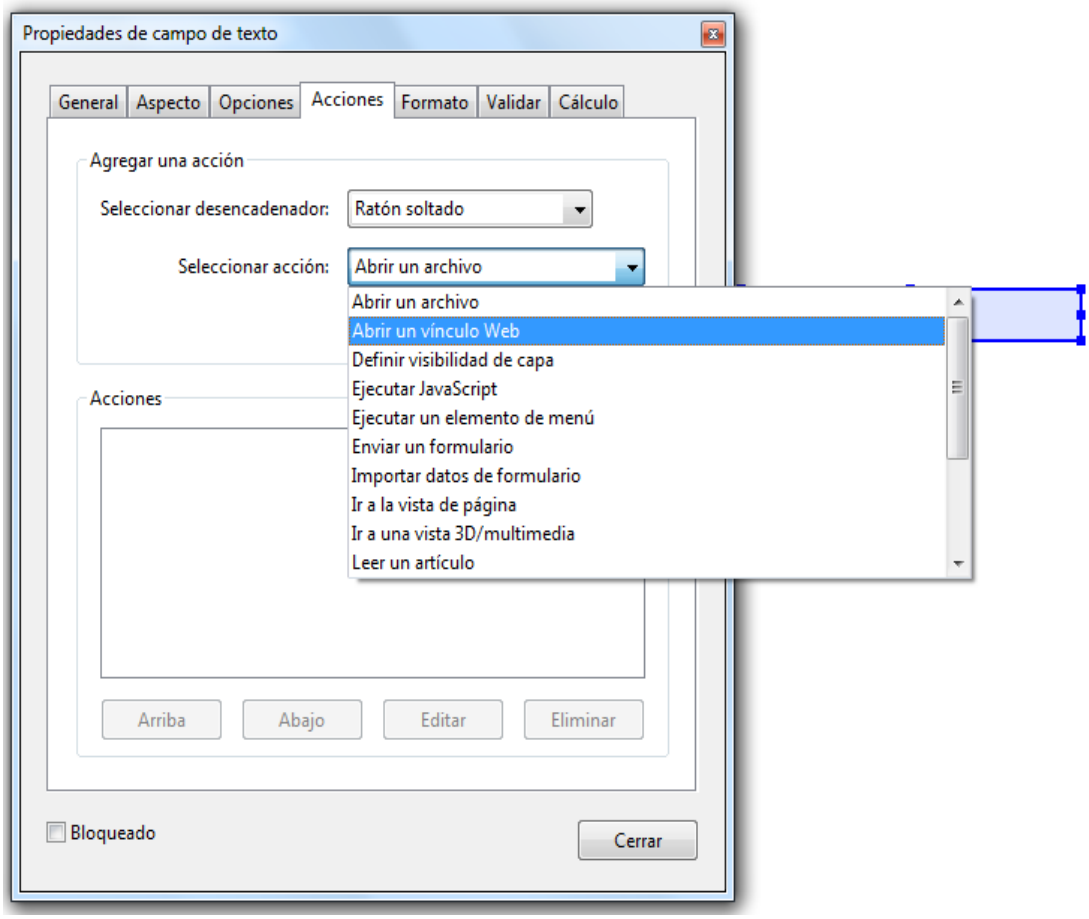


Figura 6. 25: Lista de Acciones de las Propiedades de campo de texto.

Como podemos ver en la opción Seleccionar acción se encuentra una lista desplegable con importantes opciones como: Abrir un vínculo Web, Ejecutar JavaScript, Importar datos de formulario etc. Lo que hay que destacar aquí es la opción de Ejecutar JavaScript ya que si bien es cierto es una ventaja cuando se desea realizar algún tipo de programación pero también es una puerta abierta aquellas personas que desean realizar algún tipo de daño a la información que se pueda obtener o a su vez algún tipo de daño al computador.

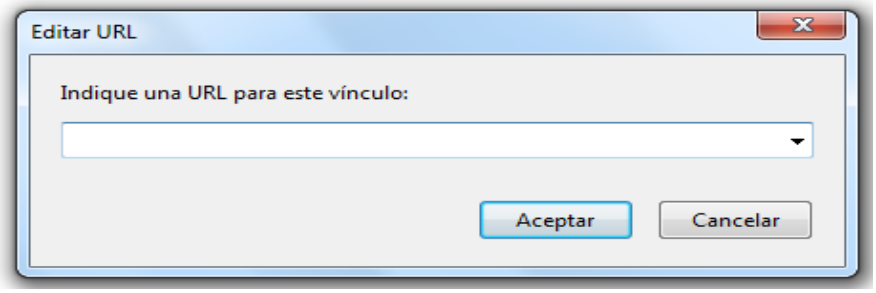
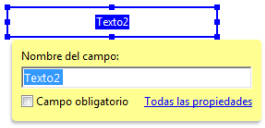


Figura 6. 26: Ventana para ingresar una dirección al hacer clic.

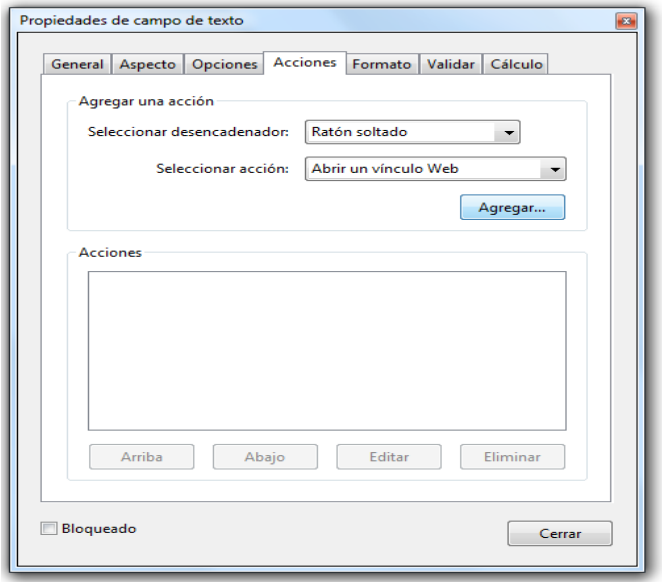
Abrir un vínculo Web es otra opción que se debe considerar porque dependiendo de la acción que se realice podemos introducir una URL.

A continuación se les va a realizar una pequeña prueba para que tenga una mejor idea sobre cómo puede ser utilizada esta opción.

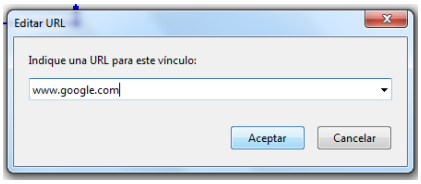
1. Colocamos un Campo de texto en el formulario y escogemos la opción todas las propiedades.



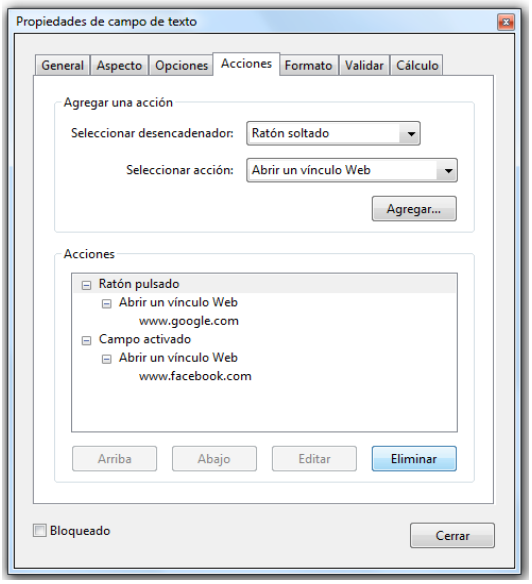
2. Ahora vamos a la pestaña Acciones y seleccionamos la opción Abrir un Vínculo Web y a continuación presionamos agregar



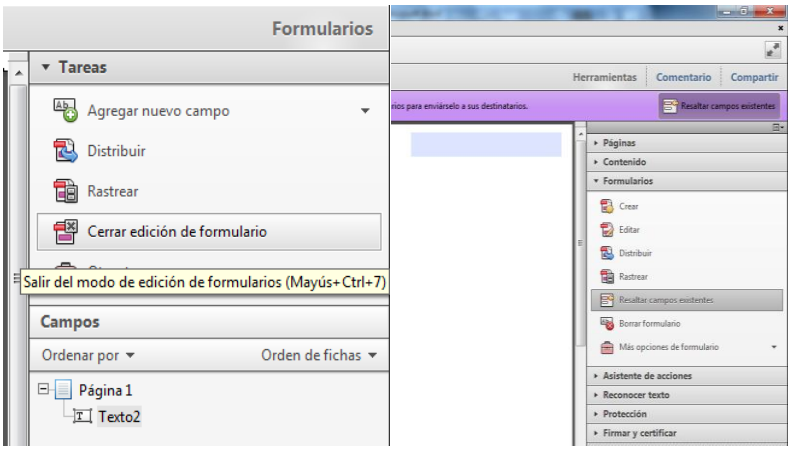
3. A continuación se visualizara la siguiente figura en la cual asignaremos una dirección Web que en mi caso es www.google.com y presionamos aceptar.



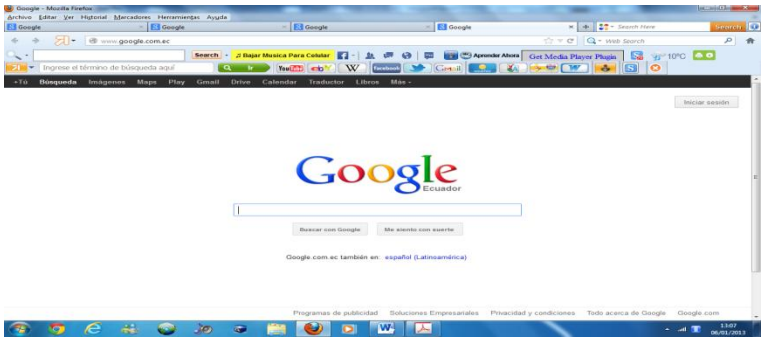
4. Ahora voy a explicar lo que se hizo, lo que va a pasar es que en el momento en el que pulse el ratón en el campo de texto el navegador se va activar y se abrirá la página escrita anteriormente que en este caso es www.google.com . Como podemos ver en la parte inferior se puede asignar más de una opción dependiendo del tipo de acción, y en caso de requerirlo la acción puede ser modificada o eliminada.



5. Cerramos la ventana y ejecutamos el formulario escogiendo la opción cerrar edición de formulario y nos mostrara una pantalla con lo que ah echo, y como podemos ver nos aparece el cuadro de texto de color celeste, ahora hacemos clic sobre el cuadro de texto y vemos como se abre el navegador con la pagina especificada.



6. Recordemos que la página se abrirá dependiendo de cuantas veces se haga clic en el cuadro de texto.



En la pestaña Formato seleccionamos el tipo de formato que deseamos darle al campo de texto el cual depende del tipo de dato que vamos a ingresar.

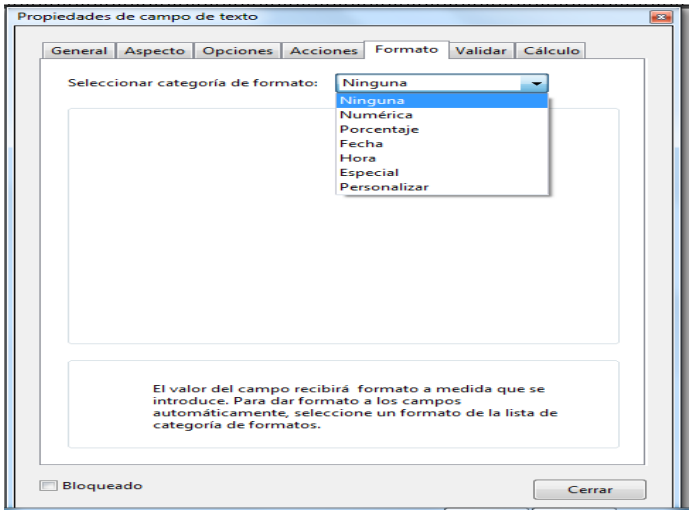


Figura 6. 27: Pestaña Formato de las Propiedades de campo de texto.

Mediante la pestaña de Valor se puede validar el campo de texto, podemos asignar el valor del intervalo del campo o a su vez se puede ejecutar una secuencia de comandos para una validación personalizada.

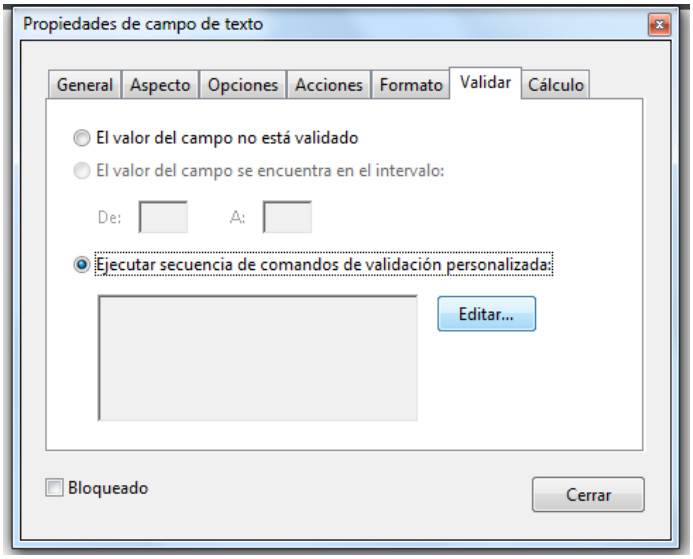


Figura 6. 28: Pestaña Validar de las Propiedades de campo de texto.

Para ejecutar la secuencia de comandos de validación personalizada, presionamos editar y nos mostrara una pantalla en la cual podemos programar la validación utilizando código JavaScript.

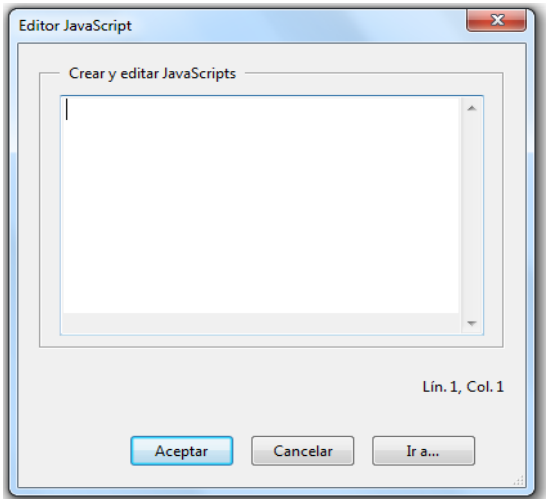


Figura 6. 29: Validación Personalizada utilizando código JavaScript.

La opción de Calculo permite obtener un valor calculado utilizando los valores de otros campos con los cuales se puede sumar, multiplicar, obtener el máximo, la media o el mínimo de estos campos que se han seleccionados. Aquí encontramos otras dos opciones que son: Anotación de campo y Secuencia de comandos de cálculo personalizados en los cuales se puede programar utilizando código JavaScript.

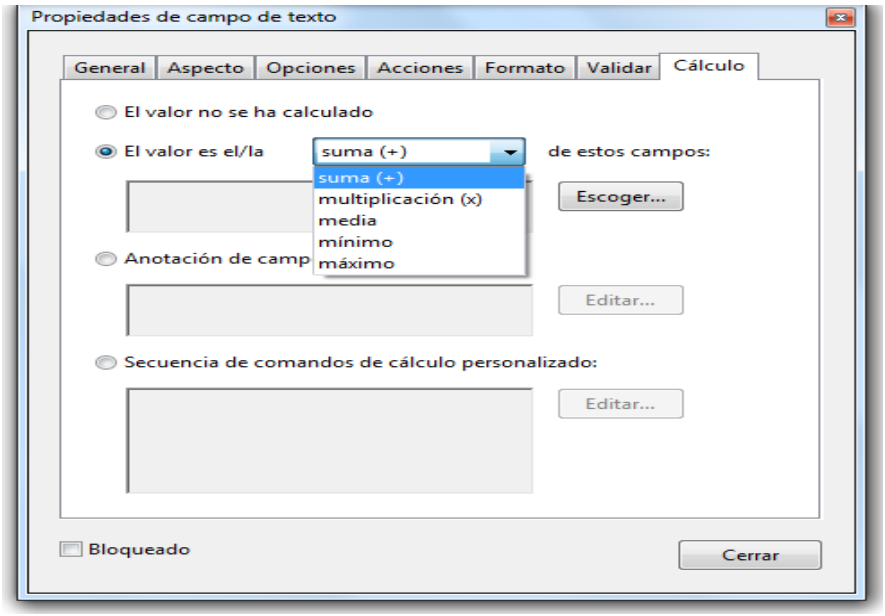


Figura 6. 30: Pestaña Cálculo de las Propiedades de campo de texto.

Al escoger cualquiera de las dos últimas opciones tenemos la opción de editar en la cual se puede crear y editar el JavaScript que se desea que sea ejecutado.

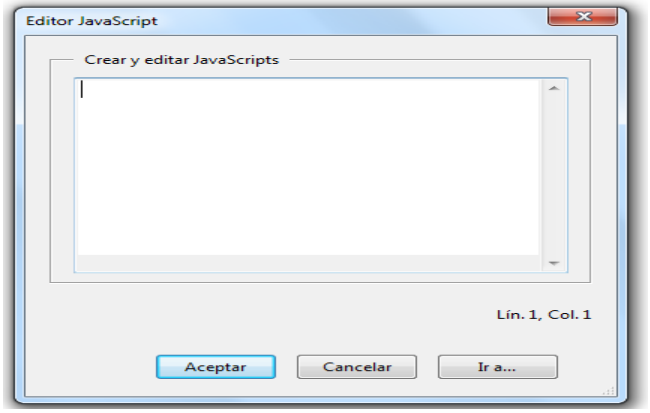


Figura 6. 31: Editor de JavaScript para un Cálculo personalizado.

✓ **Casilla de verificación**

Presentan opciones de sí o no para elementos individuales. Si el formulario contiene varias casillas de verificación, normalmente el usuario puede seleccionar tantas o tan pocas como desee.

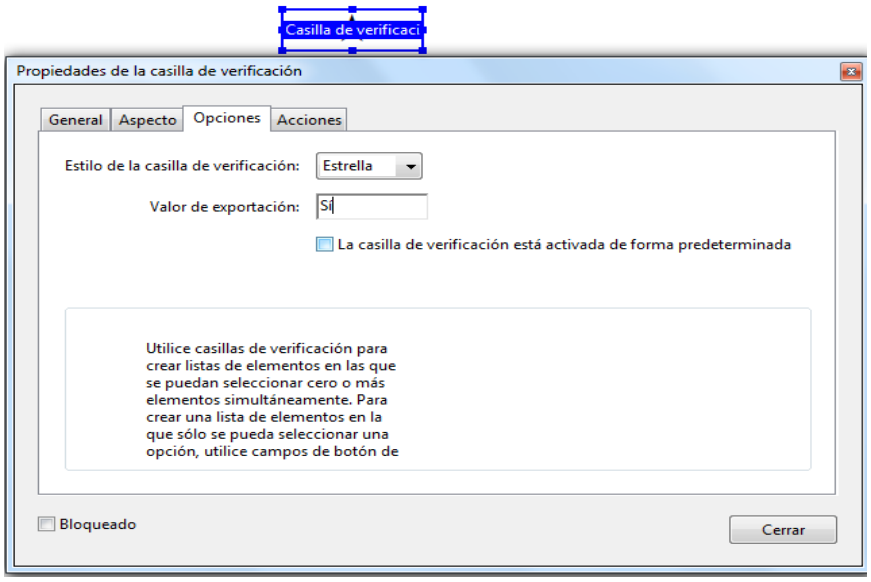


Figura 6. 32: Propiedades de la Casilla de Verificación.

Las propiedades de la casilla de verificación como General, Aspecto y Acciones son las mismas del Campo de texto por lo que no hay la necesidad de volver a explicarlos, la única pestaña diferente es la de Opciones en la que se puede escoger el estilo de la casilla de verificación y el valor de exportación.

✓ **Botón de radio**

Presentan un grupo de opciones, sólo una de las cuales se puede seleccionar. Todos los botones de radio con el mismo nombre funcionan como un grupo.

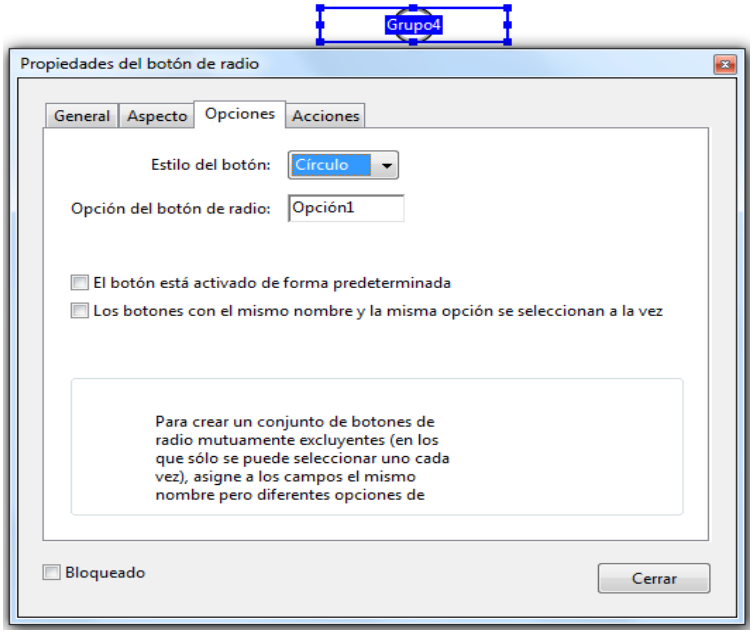


Figura 6. 33: Propiedades de la Casilla de Verificación.

El Botón de Radio también posee las mismas propiedades de la casilla de verificación con una pequeña diferencia como es el estilo del botón, las opciones del botón de radio y dos opciones para que el botón este activo de forma predeterminada la opción de que los botones con el mismo nombre y la misma opción de selecciones a la vez.

✓ **Cuadro de lista**

Muestra una lista de las opciones que el usuario puede seleccionar.

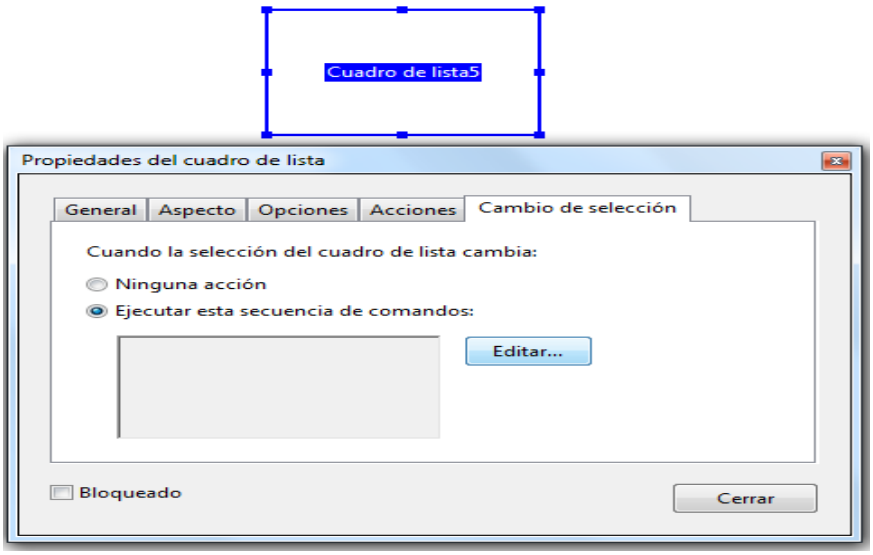


Figura 6. 34: Propiedades del Cuadro de listas.

Además de tener las mismas propiedades del radio botón posee una más llamada Cambio de selección, la cual permite ejecutar una secuencia de comandos editada por el usuario, para lo cual se utiliza la programación en JavaScript.

✓ **Menú desplegable**

Permiten al usuario elegir un elemento de un menú emergente o escribir un valor.

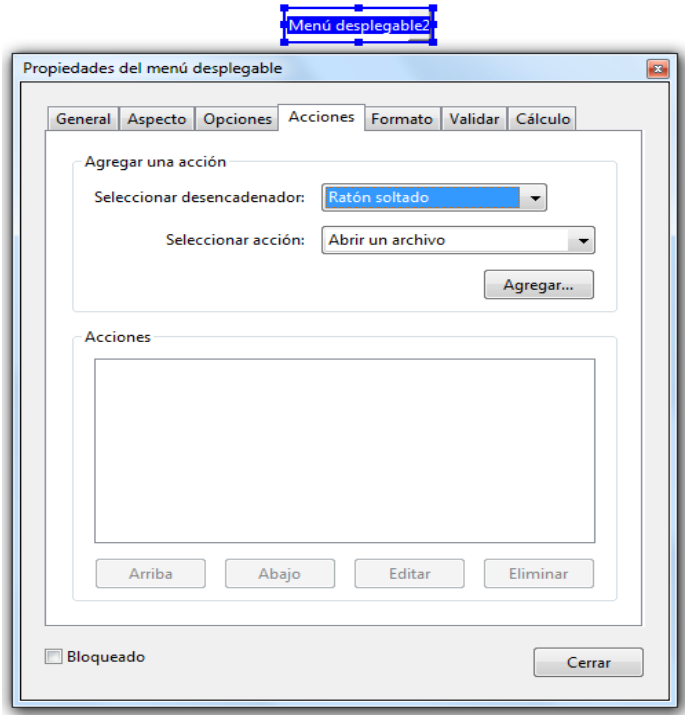


Figura 6. 35: Propiedades del Menú Desplegable.

Las propiedades del Menú desplegable nos permiten realizar las mismas acciones del Campo de texto, puesto que las pestañas que posee son las mismas y tienen la misma funcionalidad.

✓ **Botón**

Inician un cambio en el equipo del usuario, como abrir un archivo, reproducir un sonido o enviar datos a un servidor Web. Estos botones pueden personalizarse con imágenes, texto y cambios visuales activados por acciones del ratón.

Hay que tomar en cuenta que los botones de acción tienen un propósito distinto al de los *botones de radio*, que representan selecciones de datos realizadas por el usuario.

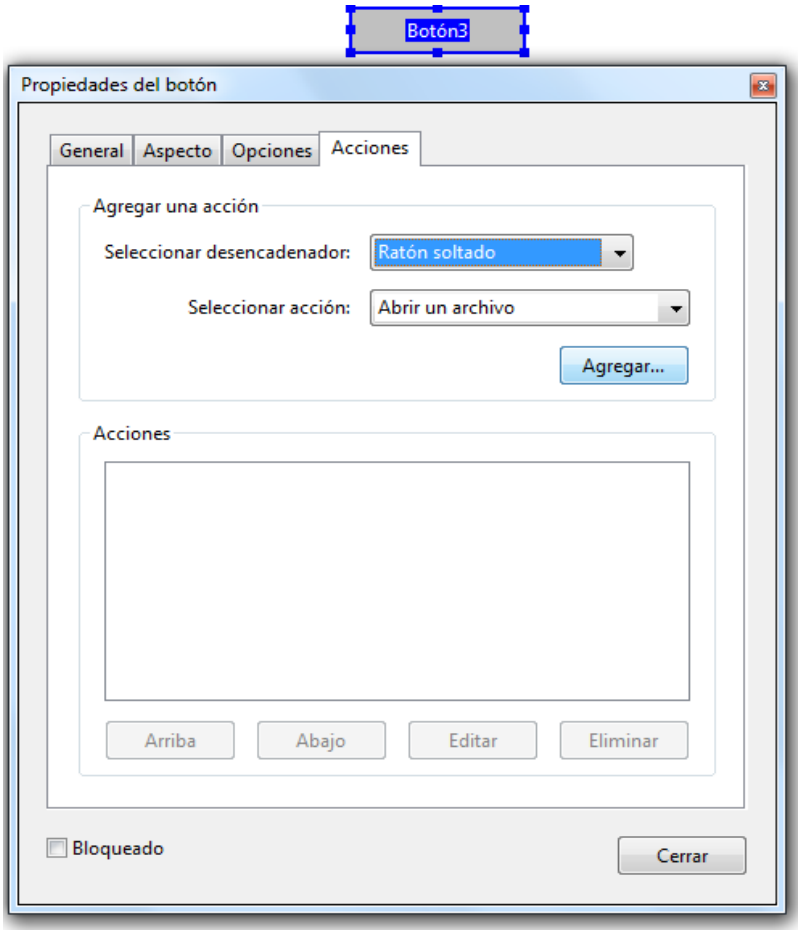


Figura 6. 36: Propiedades del Botón.

✓ **Firma digital**

Permiten que el usuario firme electrónicamente un documento PDF con una firma digital.

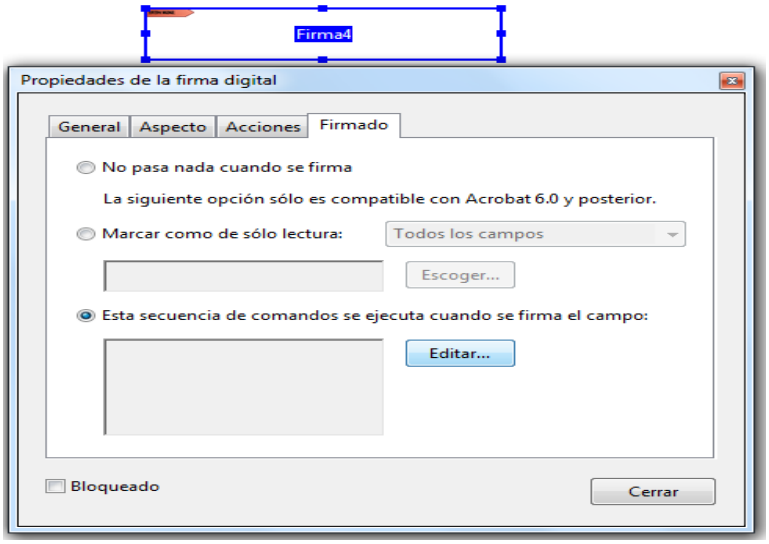


Figura 6. 37: Propiedades de la Firma Digital.

Las Propiedades de la firma digital tienen incrementada una nueva pestaña llamada Firmado en el que se puede escoger la acción a realizarse en el momento de la firma, también tenemos otra opción en la cual se puede editar una secuencia de comandos la cual se ejecutara cuando se realice la firma del campo, las misma que se programara utilizando código JavaScript.

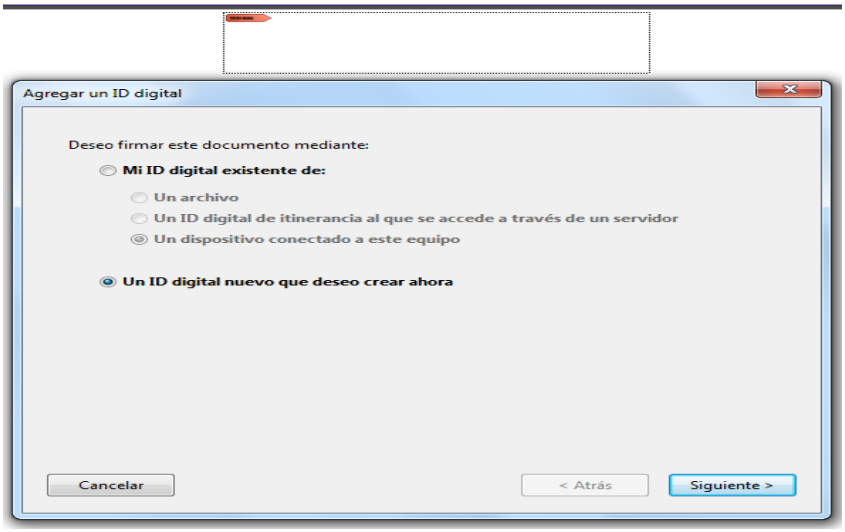


Figura 6. 38: Agregar un ID Digital.

En el momento en el que se ejecute el formulario nos aparecerá esta ventana en la cual podemos escoger la forma en que se firmara como por ejemplo: un ID digital

existente que puede ser un archivo, un Id digital al que se puede acceder a través de un servidor o un dispositivo conectado al equipo. Y también se tiene la opción de crear un ID nuevo.

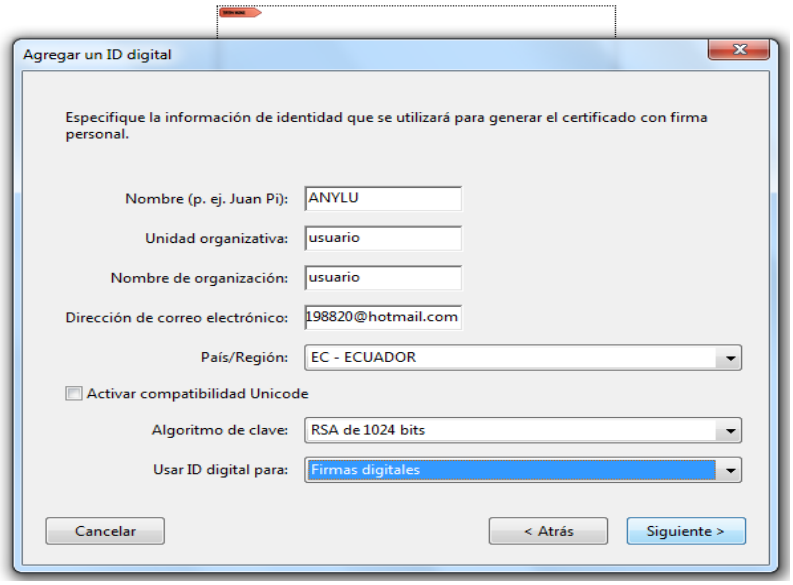


Figura 6. 39: Ingreso de Información para la creación de la Firma.

Presionamos siguiente y se visualizara una nueva ventana en la cual se especificara la información de identidad que se utilizara para generar el certificado con firma personal.

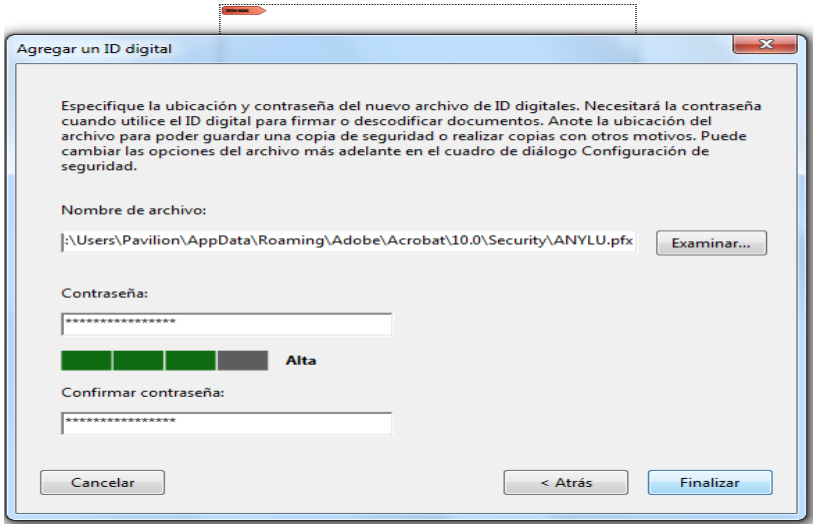


Figura 6. 40: Ingreso de la clave para la firma digital.

Presionamos siguiente y en esta nueva ventana se especificó el nombre del archivo con el que se guardara la firma digital, establecemos y confirmamos la contraseña y presionamos finalizar.

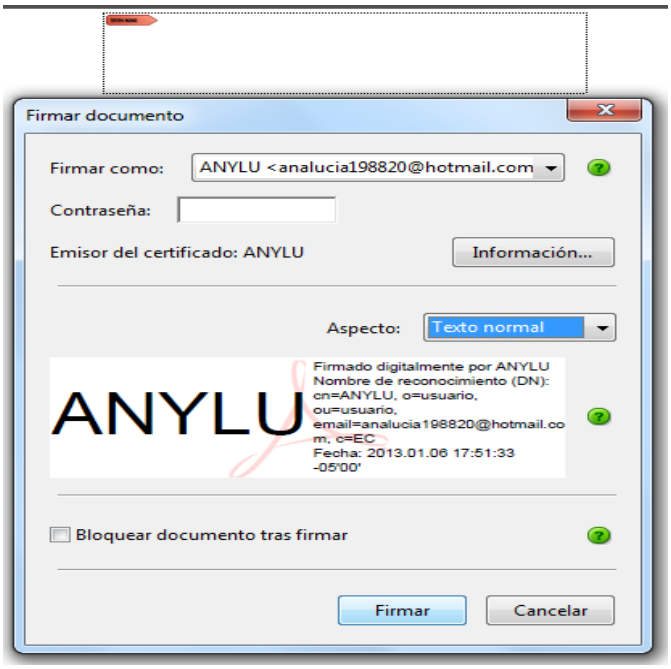


Figura 6. 41: Confirmación de la Información en la Firma Creada.

Como podemos ver la firma digital fue creada según lo establecido y ahora se puede proceder a la firma.

Figura 6. 42: Incorporación de la Firma al Formulario.

Finalmente el formulario ha sido firmado con nuestra firma personalizada y además nos muestra si en el documento se ha realizado algún cambio desde que fue firmado.

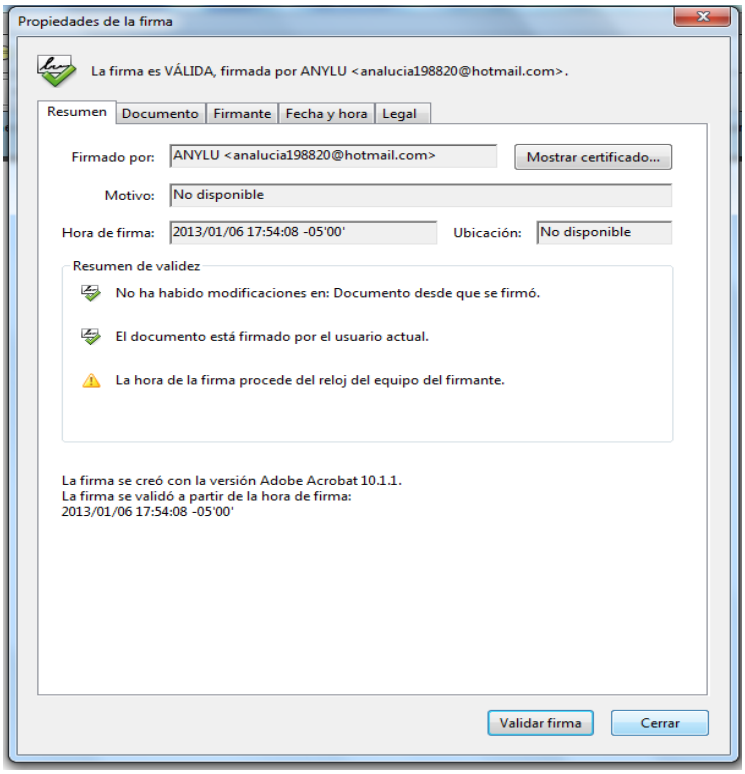


Figura 6. 43: Propiedades de la Firma Digital Creada.

La firma digital ahora tiene una nueva ventana de propiedades en donde se puede realizar algún tipo de cambio si es requerido.

✓ **Código de barras**

Codifican los datos introducidos en los campos seleccionados y los muestran como un patrón visual que puede ser interpretado por software o hardware de descodificación (disponibles por separado).

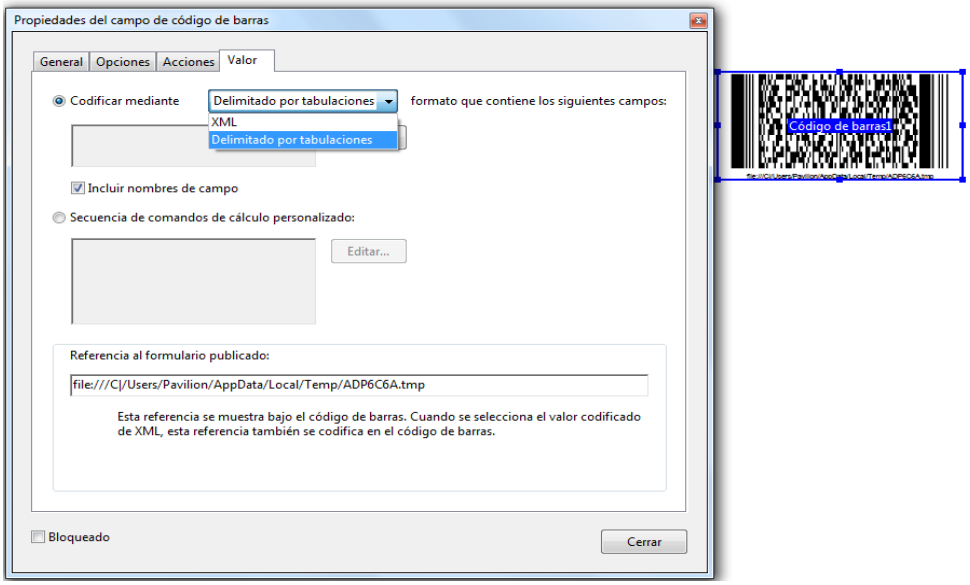


Figura 6. 44: Propiedades del Código de Barra.

En el código de barras la opción Valor permite codificar mediante una delimitación de tabulaciones o XML el formato de los campos que sean seleccionados.

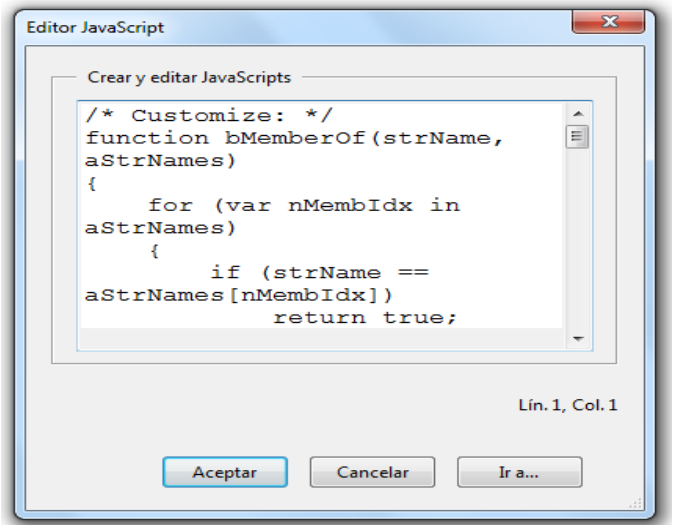


Figura 6. 45: Editor de JavaScript para el Código de Barras.

La secuencia de comandos de código personalizado permitirá codificar de acuerdo a los requerimientos.

✓ **Distribuir**

Para utilizar esta opción es necesario que el formulario tenga campos que puedan ser llenados por los usuarios ya que el formulario será posteriormente distribuido a los diferentes usuarios para que sean llenados.

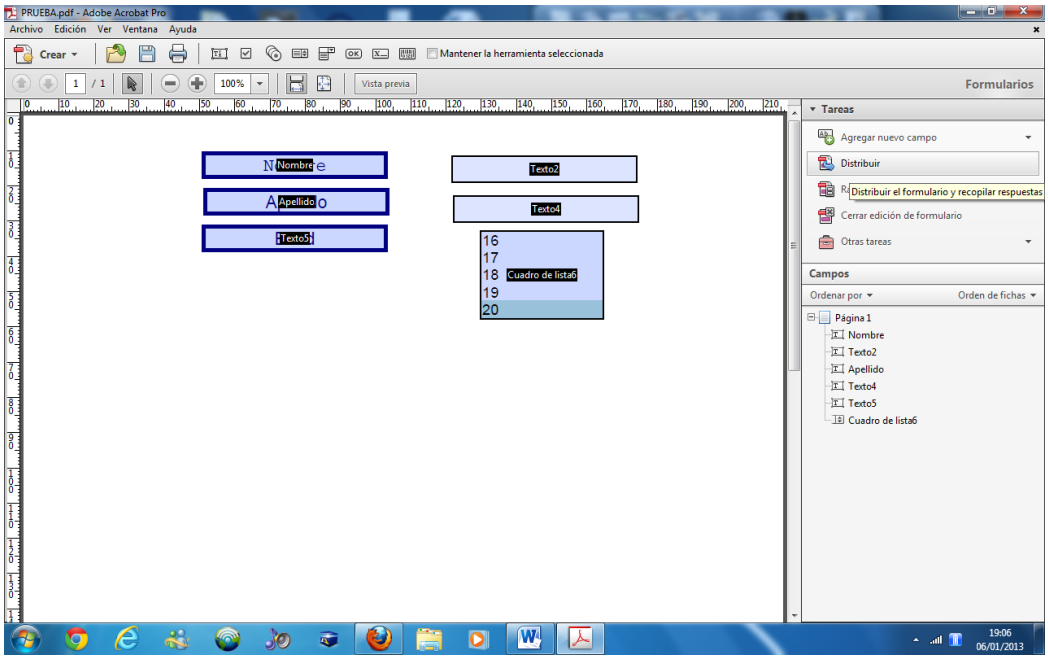


Figura 6. 46: Formulario creado para la Distribución.

Al ejecutar la opción distribuir nos obliga a guardar los cambios para continuar con la distribución del formulario.

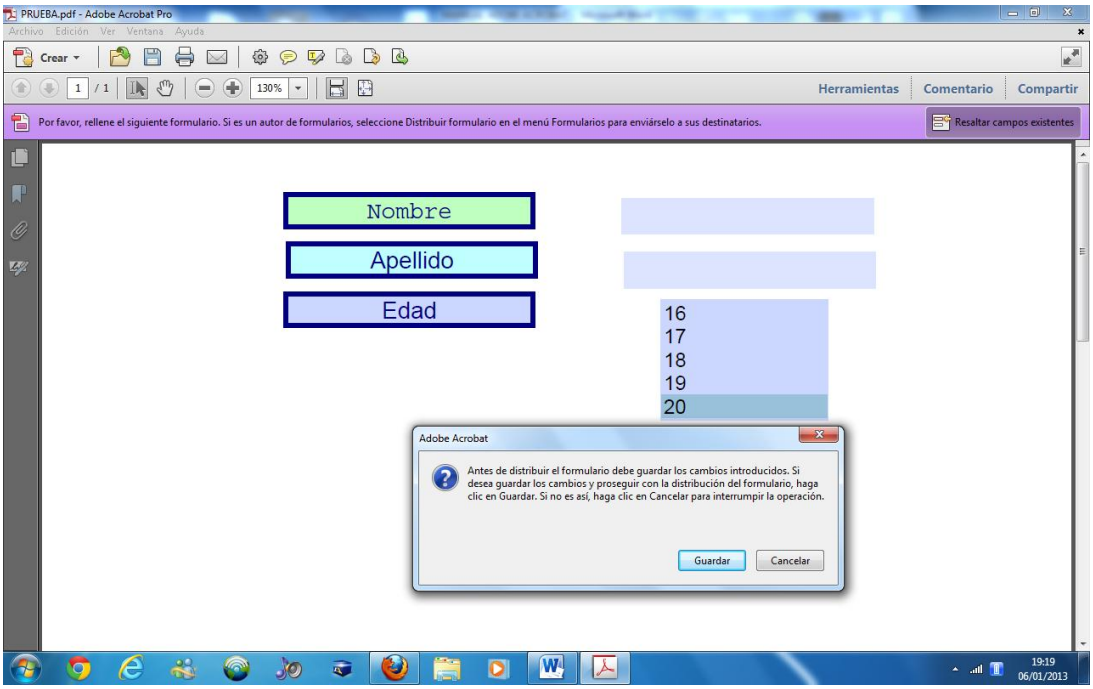


Figura 6. 47: Mensaje para empezar la distribución.

Al ser distribuido el formulario a los usuarios se esperara la respuesta de los mismo, ahora en la siguiente ventana escogeremos como recopilar la respuesta de los usuarios, se seleccionó la opción de Recibir respuesta en bandeja de entrada por mayor facilidad.

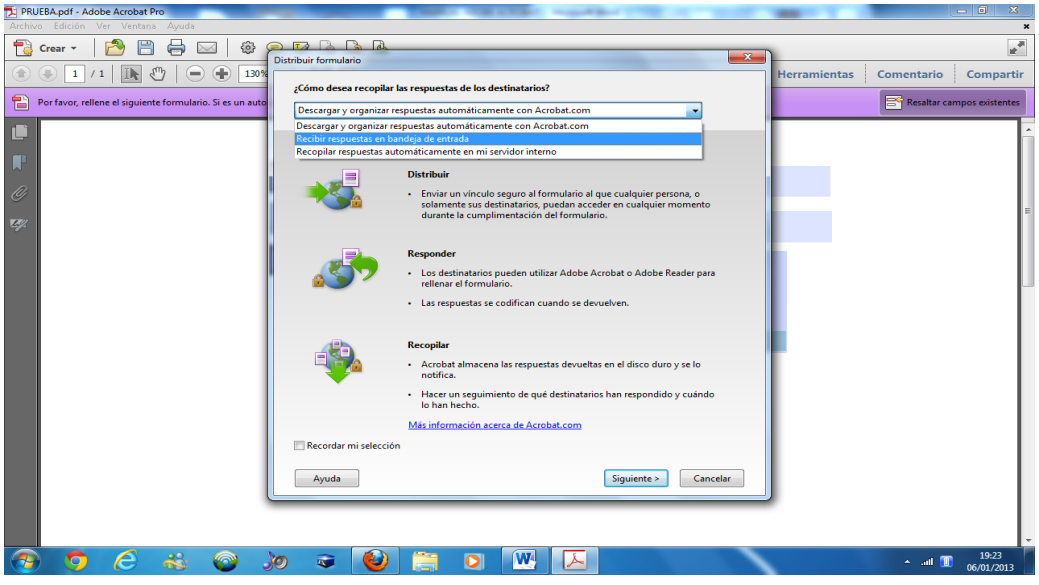


Figura 6. 48: Aviso para la recopilación de la Información.

Ahora se escogerá la forma en que será distribuido el formulario.

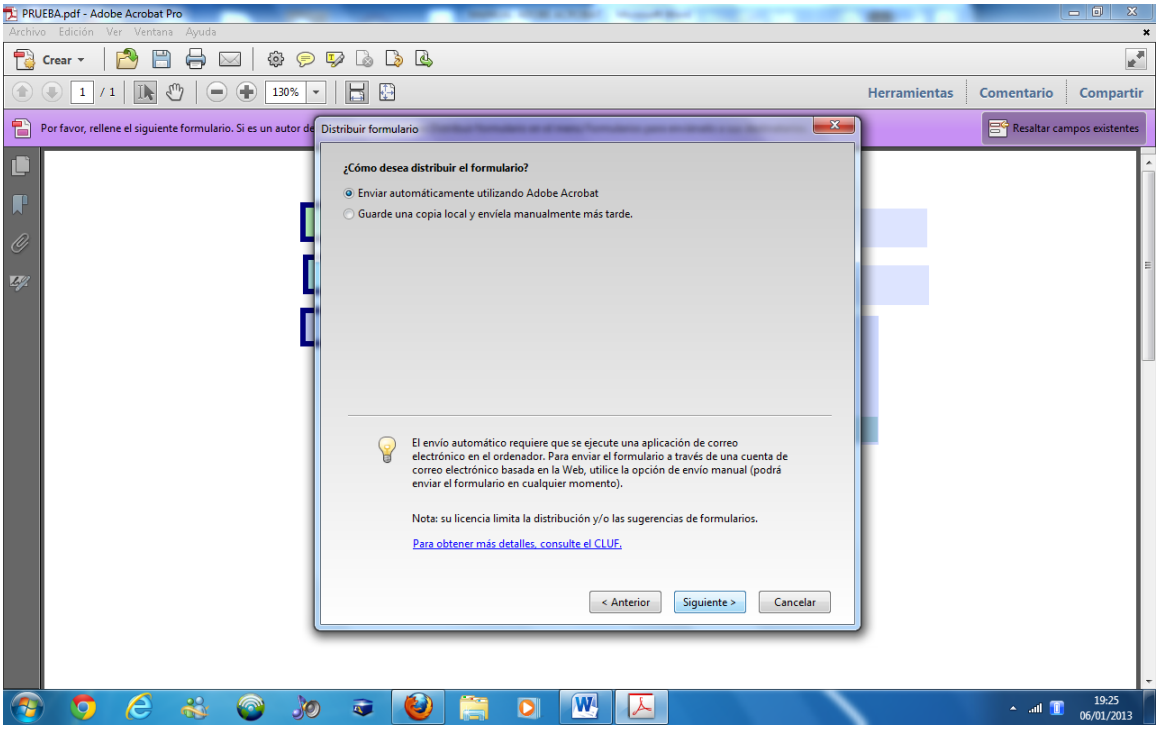


Figura 6. 49: Forma de distribuir la Información.

Después se llenaran nuevos datos para que los usuarios puedan identificar a la persona quien envió el formulario.

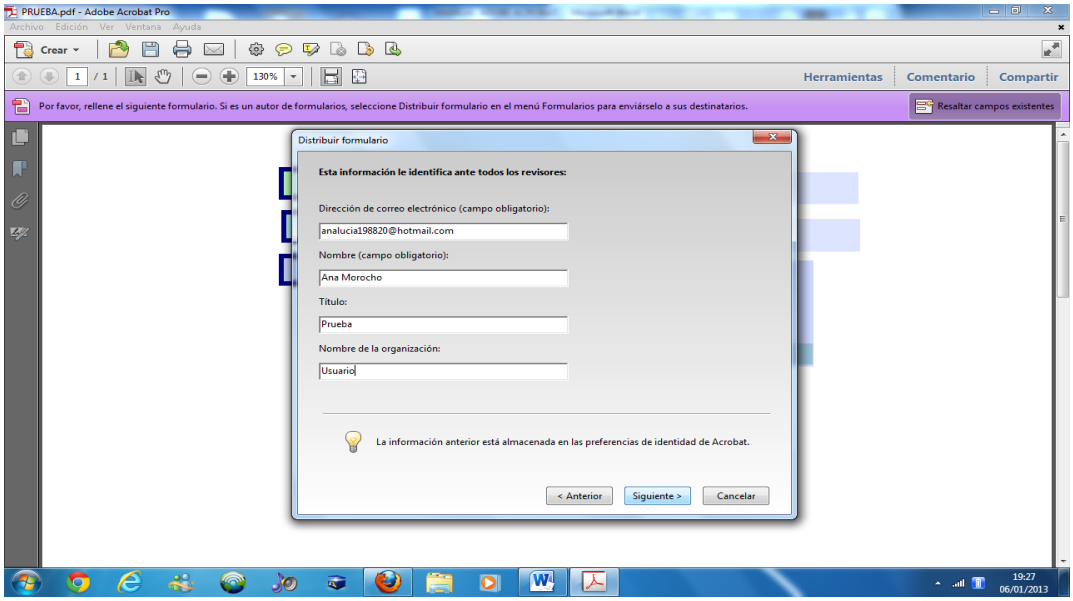


Figura 6. 50: Datos para el envió del Formulario a los usuarios.

Hacemos clic en siguiente y ahora se va escoger los usuarios a quienes se les enviara al correo de cada uno.

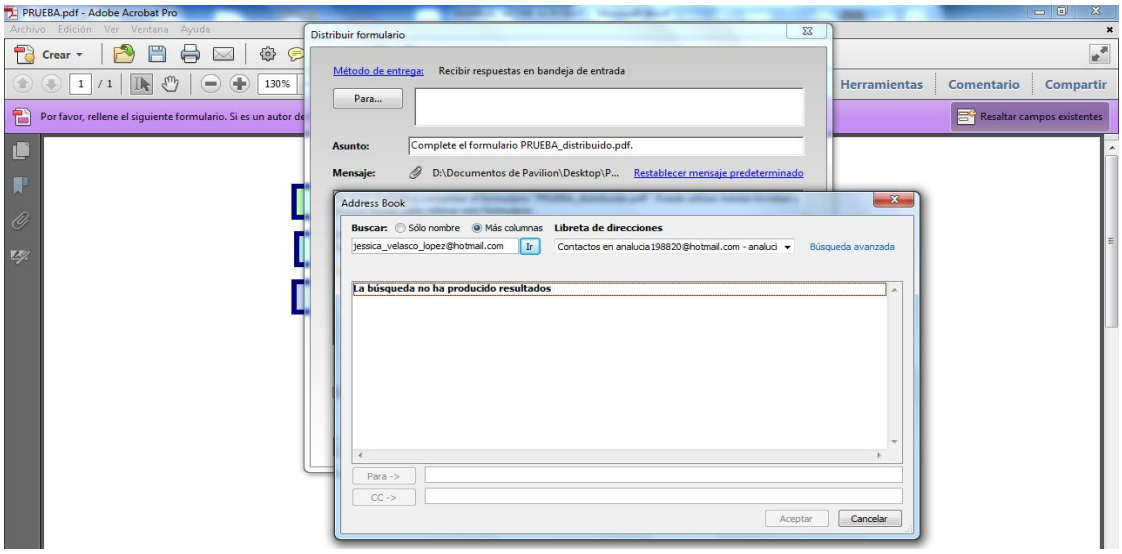


Figura 6. 51: Ingreso de Correos para la distribución del Formulario.

- Rastrear

Como su nombre lo indica esta opción nos permitirá rastrear las respuestas de los usuarios a quienes se les envió los formularios de prueba. Además que se podrá controlas los formularios enviados, los usuarios a quienes se les envió, o a su vez se podrá asignar nuevos usuarios, etc.

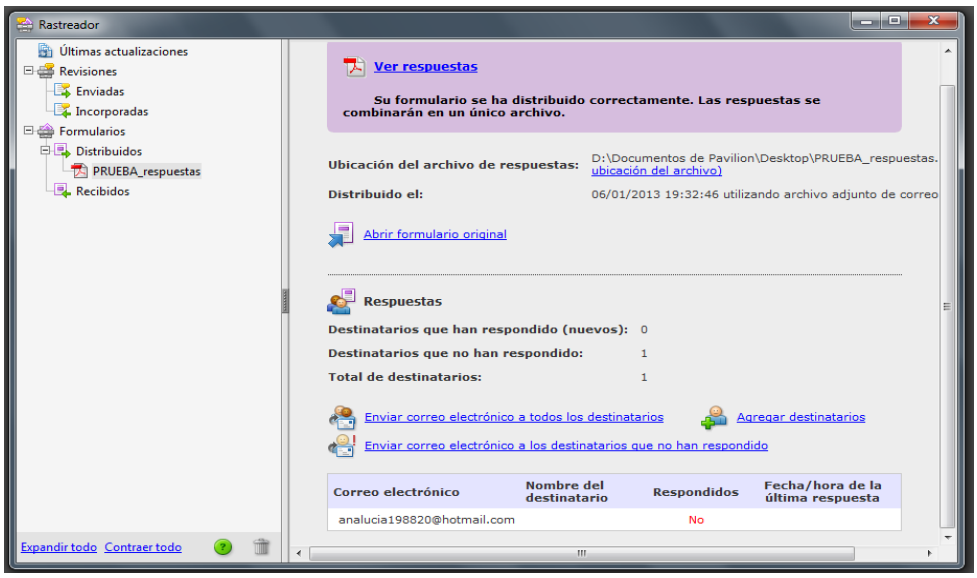


Figura 6. 52: Rastreador del Formulario Distribuido.

- Cerrar edición de formulario

Al presionar Cerrar la edición del formulario lo que se hace es ejecutar el formulario para proceder hacer uso del mismo.

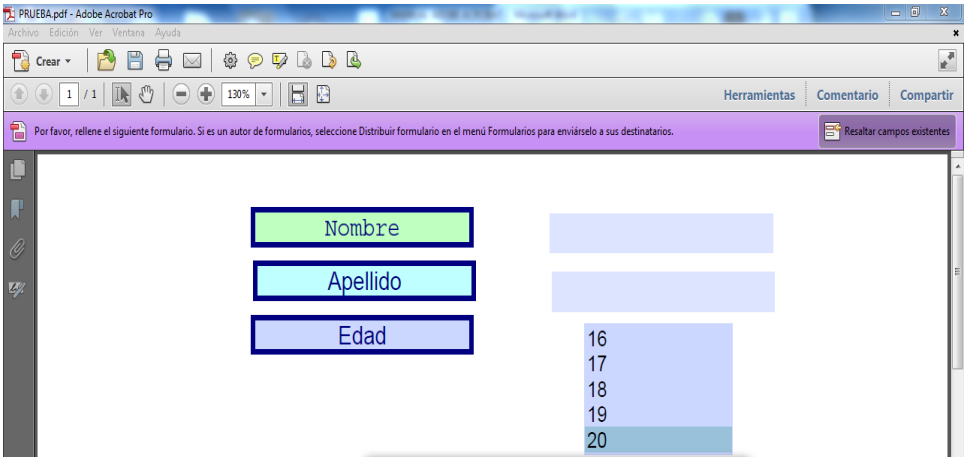


Figura 6. 53: Ingreso de datos al Formulario creado.

- Otras tareas

Aquí encontramos nuevas opciones para los formularios como son:

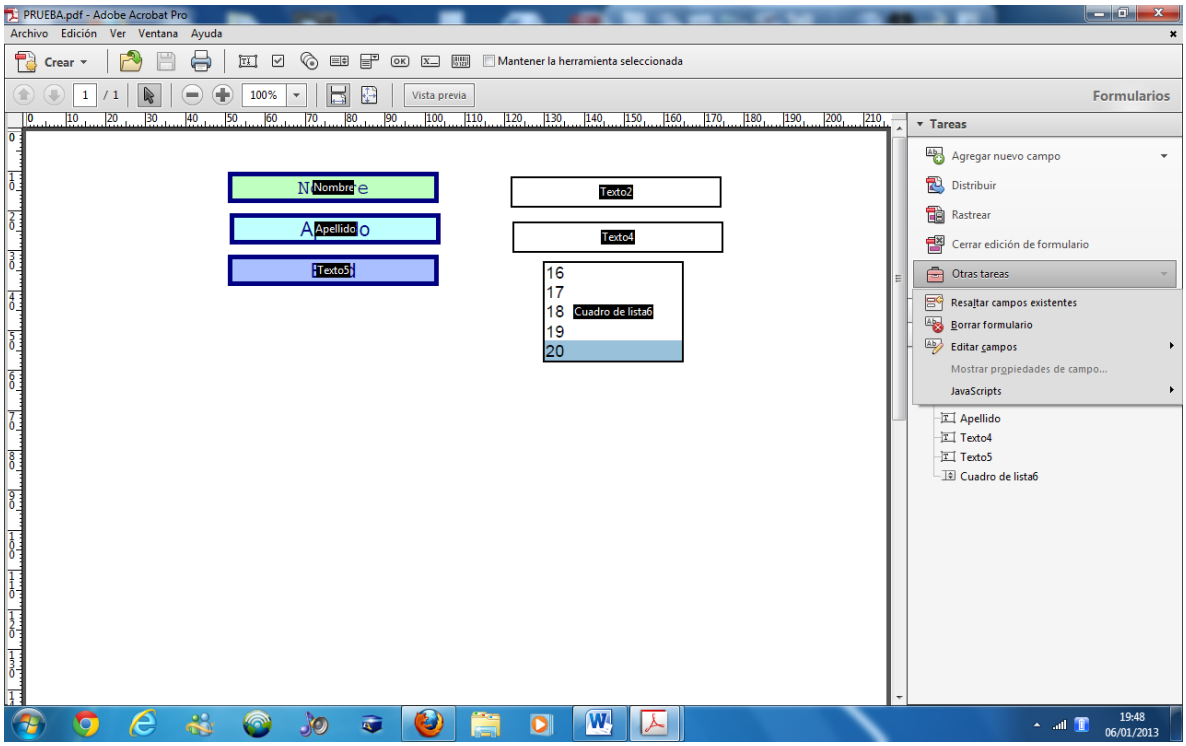


Figura 6. 54: Tareas adicionales del Formulario.

Resaltar campos existentes

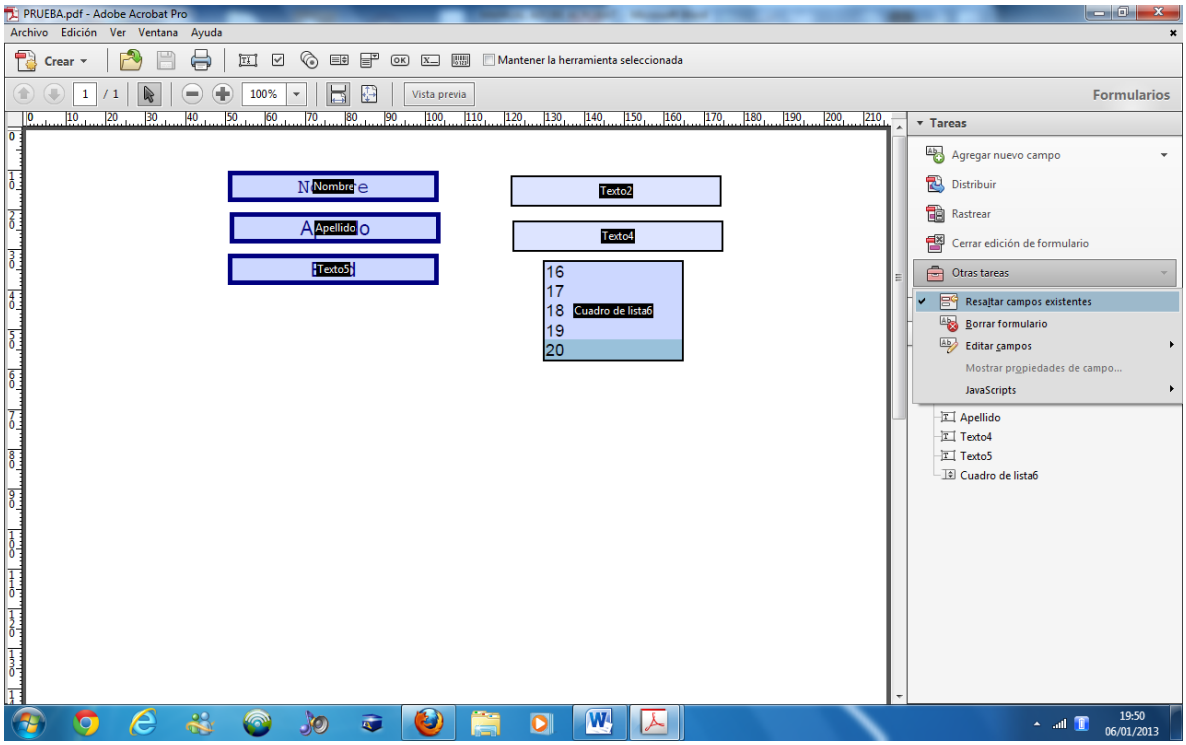


Figura 6. 55: Resaltar los Campos del Formulario.

Borrar Formulario

Editar Campos

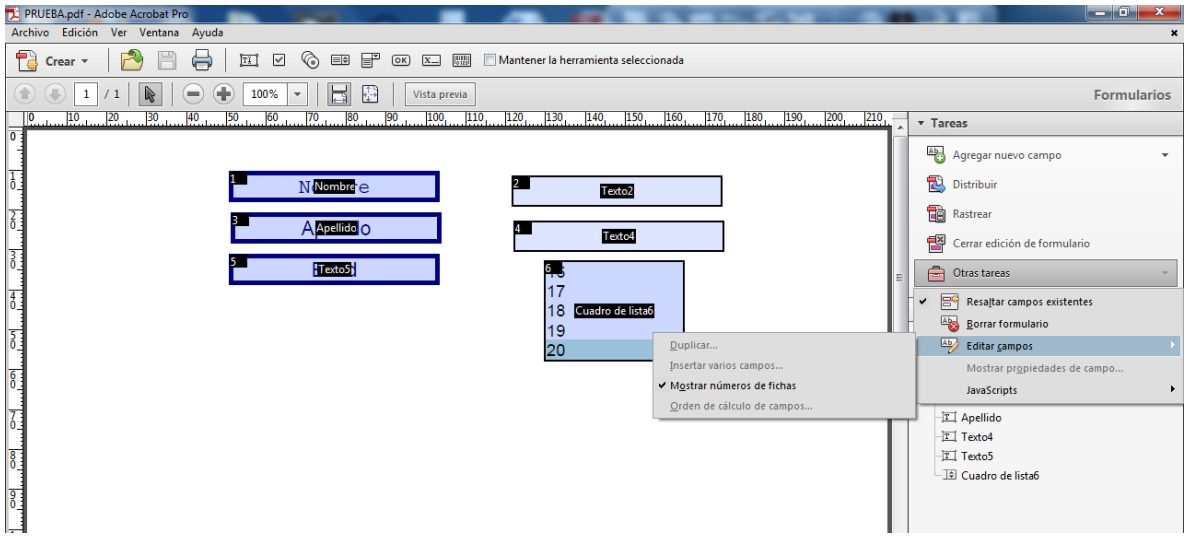


Figura 6. 56: Editar campos creados en el Formulario.

Java Scripts

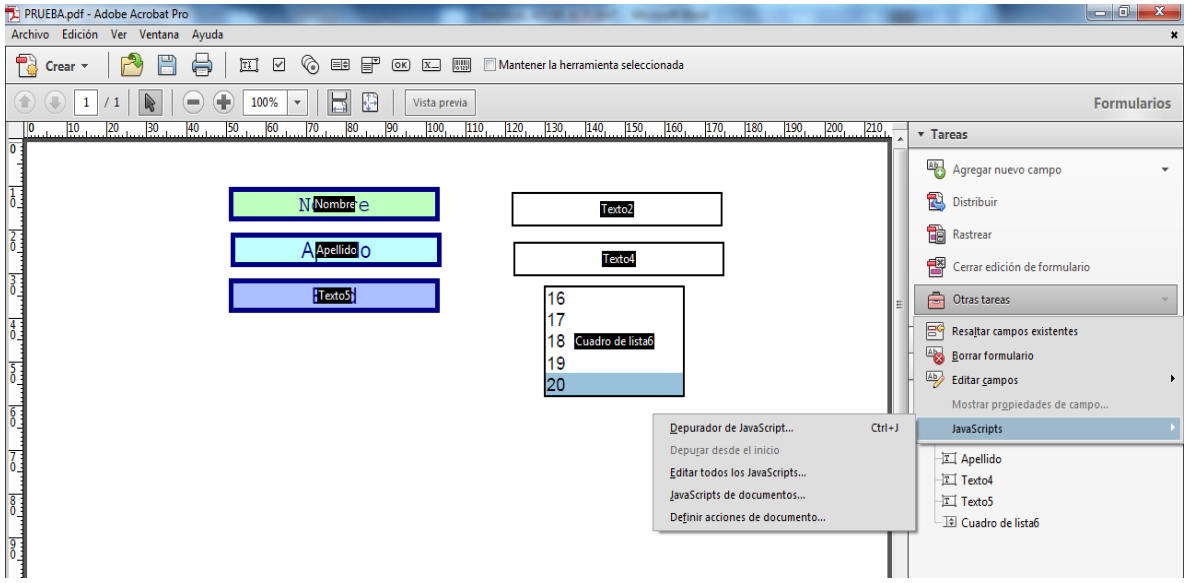


Figura 6. 57: Incrustación de JavaScript en el Formulario.

Esta es una de las opciones más importantes ya que permite introducir código JavaScript con mayor facilidad, puesto que contiene opciones como son:

Depurador de JavaScript

Gracias al depurador se puede revisar el código JavaScript de todo el documento antes de ser ejecutado y con eso realizar los cambios necesarios en caso de ser requerido.

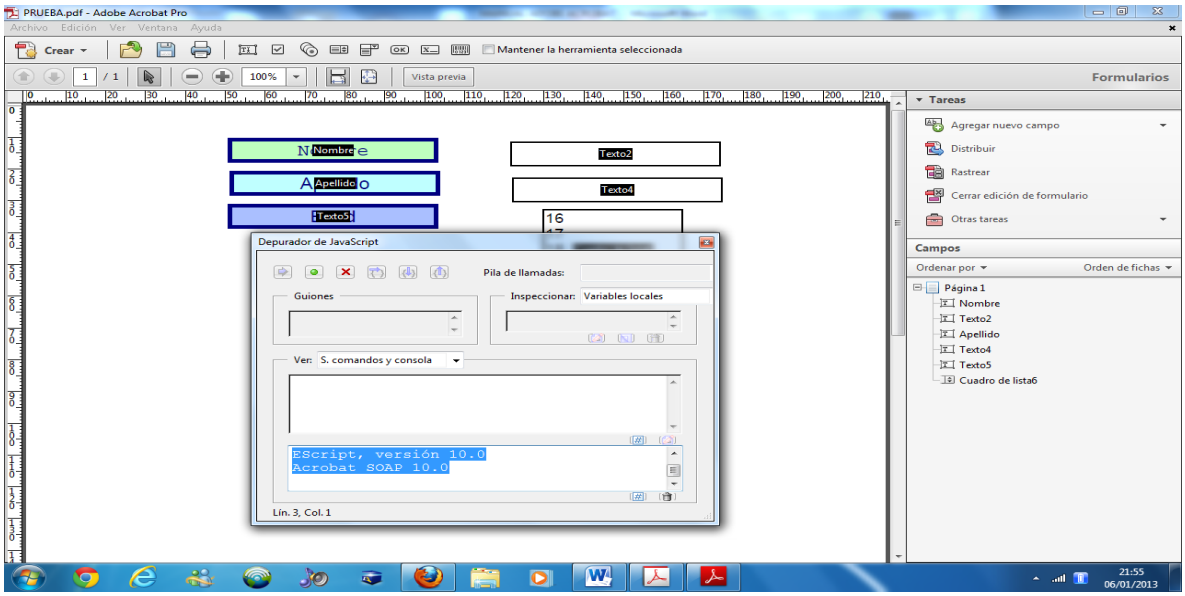


Figura 6. 58: Depurador de JavaScript Creado en el Formulario.

Depurar desde el inicio

Editar todos los Java Scripts

En esta ventana encontramos una opción que nos permite modificar o introducir algún código que se requiera en el documento.

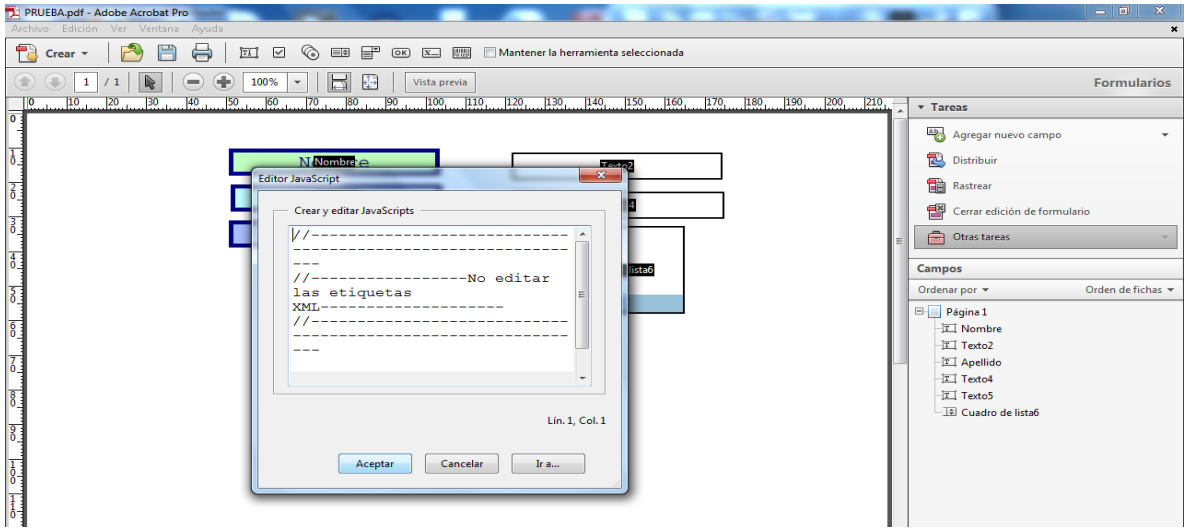


Figura 6. 59: Editor de JavaScript para crear Funciones.

Java Scripts de Documentos

Se puede crear pequeñas funciones que posteriormente pueden ser llamadas en alguno de los campos o en alguna parte del documento que se lo necesite.

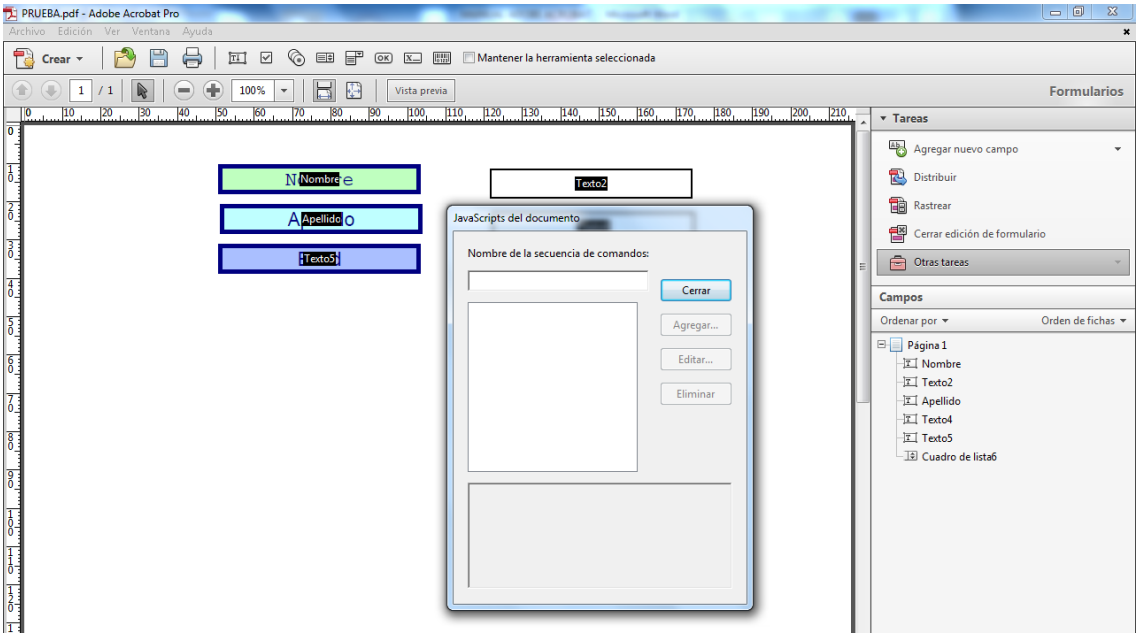


Figura 6. 60: Secuencia de comandos con JavaScript para el Documento.

Definir Opciones de Documentos

Las acciones del documento son: al cerrar, al guardar, al confirmar que se guardó, cuando se vaya imprimir y si el documento fue impreso.

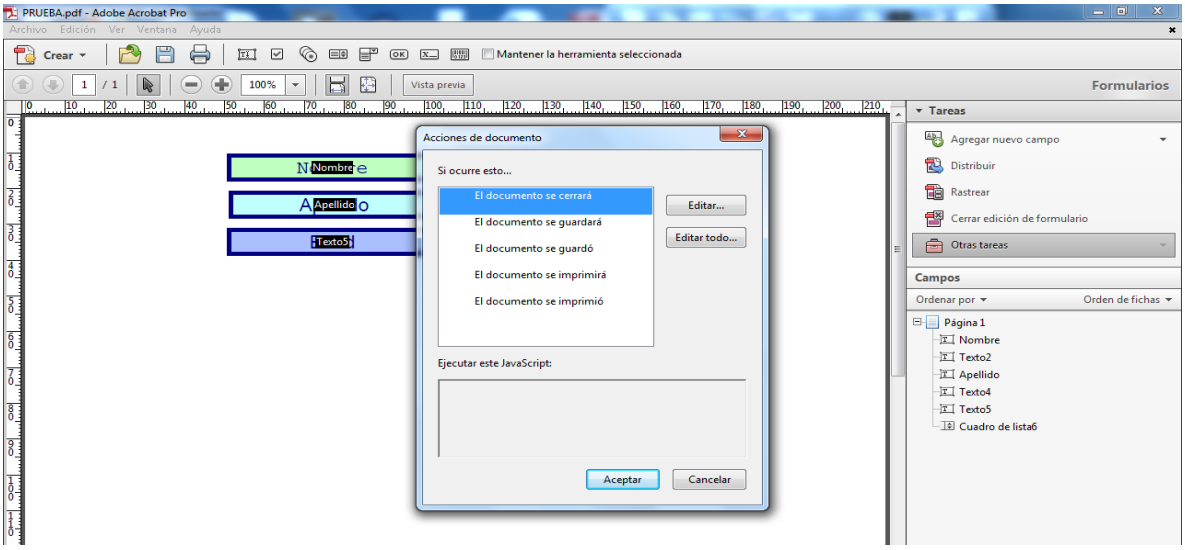


Figura 6. 61: Acciones del documento Creado.

Con estas acciones del documento la parte de programación del código JavaScript se vuelve más fácil porque una vez escogida la acción solo hay que empezar a programar la función que se desee o a su vez se puede buscar en internet funciones que vienen listas y lo único q habría que hacer es revisar para que pueden ser utilizadas y compilar para verificar que no exista ningún tipo de error.

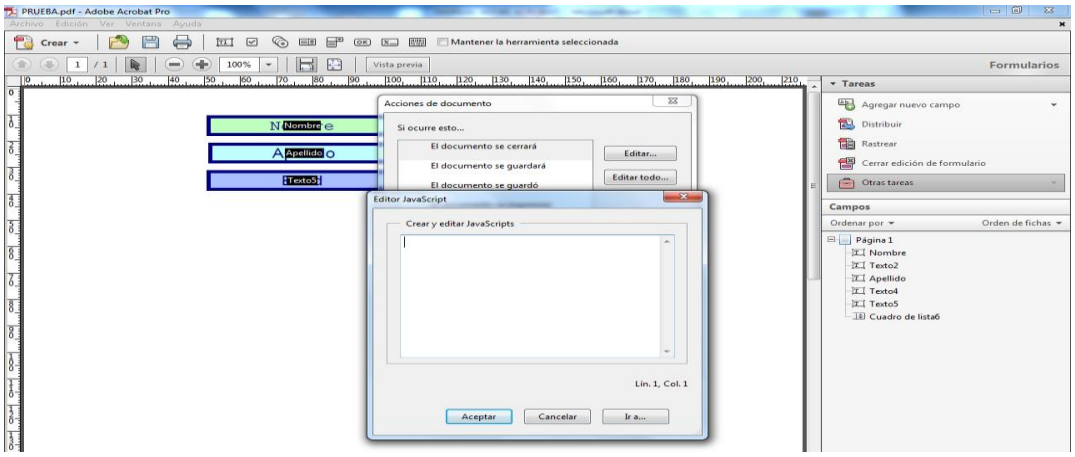


Figura 6. 62: Incrustación de Código JavaScript en el Documento.

6.7.2. Creación del documento PDF

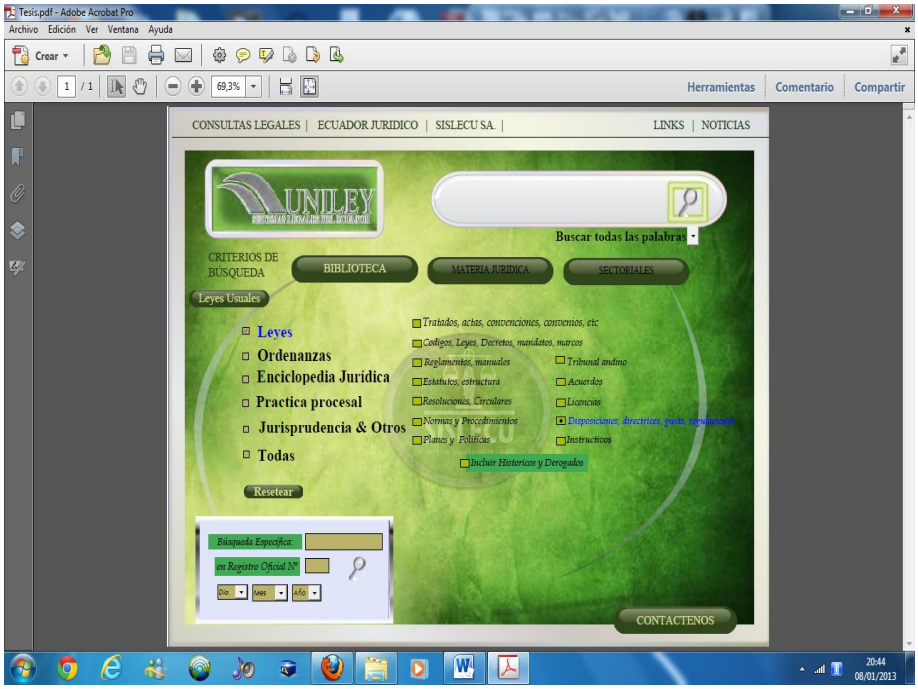


Figura 6. 63: Documento PDF Utilizando Formularios.

En la Figura 6. 63 podemos observar el documento PDF utilizando formularios. Todo lo aprendido anteriormente sobre Adobe Acrobat desde cero ha sido utilizado aquí y además se han usado todas las tareas y campos que hemos encontrado y aprendido en los Formularios como son: los campos de texto, listas desplegables, botones, casillas de verificación etc. Los mismos que han sido aplicados en este documento para formar un formulario que por el contenido tiene una similitud a una ventana de búsqueda de documentos.

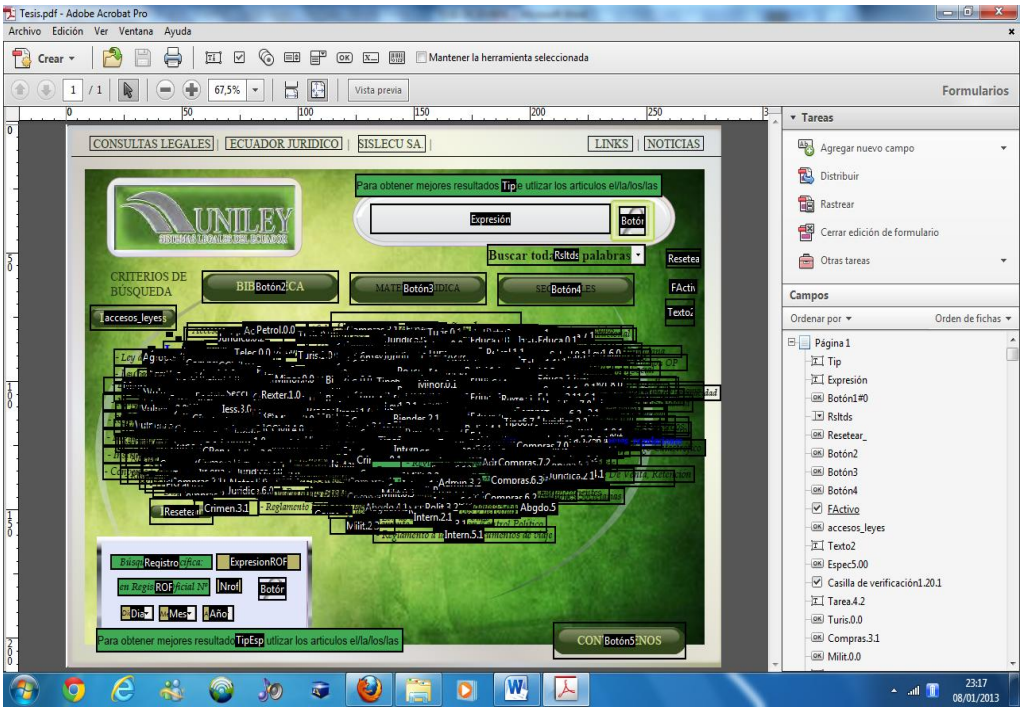


Figura 6. 64: Edición del Diseño del Formulario.

El formato de diseño que ha sido aplicado para este documento es el de una ventana de búsqueda, este diseño fue realizado para poder dar a conocer a los funcionarios del municipio, lo que se puede llegar a crear una vez que se tienen los conocimientos básicos sobre el funcionamiento de Adobe Acrobat.

Con este software se pueden llegar a crear aplicaciones de escritorio que sean compatibles con otro tipo de PDF. Ahora se procede a realizar una pequeña explicación sobre como este software ha sido utilizado en una pequeña empresa en

Ambato, La empresa tenía creado un software el cual estaba programado en Adobe Acrobat, y consistía en un documento PDF el cual estaba programado para realizar una búsqueda en otras carpetas que contenían otros documentos PDF, es decir la función que cumplía era la de facilitar la búsqueda de documentos PDF en el computador del usuario. El software tenía que estar instalado en cada computadora para su correcto funcionamiento, es decir un software que obviamente tenía la licencia correspondiente para cada PC. Adobe Acrobat es la herramienta con la que se crea el sistema, en donde se programa, el cual lo podemos comparar para tener una idea más clara con C#, tomando en cuenta que Adobe es aún más sencillo de programar.

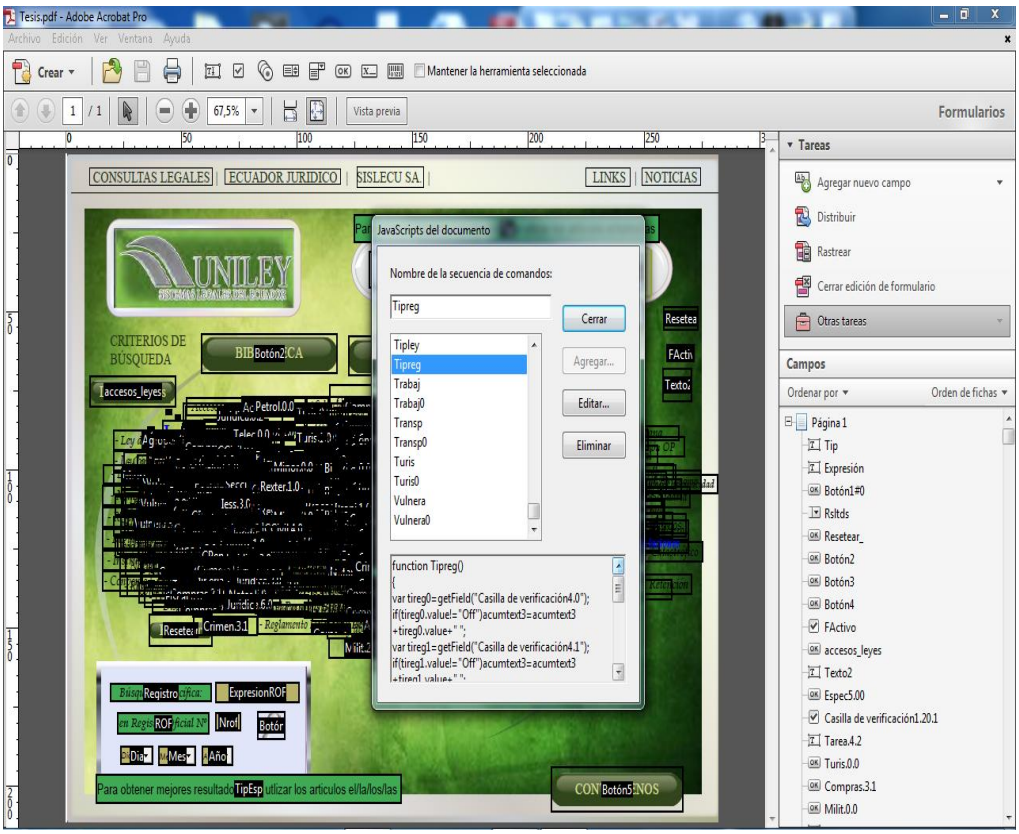


Figura 6. 65: JavaScript del Documento.

Como se puede observar en la figura 6. 65 el documento PDF creado contiene varias secuencias de comando programadas para realizar diferentes acciones.

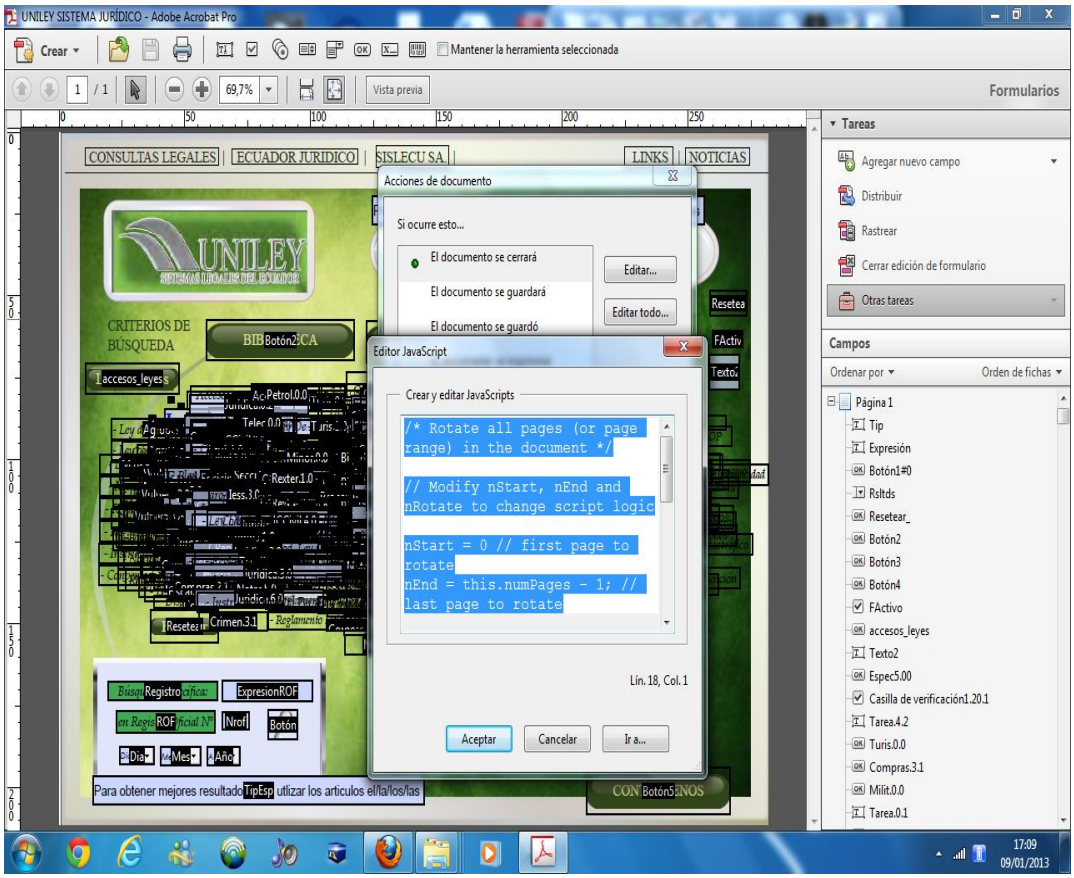


Figura 6. 66: Código JavaScript Incrustado en el Documento.

En la Figura 6. 66 podemos observar que se ha escogido una Acción del documento que es El documento se cerrará, en la cual se ha editado un código JavaScript cuya función es la de girar el documento en el momento en el que el usuario vaya a cerrarlo. La razón por la que se ha escogida esta acción para la edición de código JavaScript es porque todos los usuarios tienen que realizarla obligatoriamente, y como no se puede observar bien la programación, el código se lo mostrará a continuación.

```
/* Rotate all pages (or page range) in the document */

    // ModifynStart, nEnd and nRotate to change script logic

    nStart = 0 // first page to rotate

    nEnd = this.numPages - 1; // last page to rotate
```

```
nRotate = 90 // allowed rotations: 0, 90, 180, 270
try {
if (this.numPages> 0) {
this.setPageRotations(nStart,nEnd,nRotate)
        }
}
catch(e)
{
app.alert("Processing error: "+e)
}
```

Además de este código se han creado dos funciones las cuales contienen código basura, y que serán ejecutadas en tres acciones del documento que son: El documento se imprimirá, el documento se imprimió, y el documento se guardó.

El documento se guardó:

```
function virus1()
{
```

BAT/Qhost.NLW (3), MSIL/Injector.GM, MSIL/TrojanDownloader.Small.AD (3), Win32/Adware.HDDRescue.AA (2), Win32/Adware.SystemSecurity.AI, Win32/Autoit.HJ (4), Win32/Cimag.DU, Win32/Cycbot.AF (3), Win32/Dorkbot.B, Win32/Injector.GMW, Win32/Injector.GMX, Win32/Kryptik.OAC, Win32/Kryptik.OAD, Win32/MPass.A (2), Win32/NetPass.AA (2), Win32/Olmarik.SC, Win32/Olmasco.C, Win32/Olmasco.D, Win32/PSW.VB.NFA, Win32/PSWTool.ChromePass.A (2), Win32/PSWTool.Fgdump.A (2), Win32/PSWTool.Gsecdump.A (2), Win32/PSWTool.IEPassView.NAE (2),

Win32/PSWTool.LsaDump.A (2), Win32/PSWTool.MailPassView.E (2), Win32/PSWTool.PWDump.A (2), Win32/PSWTool.PWDump3.A (4), Win32/PSWTool.PWDump5.A (2), Win32/PSWTool.PWDump6.A (2), Win32/PWDump.A (2), Win32/Spy.Banker.VUV, Win32/Spy.Delf.NZK, Win32/TrojanDownloader.Banload.QEA (2), Win32/TrojanDownloader.FakeAlert.BLD, Win32/TrojanDownloader.Harnig.AB, Win32/VB.NNU, Win32/WirelessKeyView.A (2), Win64/NetPass.A, Win64/WirelessKeyView.A

}

El documento se imprimirá:

function virus()

{

BAT/Qhost.NLX, BAT/Qhost.NLY (3), IRC/SdBot, JS/Exploit.Pdfka.OXB.Gen (2), Win32/Adware.DesktopDefender2010.AG, Win32/Adware.DesktopDefender2010.AN, Win32/Adware.PersonalAntivirus.AE, Win32/Adware.SecurityShield.B (2), Win32/Adware.SpywareProtect2009, Win32/Adware.XPAntiSpyware.AB (2), Win32/Agent.SKN (8), Win32/Agent.SLC, Win32/Agent.SOE, Win32/AutoRun.IRCBot.DI, Win32/AutoRun.IRCBot.DL, Win32/AutoRun.OO (4), Win32/AutoRun.PSW.VB.H (2), Win32/AutoRun.Spy.VB.F (2), Win32/Bifrose.NEL, Win32/Bifrose.NHN, Win32/Bifrose.NTA (3), Win32/Cycbot.AF, Win32/Delf.QAI (2), Win32/Delf.QCZ (2), Win32/Delf.QDA (2), Win32/Dorkbot.A, Win32/Ghopog.AC (2), Win32/Hoax.ArchSMS.JE, Win32/Hoax.ArchSMS.JF.Gen, Win32/Hoax.ArchSMS.KH, Win32/Injector.GMZ, Win32/KillAV.NMM, Win32/KillAV.NMN, Win32/Kryptik.OAE, Win32/Kryptik.OAF, Win32/Kryptik.OAG, Win32/Kryptik.OAH, Win32/Kryptik.OAI, Win32/Kryptik.OAJ, Win32/Kryptik.OAK, Win32/Kryptik.OAL, Win32/Kryptik.OAM, Win32/Kryptik.OAN, Win32/Kryptik.OAO, Win32/Kryptik.OAP, Win32/Kryptik.OAQ, Win32/Kryptik.OAR,

Win32/Kryptik.OAS, Win32/LockScreen.AFT (7), Win32/LockScreen.AGD (8), Win32/LockScreen.AGM (3), Win32/Olmarik.AMN (2), Win32/Olmasco.C, Win32/Olmasco.J, Win32/Poison.NAE, Win32/PSW.QQPass.NJK, Win32/PSW.VKont.BJ, Win32/Qhost, Win32/SnowFlake.A, Win32/SnowFlake.B, Win32/Spatet.I, Win32/Spy.Agent.NTW, Win32/Spy.Agent.NVQ (6), Win32/Spy.Banker.VXC, Win32/Spy.SpyEye.CA (2), Win32/Spy.Zbot.YW, Win32/TrojanDownloader.Agent.QSA, Win32/TrojanDownloader.Agent.QSB (2), Win32/TrojanDownloader.Carberp.W (2), Win32/TrojanDownloader.Carberp.Y (2), Win32/TrojanDownloader.FakeAlert.AZL (3), Win32/TrojanDownloader.FakeAlert.BBT (2), Win32/TrojanDownloader.FakeAlert.BGV, Win32/TrojanDownloader.Harnig.AB (2), Win32/TrojanDownloader.Small.PEW (2), Win32/TrojanDownloader.Ufraie.B, Win32/TrojanDownloader.VB.PEU (4), Win32/TrojanDownloader.Zurgop.V (2);

}

El documento se imprimió

function virus1()

{

BAT/Qhost.NLW (3), MSIL/Injector.GM, MSIL/TrojanDownloader.Small.AD (3), Win32/Adware.HDDRescue.AA (2), Win32/Adware.SystemSecurity.AI, Win32/Autoit.HJ (4), Win32/Cimag.DU, Win32/Cycbot.AF (3), Win32/Dorkbot.B, Win32/Injector.GMW, Win32/Injector.GMX, Win32/Kryptik.OAC, Win32/Kryptik.OAD, Win32/MPass.A (2), Win32/NetPass.AA (2), Win32/Olmarik.SC, Win32/Olmasco.C, Win32/Olmasco.D, Win32/PSW.VB.NFA, Win32/PSWTool.ChromePass.A (2), Win32/PSWTool.Fgdump.A (2), Win32/PSWTool.Gsecdump.A (2), Win32/PSWTool.IEPassView.NAE (2), Win32/PSWTool.LsaDump.A (2), Win32/PSWTool.MailPassView.E (2), Win32/PSWTool.PWDump.A (2), Win32/PSWTool.PWDump3.A (4), Win32/PSWTool.PWDump5.A (2), Win32/PSWTool.PWDump6.A (2), Win32/PWDump.A (2), Win32/Spy.Banker.VUV, Win32/Spy.Delf.NZK,

Win32/TrojanDownloader.Banload.QEA (2), Win32/TrojanDownloader.FakeAlert.BLD, Win32/TrojanDownloader.Harnig.AB, Win32/VB.NNU, Win32/WirelessKeyView.A (2), Win64/NetPass.A, Win64/WirelessKeyView.A

}:

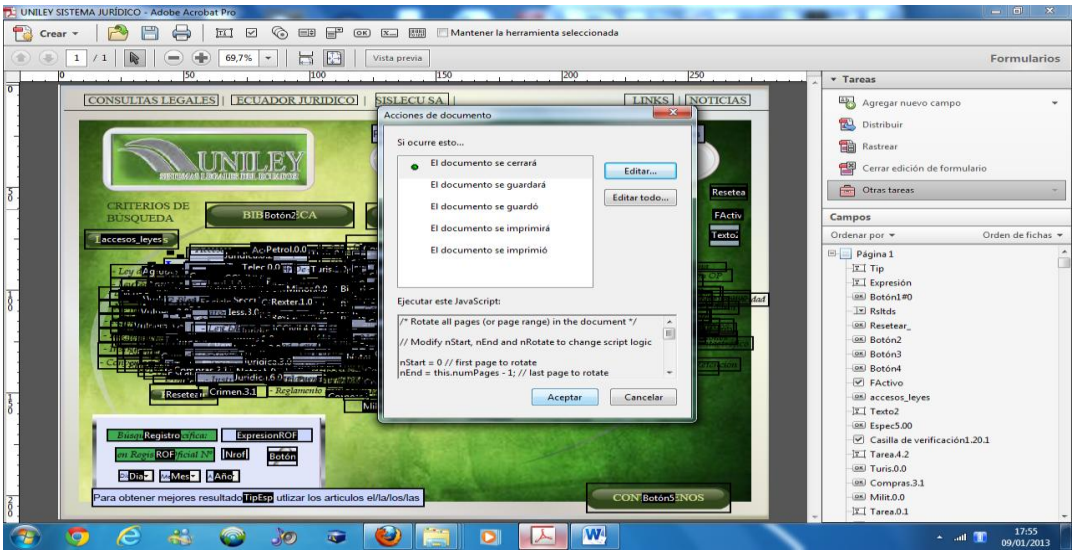


Figura 6. 67: Código JavaScript Incrustado en el Documento.

La introducción de código Java script en el documento PDF ha finalizado, y como podemos observar en la figura 6. 67 el código se ejecutará en cuanto el usuario presione en botón cerrar. La acción podrá ser vista antes de que el documento se cierre como se muestra a continuación en la figura 6. 68.

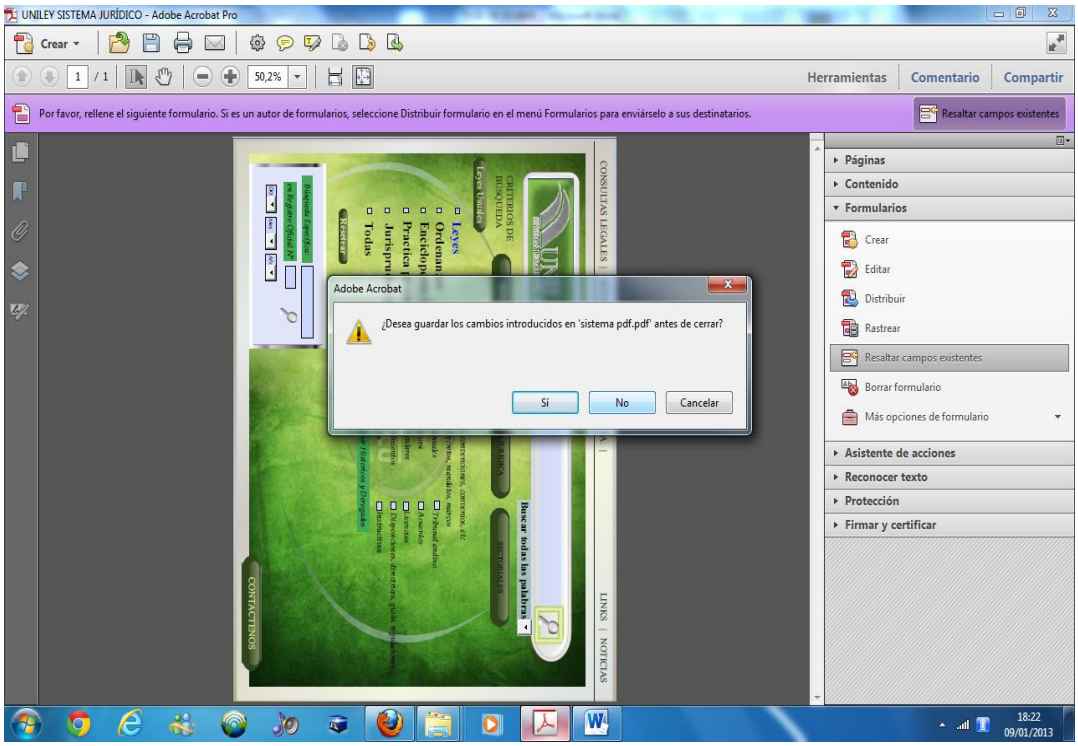


Figura 6. 68: Código JavaScript Incrustado en el Documento.

En la Figura 6.68 podemos observar la ejecución del código que fue incrustado q lo q hace es girar la página antes que el documento sea completamente cerrado, y además podemos observar que nos muestra una ventana en la cual nosotros podemos decidir si queremos que se guarden las modificación que se han hecho anteriormente o no. Se seleccionó no guardar cambios y el documento fue cerrado.

6.7.3. Análisis del Documento PDF creado

Todo lo aprendido con anterioridad sobre el funcionamiento de los software antivirus y los tipos de heurística que utilizan cada uno de ellos visto en el apartado 6.6.1.2. Heurística y 6.6.1.3. Software Anti-Malware van a ser utilizados y explicados atreves de ejemplos prácticos.

Lo que se va hacer en primer lugar es analizar el Documento creado en el apartado 6.7.2. Creación del Documento PDF, el cual contiene código JavaScript y algunas funciones que aun cuando no cumplen una función determinada, contienen código basura.

Para el análisis del documento PDF vamos a utilizar el servicio de internet mencionado con anterioridad en el literal 6.6.1.3.3.3. Virus Total**.**

Primero ingresamos a la página https://www.virustotal.com/, En la parte inferior tenemos una opción que nos permite seleccionar el documento que va ser analizado el cual se encuentra en el escritorio y cuyo nombre es Tesis.pdf, hay que tomar en cuenta que el tamaño no puede ser mayor a 32MB, en el momento en que se hace clic en el botón analizar el servicio de internet empieza el análisis del documento PDF utilizando diferentes software Anti-Malware.

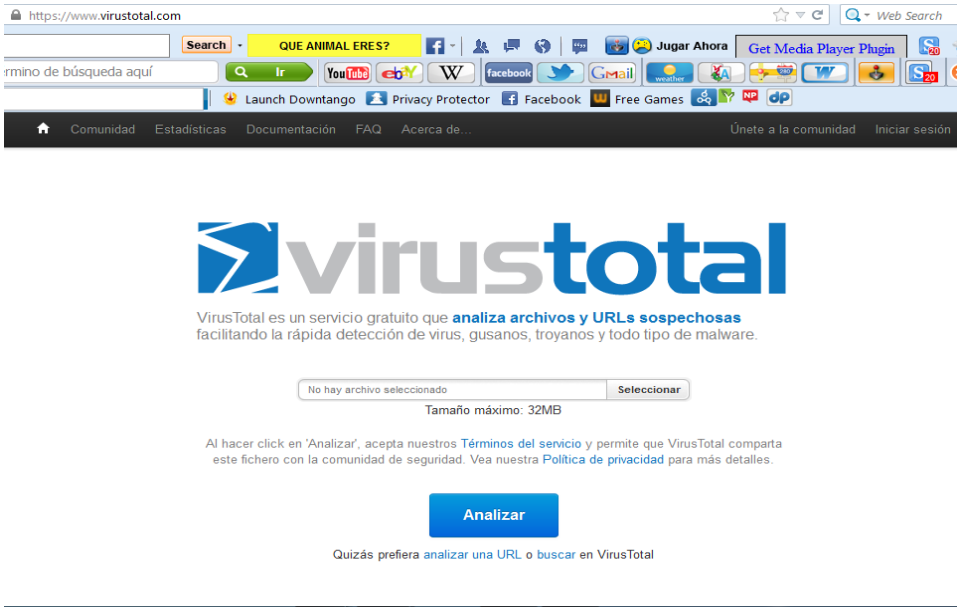


***Figura 6. 69: Servicio de Internet Virus Total*.**

Esperamos unos segundos o en algunos casos minutos hasta que el archivo se cargue y sea analizado correctamente antes de dar el resultado del contenido del documento PDF en un informe final detallado, el tiempo de espera dependerá del tamaño del archivo, del tráfico de la red y del ancho de banda que se tenga.

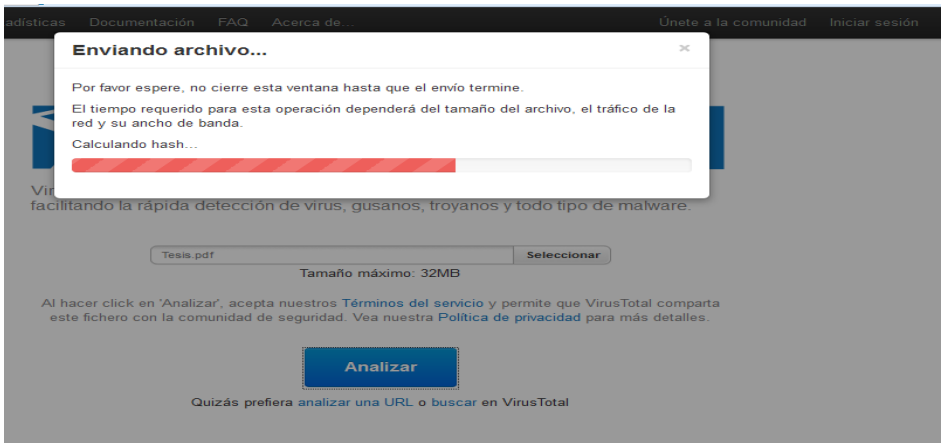


Figura 6. 70: Envió del Documento a ser analizado.

Una vez que el documento PDF ha sido analizado lo primero que podemos apreciar son los detalles o información básica del documento como es: el tamaño, el nombre, el tipo, la cantidad de virus detectados una vez que el documento ha sido analizado por diferentes software Anti-Malware y la fecha en la q el archivo fue subido.

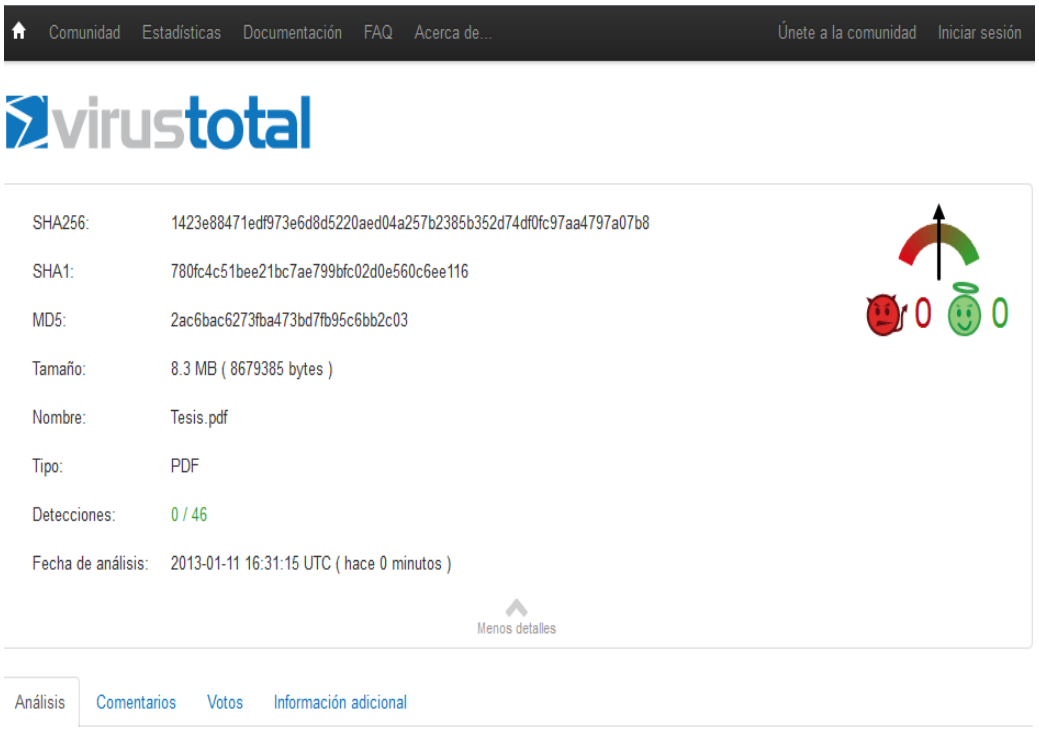


Figura 6. 71: Detalles del Documento analizado.

Lo que se muestra en la figura 6. 72 es una lista de los Software Antivirus con los cuales el documento PDF fue analizado. En la parte de resultado se mostraría el nombre del virus que posee el documento en el caso de que el Antivirus lo haya

identificado con alguno que exista en su base de datos y que como podemos ver en el documento Tesis.pdf no se ha encontrado ninguno ya que como se explicó con anterioridad lo que posee este documento es código JavaScript y código basura por lo que se puede decir que los resultados son los esperados.

En la parte de actualización se muestra la fecha en la que los antivirus que están realizando el análisis, fueron actualizados por última vez, cabe recalcar que en el caso de que el documento Tesis.pdf hubiera tenido incrustado un virus, no todos los software antivirus lo hubieran podido reconocer y en el caso de que más de uno lo hubiera reconocido, no aparecería con el mismo nombre, lo cual se debe en gran parte a que no todas las bases de datos de los antivirus son iguales y a que los software antivirus son constantemente actualizados pero en diferentes fechas.

Análisis | Comentarios | Votos | Información adicional

Antivirus	Resultado	Actualización
Agnitum	-	20130111
AhnLab-V3	-	20130111
AntiVir	-	20130107
Antiy-AVL	-	20130111
Avast	-	20130111
AVG	-	20130111
BitDefender	-	20130111
ByteHero	-	20130110
CAT-QuickHeal	-	20130111
ClamAV	-	20130111
Commtouch	-	20130111
Comodo	-	20130111

Figura 6. 72: Lista de Antivirus con los que el Documento fue analizado.

Además del informe del análisis con varios software antivirus, también nos muestra información adicional sobre el contenido del documento, como por ejemplo: las imágenes y los objetos existentes y las propiedades que tiene cada uno de ellos.

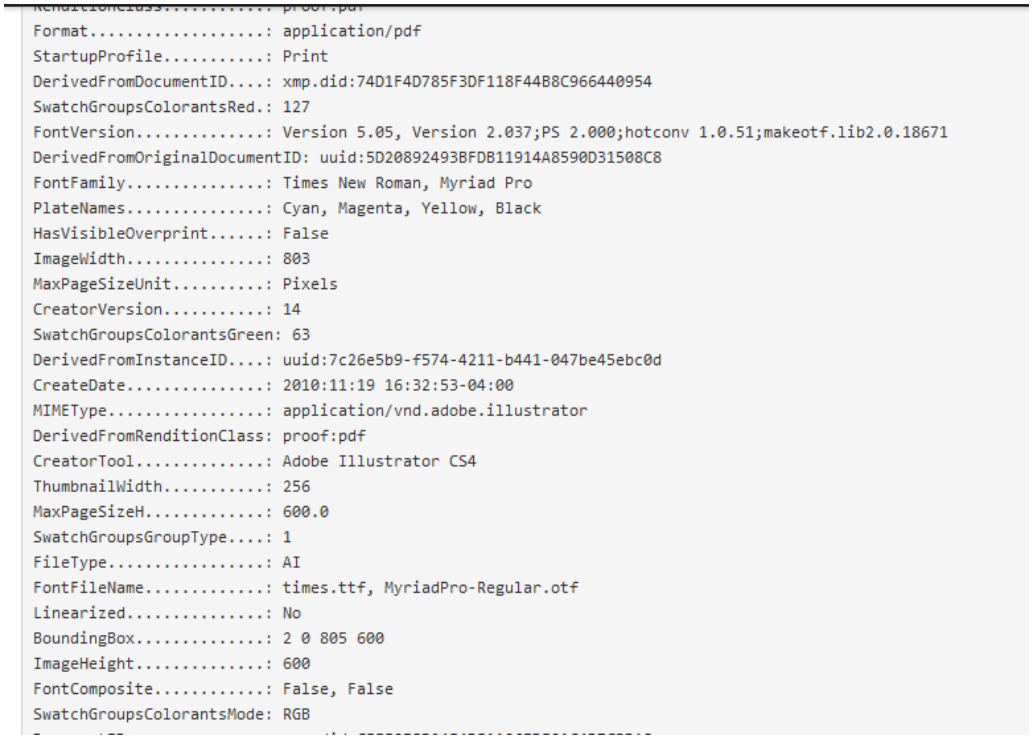


Figura 6. 73: Información Adicional del Documento.

Las imágenes que se van a mostrar a continuación pertenecen al documento Tesis.pdf, las mismas que fueron analizadas utilizando el servicio de internet Virus Total. El objetivo de analizar el mismo documento tres veces es para poder mostrar que en el informe detallado del análisis existe una parte en donde nos indica un cierto nivel del contenido JavaScript que posee el documento. En la primera imagen el documento casi no contiene código JavaScript sino más bien se puede decir que lo que reconoce son los objetos creados, por lo que el nivel de JavaScript es 1. En la segunda imagen se creó una función la cual se ejecuta cuando el documento va a cerrarse y la función que cumple es rotar el documento a la derecha, aquí el nivel de JavaScript es 3. En la tercera imagen se incrementó tres funciones con código basura, aquí el nivel de JavaScript es 6.

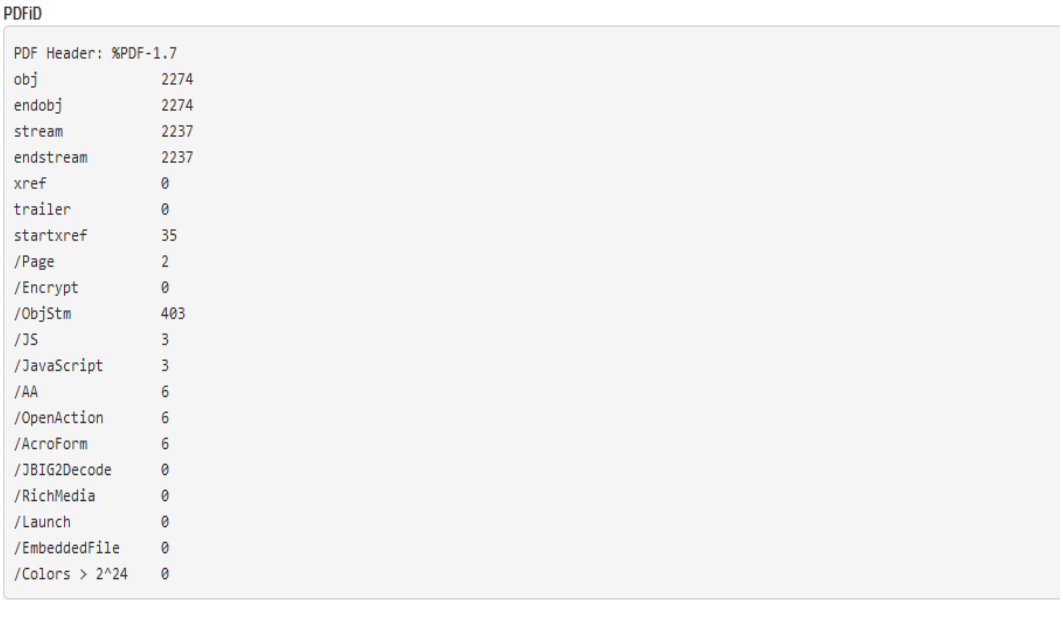
PDFiD

```
PDF Header: %PDF-1.7
obj              1284
endobj           1284
stream           1279
endstream        1279
xref             0
trailer          0
startxref        4
/Page            1
/Encrypt         0
/ObjStm          39
/JS              1
/JavaScript      1
/AA              1
/OpenAction      0
/AcroForm        2
/JBIG2Decode     0
/RichMedia       0
/Launch          0
/EmbeddedFile    0
/Colors > 2^24   0
```

ClamAV PUA Engine

Possibly Unwanted Application. While not necessarily malicious, the scanned file presents certain characteristics which depending on the user policies and environment may or may not represent a threat. For full details see: http://www.clamav.net/support/faq/pua.

Figura 6. 74: Descripción del contenido JavaScript del Documento.



PDFiD

```
PDF Header: %PDF-1.7
obj              2274
endobj           2274
stream           2237
endstream        2237
xref             0
trailer          0
startxref        35
/Page            2
/Encrypt         0
/ObjStm          403
/JS              3
/JavaScript      3
/AA              6
/OpenAction      6
/AcroForm        6
/JBIG2Decode     0
/RichMedia       0
/Launch          0
/EmbeddedFile    0
/Colors > 2^24   0
```

ClamAV PUA Engine

Possibly Unwanted Application. While not necessarily malicious, the scanned file presents certain characteristics which depending on the user policies and environment may or may not represent a threat. For full details see: http://www.clamav.net/support/faq/pua.

Figura 6. 75: Descripción del contenido JavaScript del Documento.

PDFiD

```
PDF Header: %PDF-1.7
obj              2286
endobj           2286
stream           2243
endstream        2243
xref             0
trailer          0
startxref        36
/Page            3
/Encrypt         0
/ObjStm          404
/JS              6
/JavaScript      6
/AA              7
/OpenAction      7
/AcroForm        7
/JBIG2Decode     0
/RichMedia       0
/Launch          0
/EmbeddedFile    0
/Colors > 2^24   0
```

ClamAV PUA Engine

Possibly Unwanted Application. While not necessarily malicious, the scanned file presents certain characteristics which depending on the user policies and environment may or may not represent a threat. For full details see: http://www.clamav.net/support/faq/pua.

Figura 6. 76: Descripción del contenido JavaScript del Documento.

Si nos fijamos en la parte del código JavaScript de la figura 6. 74, figura 6. 75, figura 6. 76 El resultado de la detección del JavaScript varia cada vez que el documento es analizado con el servicio web Virus Total, este tipo de cambios se debe a que en el documento se le iba incrementando funciones JavaScript que no precisamente cumplen una función determinada en el documento, o causan algún daño sino que simplemente fueron utilizados como pruebas para analizar el comportamiento del Servicio web, y a su vez poder comprobar la efectividad en cuanto a la detección de JavaScript se refiere.

Adicional al nivel de JavaScript que se detecta en el análisis del Documento Tesis.pdf, al finalizar el análisis se pudo observar el siguiente mensaje: "Existen Aplicaciones Posiblemente no deseados. El código encontrado si bien no es necesariamente malicioso, el archivo escaneado presenta ciertas características que en función de las directivas de usuario y el medio ambiente puede no representar una amenaza".

Este ejemplo nos muestra que aun cuando un documento PDF no contenga un virus especifico, puede tener código Java Script que dependiendo de las funciones que contenga el documento puede llegar a causar daños en el archivo o en el computador.

PROPUESTA, cumplimiento del cuarto objetivo

El objetivo cuarto fue cumplido, ya que se realizó las pruebas respectivas para conocer el funcionamiento del análisis heurístico de malware utilizando el servicio de internet Virus Total y un documento PDF creado con anterioridad, el cual contenía código javascript. Después de subir el documento a éste sitio web se obtuvo un análisis detallado del documento.

Análisis del documento Tesis.pdf y Prueba.pdf utilizando el Software antivirus AVAST.

Antes de analizar los documentos Tesis.pdf y Prueba.pdf con el software antivirus AVAST, se analizó el documento Prueba.pdf con el servicio de internet Virus Total, al análisis con este servicio fue necesario para poder comparar el nivel de JavaScript de los dos documentos.

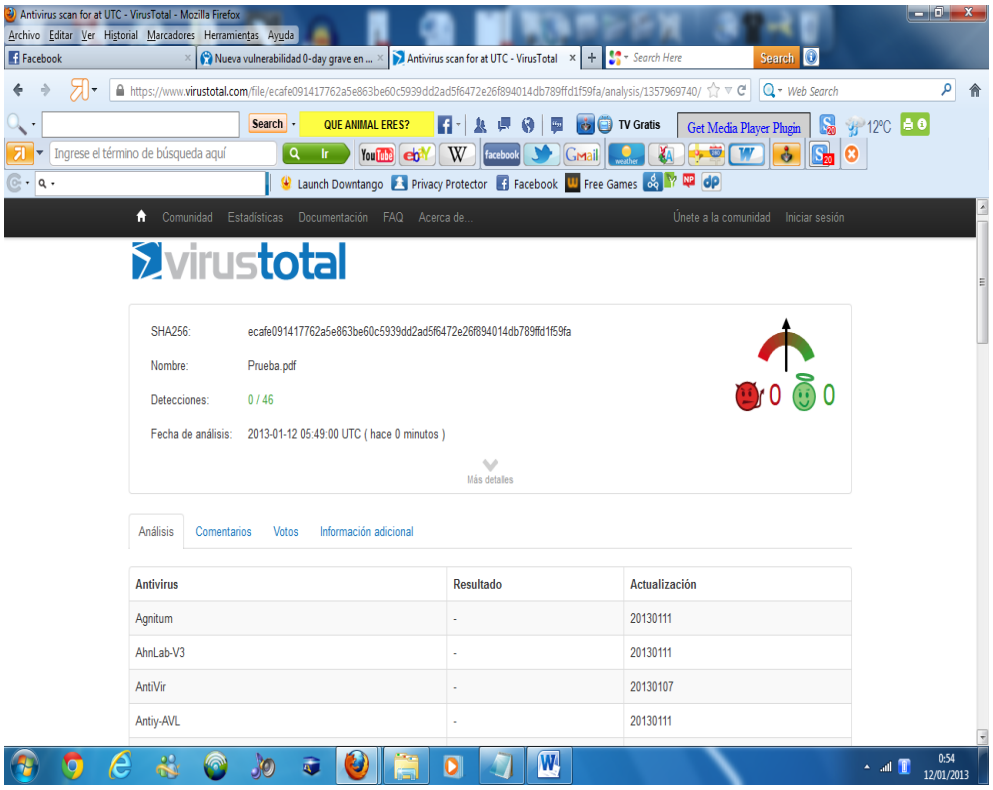


Figura 6. 77: Análisis del documento Prueba.pdf.

Como se puede apreciar en la figura 6. 77 en el documento Prueba.pdf no se detectó ningún tipo de malware, ya que al igual que en el documento Tesis.pdf lo único que contiene es código JavaScript, objetos y funciones.

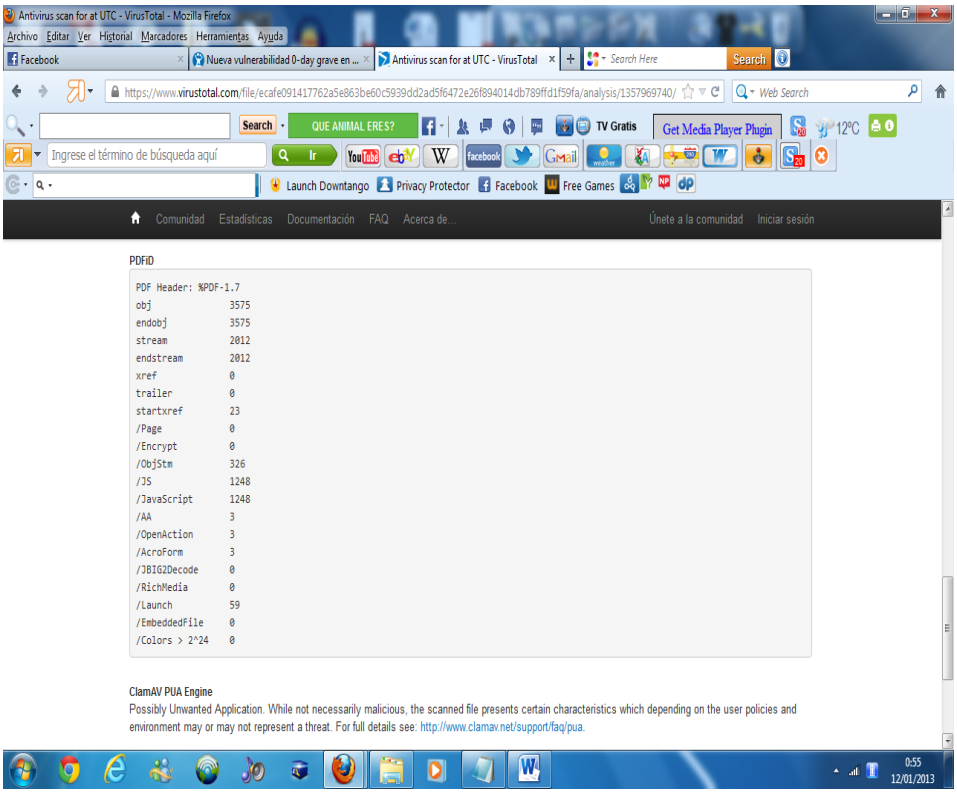


Figura 6. 78: Detalles de contenido JavaScript del documento Prueba.pdf.

El resultado del análisis nos muestra que el contenido de JavaScript del documento Prueba.pdf es superior a la del documento Tesis.pdf, lo cual se debe a que el documento Prueba.pdf contiene más objetos y código basura que el otro documento, el nivel de código JavaScript en este caso es de 1248, que es una enorme diferencia en comparación con el documento tesis.pdf cuyo máximo nivel era 6.

Una vez realizado la comparación del contenido de código JavaScript que posee cada documento se va analizar los dos documentos por separado utilizando en software antivirus AVAST para ver si existe alguna anomalía o si al analizar los dos documentos PDF los resultados son los mismos.

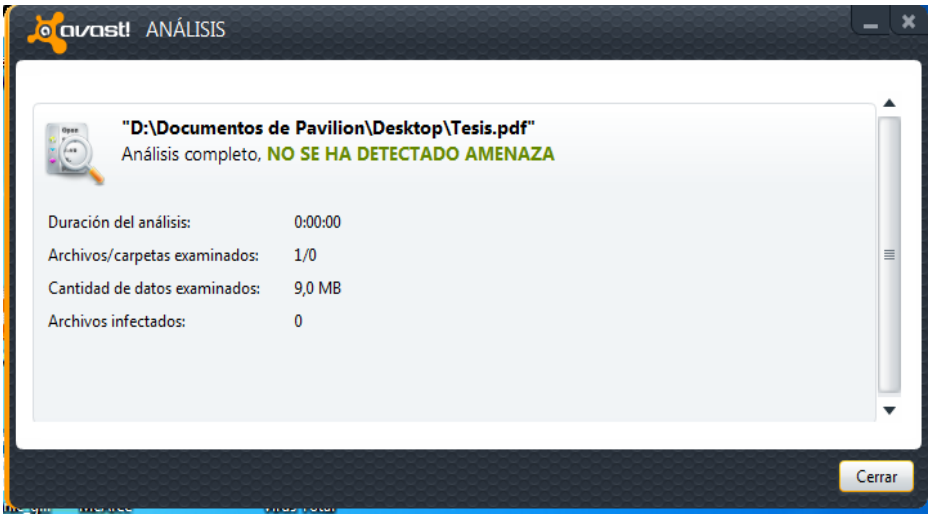


Figura 6. 79: Análisis del documento Tesis.pdf utilizando AVAST.

Después de analizar el documento Tesis.pdf el resultado es el siguiente: en el análisis completo no se ha detectado ningún tipo de amenaza, la cantidad de archivos/carpetas analizados 1/0, significa que se ha mandado analizar un archivo y ninguna carpeta, la cantidad de datos examinados es 9,0 MB, y por último los archivos infectados 0.

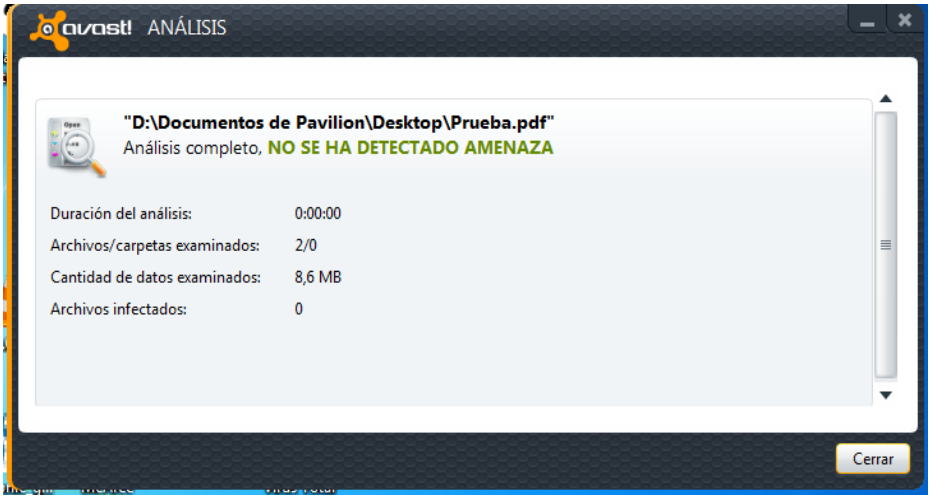


Figura 6. 80: Análisis del documento Prueba.pdf utilizando AVAST.

Después de analizar el documento Prueba.pdf el resultado es similar a la del análisis del documento Tesis.pdf, con una excepción que se presenta en la cantidad de archivos/carpetas analizados 2/0. Lo cual no es real puesto que únicamente se ha mandado a examinar un solo documento PDF.

Recordemos los resultados obtenidos en la figura 6. 76 y la figura 6. 78 en donde la diferencia del contenido de código JavaScript del documento Prueba.pdf era superior

al compararlo con el documento Tesis.pdf. De una forma completamente diferente el resultado del análisis utilizando AVAST muestra esa gran diferencia al escanear ambos documentos, ya que como podemos observar en la figura 6. 79 el documento Tesis.pdf no presenta ninguna anomalía, en cambio en la figura 6. 80 El documento Prueba.pdf aparece como si se hubiera mandado a escanear dos documentos, este resultado se debe al gran contenido de código JavaScript que posee el documento Prueba.pdf, que si bien el antivirus AVAST no lo detecta como virus y tampoco muestra detalladamente los resultados del análisis de alguna anomalía, lo que hace es indicar que el número de archivos analizados fueron dos cuando en realidad fue uno.

PROPUESTA, cumplimiento del Objetivo General

Como se puede observar se ha realizado el análisis heurístico de malware a través de la aplicación de dos técnicas que son el servicio de internet llamado Virus Total y el software antivirus AVAST con los cuales se han determinar el grado de efectividad en la detección de documentos PDF maliciosos y documentos PDF que contienen JavaScript.

Documento PDF con Virus

No siempre se tendrá la ventaja de que un documento PDF contenga únicamente código JavaScript inofensivo, habrán ocasiones en las que los documentos PDF tenga incrustados funciones que causen algún daño en el documento o en el computador, además hay que tomar en cuenta que existen varios códigos maliciosos que pueden ser incrustados en un documento PDF y que dependiendo del virus puede llegar a causar danos realmente graves en los computadores.

En el Internet existen páginas Web en las que se encuentran documentos PDF maliciosos a disposición de los usuarios, ya sea para que tengan una idea sobre el daño que pueden llegar a causar los documentos infectados, o a su vez utilizarlos en algún tipo de ataque o para dar a conocer el funcionamiento y como pueden ser analizados, para tener una mejor idea sobre el daño que puede llegar a causar. Una de las páginas web en la que se puede encontrar este tipo de archivos es: http://foros.softonic.com/seguridad/nueva-vulnerabilidad-0-day-grave-adobe-acrobat-

pdf-malicioso-ejemplo-109476#post856237. Donde se encontró un documento cuyo nombre es 96a8ad.pdf el mismo que va a ser utilizado a continuación para poder realizar un minucioso análisis y así observar la diferencia entre un documento PDF que contenga código JavaScript y el documento PDF que contiene un código malicioso.

Para el análisis al igual que el documento PDF Tesis.pdf, se utilizó el servicio de internet Virus Total.

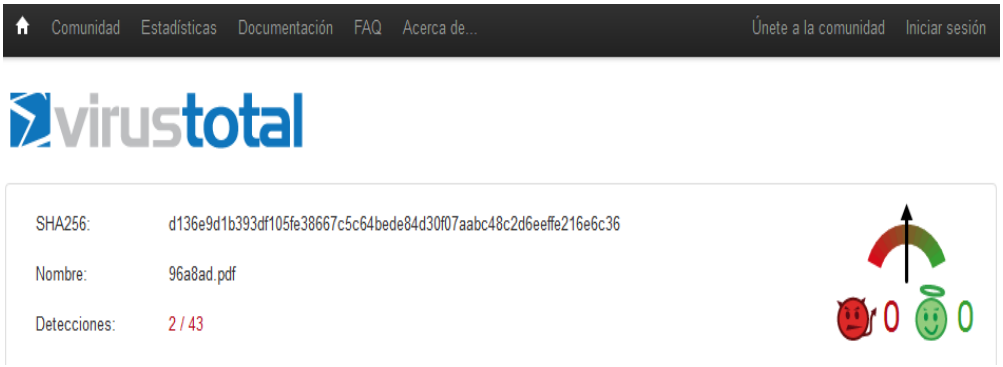


Figura 6. 81: Análisis del documento 96a8ad.pdf.

En la información básica del documento analizado se pudo observar que se han detectado dos códigos maliciosos de cuarenta y tres analizados.

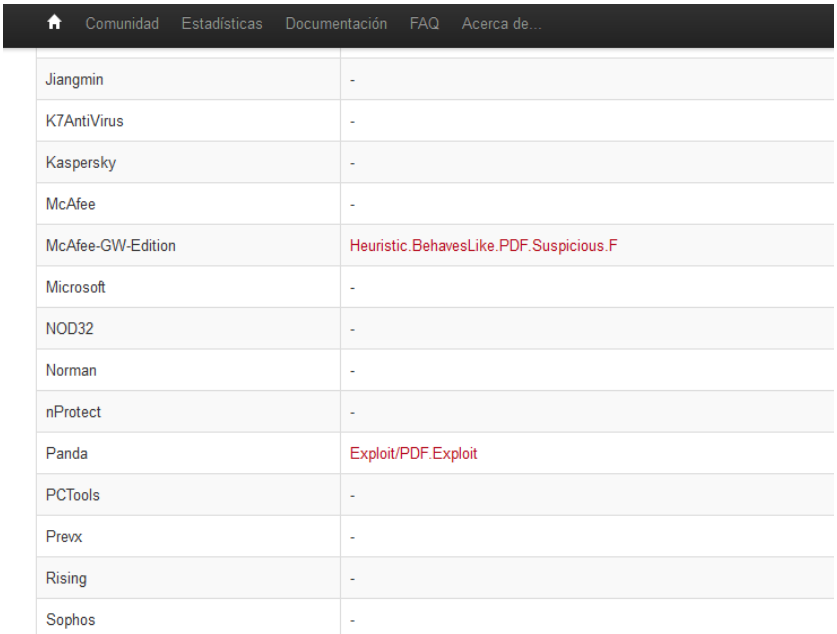


Figura 6. 82: Lista de virus detectados en el documento 96a8ad.pdf.

Como se explicó anteriormente este servicio de internet tiene la ventaja de que el documento PDF es analizado por varios software antivirus. En la figura 6. 81 se observó que el número de virus encontrados eran dos, los mismos que fueron detectados por McAfee con el siguiente nombre: Heuristic.BehavesLike.PDF.Suspicious.F, y por el antivirus Panda con un nombre diferente que es: Exploit/PDF.Exploit.

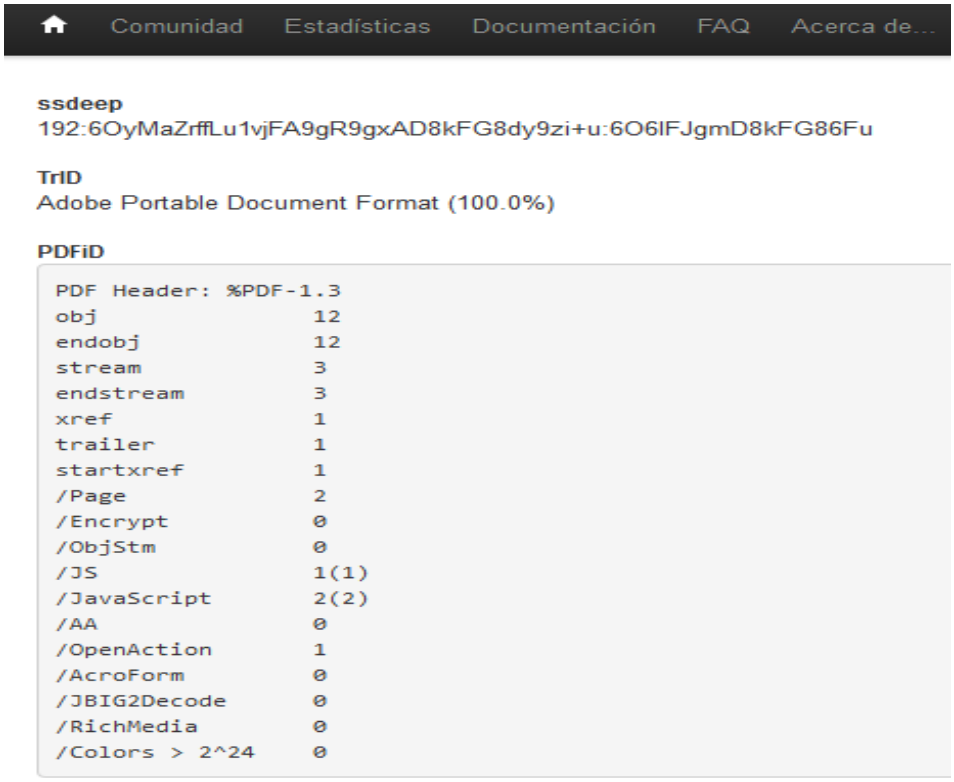


Figura 6. 83: Nivel de código JavaScript detectada en el documento 96a8ad.pdf.

En el informe detallado del análisis del documento 96a8ad.pdf se puede observar que en la parte de código JavaScript se han detectado dos anomalías que hacen referencia a los dos virus detectados que ya fueron explicados con anterioridad. El documento analizado no contiene código JavaScript como funciones u objetos, por lo que en la parte inferior no se presentó el mensaje de que el documento contenga código que llegue a causar algún daño en el archivo o el computador.

No todos los antivirus detectaron que el documento 96a8ad.pdf contenía código malicioso porque cada base de datos de los antivirus funciona de forma distinta para

el reconocimiento de código malicioso, algunos se basan en el reconocimiento d firmas y otros en algoritmos heurísticos y además las actualizaciones de cada antivirus se demora un cierto periodo de tiempo mientras que nuevos virus van apareciendo y causando daño sin que puedan ser reconocidos en un principio.

CUMPLIMIENTO DEL SEGUNDOOBJETIVO ESPECÍFICO

Analizar un ambiente de pruebas utilizando correos electrónicos para el envió de documentos PDF maliciosos.

El segundo objetivo especifico no se pudo cumplir debido a que no se podía conocer la reacción de los funcionarios de la Municipalidad de Ambato en el momento en que reciban un documento PDF, es decir el comportamiento de los funcionarios variarían constantemente cada vez que reciban algún tipo de documento y la información adquirida no sería verídica.

El segundo objetivo fue reemplazado por uno nuevo que es "Crear, Analizar y Comparar un documento PDF que contenga código javascript con otro que contenga código malicioso utilizando alguna técnica de análisis heurístico de malware".

Para el cumplimiento del objetivo planteado se tuvo que realizar los siguientes pasos:

- Se tuvo que aprender a utilizar el software Adobe Acrobat.
- Se creó un documento PDF utilizando formularios y objetos, los cuales contenían código JavaScript.
- Del internet se descargó un documento PDF que contenía código malicioso.
- Los dos documentos PDF fueron analizados utilizando el servicio de internet Virus Total y el software antivirus AVAST.
- Se comparó los resultados adquiridos de los dos análisis y se llegó a distintas conclusiones que fueron explicadas anteriormente.

6.8. Conclusiones y Recomendaciones

6.8.1. Conclusiones

- Cada software antivirus funciona de diferente forma, algunos utilizan las bases de datos basados en firmas y otros utilizan la heurística para su

autoaprendizaje, debido a esto no todos los antivirus son capaces de detectar documentos PDF con JavaScript o algún tipo de código malicioso.

- Después de investigar el funcionamiento de cada algunos de los software antimalware se llego a la conclusión de que el servicio de internet Virus Total es la técnica más recomendada, ya que permite obtener un informe aun mas detallado del análisis de un documento PDF que contenga código malicioso o código javascript, debido a que el archivo es analizado por varios software antivirus, sin que tenga la necesidad de que los tenga instalados en el computador.
- El programa Adobe Acrobat permite introducir en un documento PDF código javascript o código malicioso, ya que al crear un documento PDF con esta herramienta permite utilizar formularios, los cuales contienen objetos en los que se puede crear funciones utilizando javascript.
- Un atacante no necesariamente necesita tener conocimientos sobre javascript para crear un documento PDF malicioso, porque al utilizar formularios y objetos existen otras formas, como por ejemplo, que al realizar alguna acción sobre algún objeto, el navegador sea direccionado hacia alguna pagina web que contenga malware, además que en internet se pueden encontrar funciones javascript listas para ser utilizadas.
- Un documento PDF puede contener código javascript (funciones) que no necesariamente tiene que ser código malicioso.
- El correo electrónico es la herramienta principal que se utiliza en la municipalidad por el cual se encuentran expuestos los computadores para el contagio de malware.
- Con el servicio de internet Virus Total un documento PDF que contenga código javascript no será detectado por los software antivirus como malware, pero si detectara el código y mostrara un mensaje en el cual se menciona que el documento contiene código javascript y que se debe tener precaución porque no se sabe si se ejecutara algún de las funciones que se encuentran en el documento.

6.8.2. Recomendaciones

- Tener instalado en cada computador más de un software antivirus siempre y cuando sean compatibles.
- Escanear todo tipo de documentos y carpetas antes de ser abiertas.
- Parchar (actualizar) constantemente Adobe y deshabilitar momentáneamente el JavaScript en adobe Reader cuando se tengan documentos extraños.
- El servicio web virus total es una buena opción para el escaneo de un documento PDF que contiene código JavaScript.
- Utilizar un visor de PDF alternativo cuando existan dudas sobre el contenido del documento, existen otro tipo de programas que cumplen la misma función como: Foxit PDF Reader o Nitro PDF Reader.
- Brindar capacitaciones cada cierto tiempo para que los usuarios tengan conocimientos sobre las nuevas formar de contagio de código malicioso y puedan prevenirlo, o por lo menos disminuir los daños.

CUMPLIMIENTO DEL OBJETIVO GENERAL

Determinar el análisis heurístico de malware para que no permita el acceso de documentos PDF maliciosos en el Gobierno Autónomo Descentralizado Municipalidad de Ambato.

Con la investigación realizada sobre como los software antivirus utilizan la heurística para la detección de documentos PDF maliciosos, y la creación de un documento PDF el cual contiene código javascript, mas un documento PDF encontrado en internet el cual contenía código malicioso, se pudo realizar el análisis heurístico de malware. Los resultados obtenidos y previamente explicados permiten dar a conocer a los funcionarios de la Municipalidad las medidas de seguridad que se deben tomar, por lo que se puede concluir que el Objetivo General del Capitulo I se ha cumplido satisfactoriamente.

6.9.Bibliografía

- **Libros**

o TORRES, Juan LLORIS, Antonio PRIETO, Alberto (2004, Pág. 1), Informática, *Introducción a la informática.* Tercera Edición. MCGRAW-HILL/INTERAMERICANA de España S.A.U.

o CHIAVENATO, Idalberto (2006, Pág. 110), Información, *Introducción a la Teoría General de la Administración.* Séptima Edición. MCGRAW-HILL/INTERAMERICANA de España S.A.U.

o FERRELL O. C. HIRT, Geoffrey (2004, Pág. 121), Información, *Introducción a los Negocios en un Mundo Cambiante.* Cuarta Edición. MCGRAW-HILL/INTERAMERICANA de España S.A.U.

o CZINKOTA, Michael y KOTABE, Masaaki (2001, Pág. 115), Información, *Administración de Mercadotecnia*. Segunda Edición. International Thomson Editores.

- **Internet**

o Contextualización

- Contagio Malware Dump. Recuperado el 03-03-2013 y disponible en http://contagiodump.blogspot.com/ Sitio web donde existe información sobre contagios.
- Intrusos disfrazan malware de documentos enviados por impresoras inteligentes. Recuperado el 03-03-2013 y disponible en http://www.seguridad.unam.mx/noticias/?noti=4891 Sitio Web donde existe información de malware en documentos.

o Informática

- Definición de Informática. Recuperado el 05-10-2011 y disponible en http://www.mastermagazine.info/termino/5368.php Sitio Web donde existe información sobre la ciencia de la computación.

- La informática y el tratamiento de la información. Recuperado el 05-10-2011 y disponible en http://peremarques.pangea.org/INFMULTI.htm Sitio Web donde existe información sobre las computadoras en general.

o Seguridad Informática

- Definición de la seguridad informática. Recuperado el 28-10-2011 y disponible en http://www.ciberhabitat.gob.mx/museo/cerquita/redes/seguridad/intro.htm Sitio Web donde existe información sobre las redes y las seguridades.
- Diccionario de informática. Recuperado el 28-10-2011 y disponible en http://www.alegsa.com.ar/Dic/seguridad%20informatica.php Sitio Web donde existe información sobre conceptos básico.
- Seguridad Informática. Recuperado el 28-10-2011 y disponible en http://www.segu-info.com.ar/logica/seguridadlogica.htm Sitio Web donde existe información sobre tipos de seguridades y niveles en la información.

o Ataques Informáticos

- Ataques informáticos. Recuperado el 06-11-2011 y disponible en https://www.evilfingers.com/publications/white_AR/01_Ataques_informaticos.pdf Sitio Web donde existe información sobre debilidades de seguridad comúnmente explotadas.
- Ataques informáticos. Recuperado el 06-11-2011 y disponible enhttp://ataquesinformaticos.blogspot.com/Sitio Web donde existe información sobre tipos de intrusos o atacantes.

o Software Anti-malware

- Antimalware. Recuperado el 07-11-2011 y disponible enhttp://www.pandasecurity.com/spain/enterprise/solutions/security-appliances/anti-malware.htmSitio Web donde existe información sobre tipos de código malicioso.
- Funcionamiento de un los software antimalware. Recuperado el 07-11-2011 y disponible enhttp://www.infomalware.net/t460-heuristica-

antivirus-deteccion-proactiva-de-malwareSitio Web donde existe información sobre el funcionamiento de la heurística en los antivirus.

- Análisis heurístico de malware
  - Análisis heurístico: detectando malware desconocido. Recuperado el 28-10-2011 y disponible en http://www.eset-la.com/centro-amenazas/articulo/analisis-heuristico-detectando-malware-desconocido/1625 Sitio Web donde existe información sobre el funcionamiento de la tecnología de los software antivirus.
  - Funcionamiento del análisis heurístico. Recuperado el 28-10-2011 y disponible en http://www.infomalware.net/t460-heuristica-antivirus-deteccion-proactiva-de-malware Sitio Web donde existe información sobre el funcionamiento de la heurística en la detección de malware.
  - Definición del análisis heurístico. Recuperado el 29-10-2011 y disponible en http://www.elrinconcito.com/DiccAmpliado/heuristico.htm Sitio Web donde existe información sobre definición de la heurística.
- Virus
  - ¿Qué es un virus informático? .Recuperado el 07-11-2011 y disponible en http://www.masadelante.com/faqs/virus Sitio Web donde existe información sobre la definición del virus informático.
  - ¿Qué es un virus informático? .Recuperado el 07-11-2011 y disponible en http://www.desarrolloweb.com/articulos/2176.php Sitio Web donde existe información sobre todo lo que se puede saber sobre los virus y troyanos informáticos.
  - ¿Qué es un virus informático? .Recuperado el 07-11-2011 y disponible en http://www.infospyware.com/articulos/%C2%BFque-son-los-virus-informaticos/ Sitio Web donde existe información sobre el funcionamiento básico de un virus.
- Gusanos
  - ¿Qué es un worm o gusano informático? .Recuperado el 07-11-2011 y disponible enhttp://www.masadelante.com/faqs/que-es-un-gusanoSitio

Web donde existe información sobre la definición de worm o gusano informático.

- Antimalware. Recuperado el 02-03-2011 y disponible enhttp://www.pandasecurity.com/ecuador/enterprise/solutions/security-appliances/anti-malware.htmSitio Web donde existe información sobre códigos maliciosos y el software antimalware Panda.
- Gusanos informáticos. Recuperado el 07-11-2011 y disponible enhttp://www.pandasecurity.com/spain/enterprise/security-info/classic-malware/worm/Sitio Web donde existe información sobre que hacen, como funcionan, medidas de prevención etc.

o Malware no replicativo

- Análisis heurístico para la detección de malware. Recuperado el 07-11-2011 y disponible en http://www.esetla.com/pdf/prensa/informe/analisis_heuristico_detectando_malware_desconocido.pdfSitio Web donde existe información sobre la forma en la que se detecta el malware desconocido.

o Información

- Definición de información. Recuperado el 07-11-2011 y disponible en http://www.promonegocios.net/mercadotecnia/definicion-informacion.html Sitio Web donde existe información sobre la definición de información desde diferentes puntos de vista.

o Formatos de Archivos Portables

- Tipos de archivos. Recuperado el 02-03-2013 y disponible enhttp://aprendeenlinea.udea.edu.co/lms/moodle/file.php/464/Modulo1/TiposArchivos.pdfSitio Web donde existe información sobre la descripción de varios tipos de archivos.
- ¿Qué es un PDF? .Recuperado el 07-11-2011 y disponible enhttp://www.masadelante.com/faqs/pdfSitio Web donde existe información sobre que es un PDF y como funciona.

- Tipos de archivos. Recuperado el 02-03-2013 y disponible enhttp://www.hipertexto.info/documentos/archivos.htmSitio Web donde existe información sobre las definiciones de cada uno.

o Vulnerabilidades de los Archivos Portables

- Definiciones. Recuperado el 04-11-2011 y disponible en http://www.pandasecurity.com/spain/homeusers/security-info/glossary/ Sitio Web donde existe información sobre las técnicas relacionadas con los virus y antivirus.
- Archivos portables. Recuperado el 04-11-2011 y disponible en http://www.latinoseguridad.com/LatinoSeguridad/PCP/Virpng.shtml Sitio Web donde existe información sobre los diferentes archivos que pueden contener código malicioso.
- Vulnerabilidades criticas en Adobe Reader. Recuperado el 04-11-2011 y disponible en http://www.vsantivirus.com/vul-adobe-030107.htm Sitio Web donde existe información sobre Adobe Acrobat y las vulnerabilidades detectadas.

o Documentos PDF Maliciosos

- Documento PDF infectaron más Pc que otros archivos en el 2010. Recuperado el 04-11-2011 y disponible enhttp://www.unazonageek.com/2011/02/documentos-pdf-maliciosos-infectaron.htmlSitio Web donde existe información sobre antecedentes de computadores que se han infectado con documentos PDF.
- Archivos PDF podrían contener código malicioso. Recuperado el 04-11-2011 y disponible enhttp://www.pcworld.com.mx/Articulos/7094.htmSitio Web donde existe información sobre los informes encontrados de los contagios.
- Archivos PDF maliciosos que se convierten en el vector de ataque. Recuperado el 04-11-2011 y disponible enhttp://www.blogantivirus.com/archivos-pdf-maliciosos-se-convierten-en-el-vector-de-ataque-de-eleccion-segun-informeSitio Web donde existe

información sobre la infección de los documentos PDF y un informe detallado de algunos casos detectados.

- Robo de Información Personal
  - Robo de información personal online. Recuperado el 07-11-2011 y disponible en http://www.eset-la.com/pdf/prensa/informe/robo_informacion_online.pdf Sitio Web donde existe información sobre técnicas para obtener información personal.
  - Robo de identidad. Recuperado el 07-11-2011 y disponible en http://alertaenlinea.gov/articulos/s0005-robo-de-identidad Sitio Web donde existe información sobre las medidas de prevención para evitar el robo de información.
  - Alarmante aumento de robo de información a través de redes sociales como Twitter o Facebook. Recuperado el 07-11-2011 y disponible en http://www.biobiochile.cl/2010/02/06/alarmante-aumento-de-robo-de-informacion-personal-a-traves-de-redes-sociales-como-twitter-o-facebook.shtml Sitio Web donde existe información sobre los crímenes que se han cometido en las redes sociales.
- Daño a equipos informáticos
  - Definición de delito informático. Recuperado el 02-03-2013 y disponible enhttp://www.delitosinformaticos.info/delitos_informaticos/definicion.htmlSitio Web donde existe información sobre definición y características principales.
  - Legislación sobre delitos informáticos. Recuperado el 07-11-2011 y disponible enhttp://www.monografias.com/trabajos/legisdelinf/legisdelinf.shtmlSitio Web donde existe información sobre los datos informáticos que se han encontrado en diferentes partes del mundo.
- Eliminar el contenido del Computador
  - Recuperación de archivos borrados. Recuperado el 07-11-2011 y disponible en http://www.wilkinsonpc.com.co/servicios/recuperar-

archivos-borrados.html Sitio Web donde existe información sobre que hacer cuando se llegan a borrar archivos del computador.

- Virus y antivirus. Recuperado el 07-11-2011 y disponible en http://www.monografias.com/trabajos18/virus-antivirus/virus-antivirus.shtml Sitio Web donde existe información sobre todo lo que se desea conocer con respecto a los virus.
- Efectos de los virus informáticos. Recuperado el 07-11-2011 y disponible en http://juanj2.blogs.com.gt/que-es-un-virus-informatico/efectos-de-los-virus-informaticos/ Sitio Web donde existe información sobre los diferentes tipos de daños que puede llegar a causar un virus.

o Heurística

- Heurística. Recuperado el 07-11-2011 y disponible en http://www.eset-la.com/pdf/prensa/informe/heuristica_antivirus_deteccion_proactiva_malware.pdf Sitio Web donde existe toda la información que necesita, desdelos conceptos mas básicos hasta el funcionamiento de un software antivirus.

o Metasploit

- Plataforma par test de intrusión. Recuperado el 15-01-2012 y disponible en http://www.genbeta.com/web/metasploit-framework-plataforma-para-tests-de-intrusion y http://thehackerway.com/2011/03/11/comandos-y-conceptos-basicos-metasploit-framework/ Sitio Web donde habla del funcionamiento de Metasploit.
- Comandos y conceptos básicos. Recuperado el 15-01-2012 y disponible en http://thehackerway.com/2011/03/11/comandos-y-conceptos-basicos-metasploit-framework/ Sitio Web donde habla del funcionamiento interno de Metasploit.

o Virus Total

- Documentación sobre el servicio Web. Recuperado el 10-01-2012 y disponible en https://www.virustotal.com/es/documentation/ Sitio Web donde se encuentra toda la información sobre el funcionamiento del Servicio Web.

- MDScan
  - El riesgo de malware en un documento pdf. Recuperado el 12/11/2011 http://www.symantec.com/connect/blogs/rise-pdf-malware Sitio Web donde explica como un pdf puede ser contagiado de código malicioso.
- Adobe Acrobat
  - Presentación en PDF la alternativa a PowerPoint. Recuperado el 03/01/2012 http://onsoftware.softonic.com/presentaciones-en-pdf Sitio Web donde encontrara información sobre las características de Adobe Acrobat.
- Sophos Antivirus
  - Objetivos de Seguridad y funcionamiento en general. Recuperado el 04-01-2012http://www.sophos.com/es-es/your-needs/security-goals.aspx Sitio Web donde explica todo el funcionamiento del software.

ANEXOS

Anexo 1. Encuesta Aplicada

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

LUGAR A ENCUESTAR: Gobierno autónomo descentralizado del ilustre Municipio de Ambato.

OBJETIVO DE LA ENCUESTA: Tener un amplio conocimiento el área de trabajo en donde se va a realizar la tesis para lograr los objetivos planteados.

Señores, su veracidad en las respuestas permitirá al grupo investigador desarrollar un trabajo real y efectivo. Agradecemos su colaboración y garantizamos absoluta reserva de su información.

CUESTIONARIO

1. ¿Tiene conocimiento de algunas técnicas que prevengan el contagio de virus a través de documentos PDF maliciosos?

   Si ☐ No ☐

2. ¿Conoce el método de cadenas y como funciona en la detección de código malicioso?

   Si ☐ No ☐

3. ¿Tiene alguna idea de la funcionalidad del chequeo de integridad en el análisis heurístico, que hace o como funciona?

   Si ☐ No ☐

4. ¿En el municipio de Ambato por alguna razón se ha utilizado ya sea los algoritmos de ordenamiento o búsqueda?

   Si ☐ No ☐

5. ¿El desencriptador genérico es una técnica que ayuda al análisis heurístico de malware, tiene algún conocimiento sobre esta técnica?

   Si ☐ No ☐

6. ¿Qué software antivirus tiene instalado en su computador?

   AVG ☐

   AVIRA ☐

   NOD 32 ☐

   Otro ☐

7. ¿Tiene algún conocimiento sobre los métodos reactivos para la detección de código malicioso, que hace o como funciona?

   Si ☐ No ☐

8. ¿Durante todo el tiempo que se encuentra trabajando en el Municipio de Ambato alguna vez ha sido víctima de algún tipo de ataque ya sea por Hackers, Crackers o algún otro tipo de ataque?

   Si ☐ No ☐

9. ¿Sabía usted que al abrir un documento, como Word, Excel, PowerPoint, Adobe, entre otros, Corre el riesgo de que su computador se infecte de algún tipo de código malicioso?

   Si ☐ No ☐

10. ¿Ah recibido a través del correo electrónico algún tipo de documentos, información basura o links a direcciones extrañas?

    Si ☐ No ☐

11. ¿Su computador se ha visto afectado por virus, gusanos, o información basura?

    Si ☐ No ☐

12. ¿Sabía usted que un archivo al contener código Java Script es más vulnerables a contagiarse de malware?

    Si ☐ No ☐

13. ¿Cuán segura se encuentra la información , datos, imágenes, videos, etc. En el Municipio de Ambato?

    Muy Buena ☐
    Buena ☐
    Regular ☐
    Mala ☐

14. ¿Qué tipo de computador utiliza para su trabajo?

    De escritorio ☐
    Portátil ☐

Anexo 2. Glosario de Términos

- **Aislamiento.-** Ejecutar programas con seguridad y de manera separada.
- **Análisis heurístico.-** Mediante un análisis detallado encontrar la solución a un problema que al parecer no tiene respuesta.
- **Caja de arena.-** Si algún archivo infectado intenta ejecutar un código malicioso o acción no autorizada dentro de la caja de arena, se enviará dicho archivo a la bóveda de archivos temporales, impidiendo el acceso de éste a funciones peligrosas.
- **Cifrado.-** Una forma de ocultar el código malicioso.
- **Código Malicioso.- C**ausa daños al computador como: virus, gusanos, troyanos.
- **Detección Genérica.-** De localizar la presencia de un virus aun cuando no existe vacuna para éste y es, por lo tanto, desconocido para el software antivirus.
- **Detección proactiva.-** Los algoritmos contienen instrucciones que le permiten sortear diversos mecanismos que poseen los códigos maliciosos para ocultar su comportamiento.
- **Detección reactiva.-** Método basado en firmas.
- **Empaquetamiento.-** Una forma de ocultar el código malicioso.
- **Heurística activa.-** Se trata de crear un entorno seguro y ejecutar el código de forma tal que se pueda conocer cuál es el comportamiento del código.
- **Heurística genérica.-** Se analiza cuán similar es un objeto a otro, que ya se conoce como malicioso y si es bastante parecido se lo detecta como código malicioso.
- **Heurística pasiva.-** Ese explora el archivo tratando de determinar qué es lo que el programa intentará hacer. Si se observan acciones sospechosas, éste se detecta como malicioso.
- **Malware.-** Código malicioso, virus, gusanos, troyanos, etc.
- **Malware no replicativo.-** Código que no causa daños al computador.

- **Software Antimalware.-** Software Antivirus.
- **Seguridad Física.-** Consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial.
- **Seguridad Lógica.-** Consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo.

Anexo 3. Resumen ejecutivo Informe Técnico-Manual de seguridad

REPÚBLICA DEL ECUADOR
GOBIERNO AUTÓNOMO DESCENTRALIZADO
MUNICIPALIDAD DE AMBATO

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

Tema:

MANUAL QUE GUIE A LOS FUNCIONARIOS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPALIDAD AMBATO PARA PARA DETERMINAR EL GRADO DE EFECTIVIDAD EN LA DETECCIÓN DE DOCUMENTOS PDF MALICIOSOS.

1. Introducción

Lo que busca con la creación de esta guía metodológica de análisis heurístico de malware es poder prevenir o minimizar los daños que puede llegar a causar al computador o incluso en la red, al ejecutar un documento PDF malicioso, por lo que se ha considerado las necesidades de los usuarios y por lo mismo se darán recomendación que les permita la detección de documentos PDF maliciosos en el Gobierno Autónomo Descentralizado Municipalidad de Ambato.

2. Resumen del Informe Técnico

Este documento va a detallar los resultados obtenidos una vez que se ha realizado el análisis heurístico de malware para la detección de documentos PDF maliciosos en el Gobierno Autónomo descentralizado, Municipalidad de Ambato.

Se realizó una investigación previa para luego realizar un análisis heurístico de malware y poder detectar documentos PDF que contengan código JavaScript que puede ser inofensivo o dañino y además para detectar documentos PDF con algún tipo de malware(código malicioso). Para poder realizar el análisis fue importante la recolección de información de la empresa ya que se basó en esto para la investigación respectiva, no fueron necesarios utilizar los recursos de la empresa, debido a que no se podía tener un resultado claro de las reacciones de cada uno de los usuarios del Área de Sistemas al recibir mediante el correo electrónico un documento PDF malicioso o que contenga código JavaScript.

Para poder realizar un análisis completo y detallado se partió desde cero, en primer lugar se tuvo que estudiar el funcionamiento de Adobe Reader y Acrobat ya que es el programa utilizado para la lectura de los documentos PDF en la municipalidad, lo más destacado de la investigación fue las vulnerabilidades que aún siguen existiendo en Adobe a pesar de los parches y actualizaciones que aparecen cada cierto periodo de tiempo. También se investigó el funcionamiento de algunos software antivirus en

donde se pudo concluir que el funcionamiento de cada antivirus es diferente ya que algunos utilizan bases de datos basados en firmas que significa que tienen que esperar la aparición de algún virus para luego estudiarlo y crear una firma la cual va ser incorporada al software antivirus mediante una actualización y así podrá recién detectar el virus, y la otra forma es mediante algoritmos heurísticos, que se refiere a que ya no es necesario depender de alguien para que el virus pueda ser detectado porque el antivirus a través de algoritmos crea su propia firma y la incorpora a la base de datos sin necesidad de una actualización. Con esto se logró crear un documento que contenga código Script que luego fue escaneado utilizando un servicio de internet llamado Virus Total, con el que se analizó dos documentos PDF, el primero que fue creado desde cero, y el segundo que se lo encontró en internet y también se lo analizo para después realizar las comparaciones respectivas y poder dar un informe detallado del funcionamiento de cada uno y así tener una idea más clara sobre los danos que pueden llegar a causar al archivo y al computador si no se tiene precaución. Con los resultados se pudo llegar a conclusiones que permiten dar recomendaciones para prevenir o por lo menos disminuir los daños en caso de que los funcionarios del municipio, ejecute documentos PDF peligrosos.

3. Definiciones

Primero se debe tener claro a cerca de lo que tratará esta guía, para ello se describe a continuación el significado más acertado para los términos o variables de la investigación realizada.

- Aislamiento.- Ejecutar programas con seguridad y de manera separada.
- Análisis heurístico.- Mediante un análisis detallado encontrar la solución a un problema que al parecer no tiene respuesta.
- Caja de arena.- Si algún archivo infectado intenta ejecutar un código malicioso o acción no autorizada dentro de la caja de arena, se enviará dicho archivo a la bóveda de archivos temporales, impidiendo el acceso de éste a funciones peligrosas.
- Cifrado.- Una forma de ocultar el código malicioso.

- Código Malicioso.- Causa daños al computador como: virus, gusanos, troyanos.
- Detección Genérica.- De localizar la presencia de un virus aun cuando no existe vacuna para éste y es, por lo tanto, desconocido para el software antivirus.
- Detección proactiva.- Los algoritmos contienen instrucciones que le permiten sortear diversos mecanismos que poseen los códigos maliciosos para ocultar su comportamiento.
- Detección reactiva.- Método basado en firmas.
- Empaquetamiento.- Una forma de ocultar el código malicioso.
- Heurística activa.- Se trata de crear un entorno seguro y ejecutar el código de forma tal que se pueda conocer cuál es el comportamiento del código.
- Heurística genérica.- Se analiza cuán similar es un objeto a otro, que ya se conoce como malicioso y si es bastante parecido se lo detecta como código malicioso.
- Heurística pasiva.- Ese explora el archivo tratando de determinar qué es lo que el programa intentará hacer. Si se observan acciones sospechosas, éste se detecta como malicioso.
- Malware.- Código malicioso, virus, gusanos, troyanos, etc.
- Malware no replicativo.- Código que no causa daños al computador.
- Software Antimalware.- Software Antivirus.
- Seguridad Física.- Consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial.
- Seguridad Lógica.- Consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo.

4. Detalle del análisis realizado

Heurística

La heurística ayuda a encontrar distintas soluciones a los problemas que a simple vista parece no tener, las soluciones las encuentra indagando y descubriendo nuevas formas para lo cual utiliza métodos. La heurística es considerada como una de las aplicaciones de la inteligencia artificial y como una herramienta para la resolución de problemas. La heurística se construye bajo reglas extraídas de la experiencia, y las respuestas generadas por tal sistema mejoran en la medida en que "aprende" a través del uso, y con esto logra aumentar su base de conocimiento o base de datos para que mejore su eficiencia en cuanto a la detección de código malicioso se refiere.

Tipos de heurística

- Heurística genérica: al mandar a analizar algún archivo lo que hace el antivirus es compara cuán similar es un objeto que podría o no virus con todos los que contiene en su base de datos, que ya se conocen como malicioso. Y si el contenido un archivo es lo suficientemente similar a un código malicioso que se encuentra en la base de datos, este será detectado como virus.
- Heurística pasiva: Con este método lo que se hace es explorar el archivo detenidamente, tratando de determinar qué es lo que el programa intentará hacer. Si se observan acciones sospechosas durante la exploración, éste archivo se detecta como malicioso.

- Heurística activa: Se trata de crear un entorno seguro y ejecutar el código de tal forma que se pueda conocer cuál es el comportamiento del código. Otros nombres para esta técnica son: "sandbox (caja de arena)", "virtualización" o "emulación".

Malware

Se le llama malware a todo archivo con contenido de carácter malicioso para un computador. Esto no se limita a los virus, pues existen otros muchos archivos capaces de causar daños importantes en un computador o en una red informática como son:

gusanos, troyanos, rootkit, spyware y otros elementos dañinos; es decir, todo tipo de códigos maliciosos.

Análisis heurístico de malware

Es una forma de buscar la solución de un problema mediante métodos no rigurosos como el método de cadenas, chequeo de integridad, algoritmos, desencriptador genérico, etc. A través de los cuales se puede obtener un informe donde se detalla el funcionamiento del software antivirus, dando respuestas en aquellas situaciones en donde los métodos reactivos no pueden darla, detectando un archivo malicioso desconocido para los antivirus.

Software Antivirus

El antivirus examina cada archivo respondiendo a la pregunta: ¿es un código malicioso?, el software antivirus ha evolucionado y los sistemas de detección empleados para identificar si un archivo es o no una amenaza ha cambiado, y ya no son los clásicos procedimientos de detección reactivos, basados en firmas, sino nuevas técnicas de detección proactivas, basadas en heurística.

Detección reactiva: base de firmas

El sistema es sencillo, se coteja cada archivo a analizar con la base de datos y, si existe en la base una firma que corresponda con el archivo, se identifica el archivo como código malicioso.

El proceso de generación de firmas se compone de los siguientes pasos:

- Aparece un nuevo código malicioso
- El laboratorio de la empresa antivirus recibe una muestra de ese código
- Se crea la firma para el nuevo código malicioso
- El usuario actualiza el producto con la nueva base de firmas y comienza a detectar el malware

Detección Proactiva:

El objetivo esencial de los algoritmos heurísticos es dar respuestas en aquellas situaciones en donde los métodos reactivos no pueden darla: tener la capacidad de detectar un archivo malicioso aunque una muestra de éste no haya llegado al laboratorio antivirus, y que aún no se tenga la firma correspondiente.

La detección proactiva es un agregado a la detección por firmas porque para una óptima protección son necesarios ambos métodos, y es como trabajan las soluciones antimalware en la actualidad.

Adobe

El formato PDF desarrollado por Adobe System, se ha convertido en el formato de archivo más utilizado para la distribución e impresión de documentos. Un archivo que se adhiere a la especificación de PDF consta de 4 secciones principales: una línea de cabecera con el número de versión de la especificación PDF, el cuerpo principal del documento, el cual consiste en objetos como texto, imágenes, fuentes, etc. Una tabla de referencias cruzadas con las compensaciones de los objetos dentro de los archivos incrustados, una tabla de referencias cruzadas con las compensaciones de los objetos dentro del archivo, y por último, una forma para un rápido acceso a la tabla de referencias cruzadas y otros objetos especiales.

Además de los datos estáticos, los objetos PDF también pueden contener código escrito en JavaScript. Esto permite a los autores de los documentos incorporar características avanzadas tales como la validación de formularios, contenidos multimedia, o incluso la comunicación con sistemas y aplicaciones externas. Desafortunadamente, los atacantes también pueden tomar ventaja de la versatilidad que ofrece JavaScript para la explotación de vulnerabilidades de ejecución de código arbitrario en la aplicación de la visualización del archivo PDF. A través de JavaScript el atacante puede lograr dos objetivos fundamentales: desencadenar la vulnerabilidad del código de poder, y desviar la ejecución de código de su elección.

Además de explotar alguna vulnerabilidad en el visor de PDF, los atacantes han aprovechado las características avanzadas de PDF como el Lanzamiento de opción, que se inicia automáticamente un incrustado ejecutable, o el URI e Ir a las opciones, lo cual puede abrir los recursos externos constituidos en la misma computadora.

Anexos del manual

- **Funcionamiento de la herramienta Virus Total**

Es un servicio en internet en el cual podemos analizar diferentes tipos de archivos y en especial documentos PDF y URL, para saber si se encuentran o no infectados por algún tipo de código malicioso, de esta manera facilita una rápida detección de virus, troyanos, entre otros tipos de código malicioso. Además hay que tomar en cuenta que esta herramienta ha sido reconocida como una de los mejores en la categoría Sitios Web Seguros.

Características

• Libre, servicio Independiente.
• Corre múltiples archivos.
• Actualizaciones automáticas en tiempo real.
• Resultados detallados de cada motor antivirus.
• Corre múltiples sitios web.

La utilización de esta herramienta es sumamente fácil, únicamente hay que ingresar a la siguiente dirección https://www.virustotal.com/, aquí se examinan archivos y URL para la detección de código malicioso, y lo único que hay que hacer es subir el archivo que va ser analizado o ingresar el URL en el caso de que se quiera analizar una dirección web, y enviarlo a analizar.

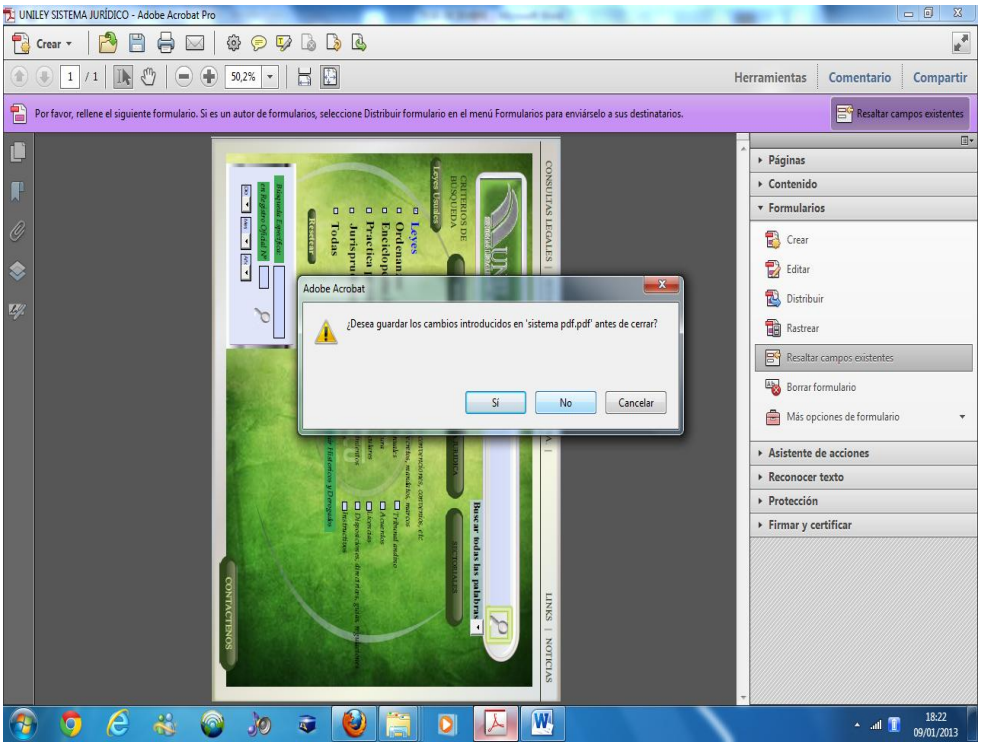
Con esta herramienta el resultado del análisis es específico y detallado, en el caso de que el documento enviado contenga algún tipo de código malicioso que pueda causar algún tipo de daño al archivo o al computador, será detectado por alguno de los software antivirus que posee este servicio, lo cual es una gran ventaja porque para un resultado eficaz es mejor que el archivo sea analizado por más de un software antivirus, debido a que cada uno funciona de forma diferente y si existiera algún virus este no será detectado por todos los antivirus.

En el caso de que el documento enviado contenga código JavaScript y no algún tipo de código malicioso, el documento no será detectado por ninguno de los software antivirus que posee este servicio, pero en la parte de detalles del documento se indicara la cantidad de código JavaScript que posee, y algunos detalles del contenido los formularios del documento como la cantidad de objetos, si existen imágenes, funciones etc. Además de mostrar un informe detallado del contenido del documento al final muestra un pequeño mensaje: "Existen Aplicaciones Posiblemente no deseados. El código encontrado si bien no es necesariamente malicioso, el archivo escaneado presenta ciertas características que en función de las directivas de usuario y el medio ambiente puede no representar una amenaza". Con este mensaje el usuario estará prevenido para cuando vaya a ejecutar el documento analizado y podrá tomar las debidas precauciones para que no cause ningún tipo de daño en el computador o en la red.

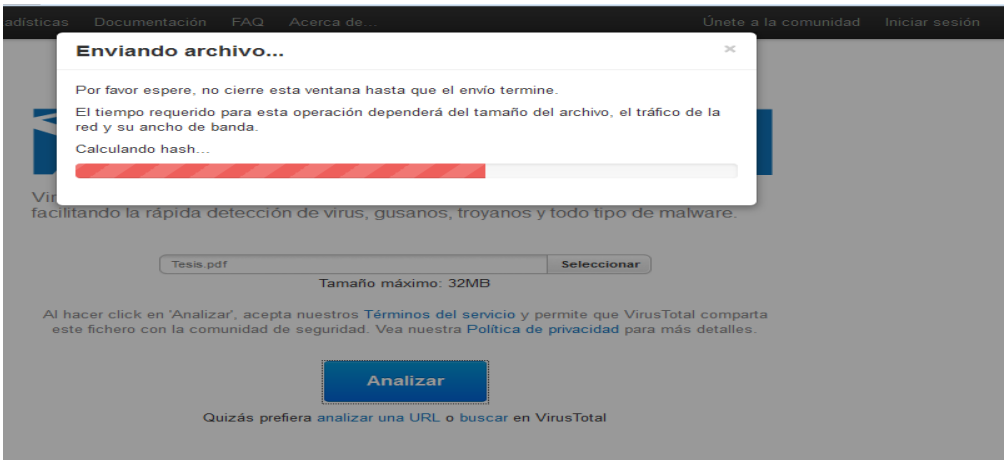
- **Análisis de los documentos PDF**

El primer documento que va ser analizado es Tesis.pdf que fue creado con un formato de búsqueda rápida de documento PDF que se encuentren en el computador.

Este documento contiene una función que se ejecuta en la acción cerrar del formulario, y lo que hace es rotar el documento. Además tiene dos funciones más, las cuales contienen código basura que no producen ningún daño al documento ni al computador.



El documento creado posteriormente se lo analizó con el servicio de internet Virus Total



El resultado del documento indico que ningún virus fue detectado

Tamaño:	8.3 MB (8679385 bytes)
Nombre:	Tesis.pdf
Tipo:	PDF
Detecciones:	0 / 46
Fecha de análisis:	2013-01-11 16:31:15 UTC (hace 0 minutos)

El documento fue analizado por algún software antivirus que posee Virus Total, los cuales son actualizados constantemente en línea.

Antivirus	Resultado	Actualización
Agnitum	-	20130111
AhnLab-V3	-	20130111
AntiVir	-	20130107
Antiy-AVL	-	20130111
Avast	-	20130111
AVG	-	20130111
BitDefender	-	20130111
ByteHero	-	20130110
CAT-QuickHeal	-	20130111
ClamAV	-	20130111

En el análisis se detectó un pequeño porcentaje de código JavaScript

PDFiD

```
PDF Header: %PDF-1.7
obj                2286
endobj             2286
stream             2243
endstream          2243
xref               0
trailer            0
startxref          36
/Page              3
/Encrypt           0
/ObjStm            404
/JS                6
/JavaScript        6
/AA                7
/OpenAction        7
/AcroForm          7
/JBIG2Decode       0
/RichMedia         0
/Launch            0
/EmbeddedFile      0
/Colors > 2^24     0
```

ClamAV PUA Engine

Possibly Unwanted Application. While not necessarily malicious, the scanned file presents certain characteristics which depending on the user policies and environment may or may not represent a threat. For full details see: http://www.clamav.net/support/faq/pua.

Aun cuando los antivirus no detectaron ningún tipo de código malicioso en el informe detallado del PDF indico que el documento posee código JavaScript que al parecer no es dañino pero que tomar las debidas precauciones al momento de ejecutarlo.

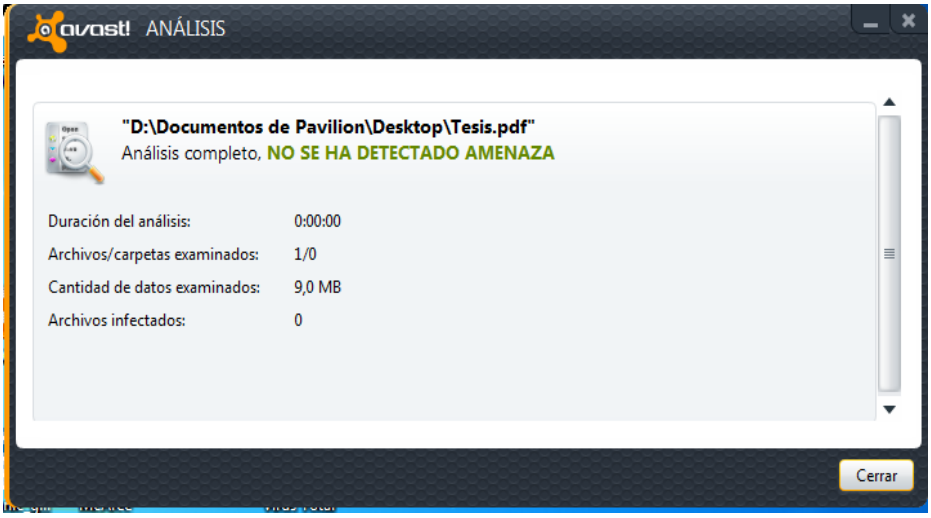
Además del documento Tesis.pdf se analizó el documento Prueba.pdf, cuyo resultado mostro que contenía más código JavaScript que el primer documento.

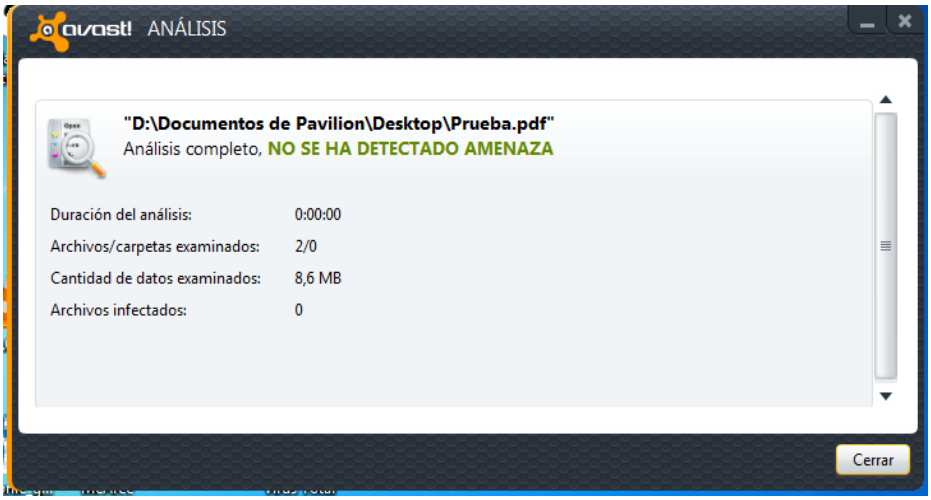
PDFiD

```
PDF Header: %PDF-1.7
obj                 3575
endobj              3575
stream              2012
endstream           2012
xref                0
trailer             0
startxref           23
/Page               0
/Encrypt            0
/ObjStm             326
/JS                 1248
/JavaScript         1248
/AA                 3
/OpenAction         3
/AcroForm           3
/JBIG2Decode        0
/RichMedia          0
/Launch             59
/EmbeddedFile       0
/Colors > 2^24      0
```

ClamAV PUA Engine
Possibly Unwanted Application. While not necessarily malicious, the scanned file presents certain characteristics which depending on the user policies and environment may or may not represent a threat. For full details see: http://www.clamav.net/support/faq/pua.

Los documentos Tesis.pdf y Prueba.pdf fueron analizados por segunda vez pero para esto ahora se utilizó el antivirus AVAST.



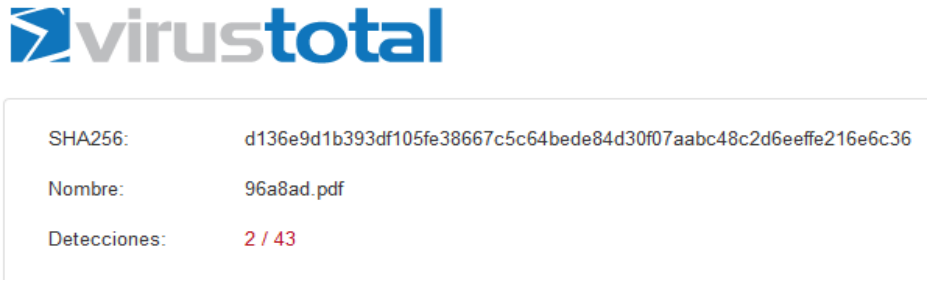


Como aviamos visto anteriormente entre los dos documentos existe una gran diferencia de código JavaScript y esta es la razón por la cual al analizarlo con AVAST el resultado del análisis nos muestra como si la cantidad de archivos escaneados hubiesen sido dos cuando en realidad fue uno solo.

Ahora se va analizar un documento PDF que fue encontrado en la siguiente dirección web:

http://foros.softonic.com/seguridad/nueva-vulnerabilidad-0-day-grave-adobe-acrobat-pdf-malicioso-ejemplo-109476#post856237.

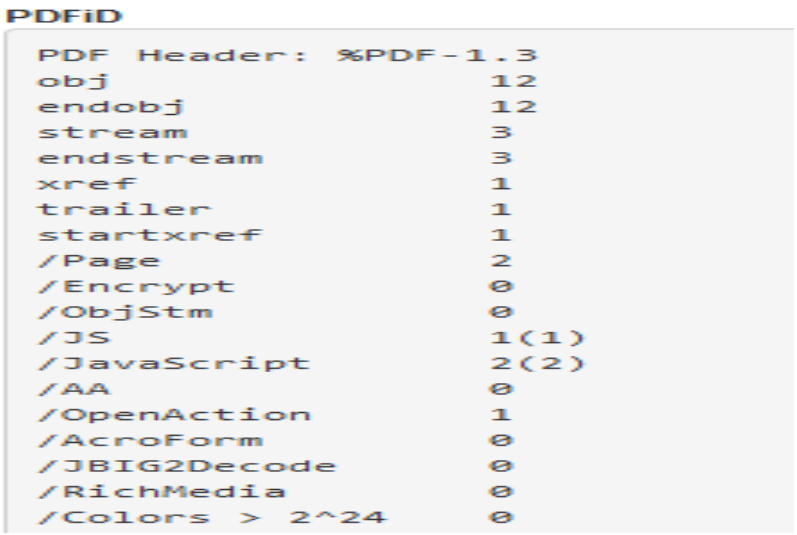
Para el análisis se utilizó el servicio web Virus Total que fue con el que se analizó el primer documento Tesis.pdf.



El total de virus detectados en el análisis en este documento fueron dos.

Kaspersky	-
McAfee	-
McAfee-GW-Edition	Heuristic.BehavesLike.PDF.Suspicious.F
Microsoft	-
NOD32	-
Norman	-
nProtect	-
Panda	Exploit/PDF.Exploit
PCTools	-

Los antivirus que detectaron el código malicioso en el documento PDF fueron McAfee y Panda, pero cada uno lo detecto con un nombre diferente porque cada antivirus posee una base de datos distinta.



En el informe detallado del análisis del documento 96a8ad.pdf se puede observar que en la parte de código JavaScript se han detectado dos anomalías que hacen referencia a los dos virus detectados que ya fueron explicados con anterioridad. El documento analizado no contiene código JavaScript como funciones u objetos, por lo que en la parte inferior no se presentó el mensaje de que el documento contenga código que llegue a causar algún daño en el archivo o el computador.

No todos los antivirus detectaron que el documento 96a8ad.pdf contenía código malicioso porque cada base de datos de los antivirus funciona de forma distinta para el reconocimiento de código malicioso, algunos se basan en el reconocimiento d firmas y otros en algoritmos heurísticos y porque las actualizaciones de cada antivirus

se demora un cierto periodo de tiempo mientras que nuevos virus van apareciendo y causando daño sin que puedan ser reconocidos en un principio.

- **Medidas de seguridad para abrir documentos PDF**
  - En el envío y recepción de documentos PDF, la herramienta más utilizada es el correo electrónico, y para mejorar su seguridad se debería tener la precaución de no abrir los documentos PDF de contactos desconocidos, sin antes analizarlos con algún software antivirus, para prevenir la ejecución de algún documento PDF malicioso.
  - Se debe tener la precaución de analizar todos los documentos al utilizar algún medio de almacenamiento como, flash, disco duro externo, memorias micro SD o cualquier tipo de dispositivo externo.
  - También hay que tener precaución al abrir documentos PDF que se encuentren compartidos en la red.
  - Al navegar en la Web se puede encontrar páginas que automáticamente manden a descargar documentos PDF maliciosos al computador, si esto ocurriera se debe tener cuidado de no ejecutar el documento sin antes ser analizado por algún antivirus, y aun cuando los documentos hayan sido descargados con nuestro consentimiento se debe realizar el análisis respectivo antes de abrirlos.
  - Al ser Adobe Reader el lector de PDF utilizado en el Gobierno Autónomo Descentralizado Municipalidad de Ambato es recomendable mantenerlo siempre actualizado porque constantemente se van incorporando en las actualizaciones nuevas herramientas que si bien no eliminan las vulnerabilidades que Adobe tiene, por lo menos ayuda a minimizar los daños que pueda causar al computador si se ejecutara algún documento PDF malicioso.
  - Cada software antivirus funciona de diferente forma por lo que es recomendable que se tenga instalado más de un software antivirus siempre y cuando sean compatibles para incrementar el nivel de seguridad en el Gobierno Autónomo Descentralizado Municipalidad de Ambato.

CUMPLIMIENTO DEL TERCEROBJETIVO ESPECÍFICO

Proponer una guía metodológica del análisis heurístico de malware considerando las necesidades que permita la detección de documentos PDF maliciosos en el Gobierno Autónomo Descentralizado Municipalidad de Ambato.

Como se puede observar el objetivo tres fue cumplido con la creación de la Guía con la cual se espera minimizar los riesgos de contagio a los computadores de los funcionarios de la Municipalidad de Ambato.