PLANTEAMIENTO DE SEGURIDAD PARA LA MINIMIZACIÓN DE FUGA, ROBO Y DAÑO DE LA INFORMACIÓN EN ARCHIVOS OFIMÁTICOS.

OMAR LEONARDO DIMIAN LEITON

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ, D. C.
2018

PLANTEAMIENTO DE SEGURIDAD PARA LA MINIMIZACIÓN DE FUGA, ROBO Y DAÑO DE LA INFORMACIÓN EN ARCHIVOS OFIMÁTICOS.

OMAR LEONARDO DIMIAN LEITON

MONOGRAFÍA PARA OPRTE EL TÍTULO DE
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Director de Proyecto:
Ing. Salomón González García

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ, D. C.
2018

Nota de aceptación

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Bogotá, D. C., Junio de 2018.

AGRADECIMIENTOS

A mi esposa e hijos por la paciencia y el tiempo empleado en la investigación y elaboración de esta monografía.

A mis tutores Fernando Zambrano, Salomón González, Fredy Acosta de la Universidad Nacional Abierta Y A Distancia – Unad, los cuales tuvieron la paciencia suficiente para corregir y generar este documento de muy buena calidad y que ayudará en ámbitos de sistemas a generar una mejor tecnología.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

Pág.

TABLAS DE ANEXOS

INTRODUCCIÓN

Históricamente en Colombia y en el mundo se han sostenido inconvenientes con la seguridad y la información generada al interior de las organizaciones con los archivos ofimáticos en la cual se percibe y experimenta la llamada fuga de información, también otros flagelos como el robo y el daño de archivos generados en aplicativos como Word, Excel, estos son los más apetecidos en el mercado y son blancos usualmente de robo o hurto de la información de las empresas, ejemplos de esta información son tales como proyectos, licitaciones, *know how*, documentación, cartas, investigaciones.

Este robo de información se da a través de los primeros responsables que son quienes generan o manipulan la información, se está hablando de los administradores o los usuarios, aquí se debe acotar que los usuarios en algunas ocasiones suministran información de los datos almacenados, pero en otras se logra concientizar de la importancia y el valor de la información, ante lo catalogado como delito y así evitarlo.

Además de esto los archivos informáticos están expuestos a ataques de secuestro [Ransomware], virus, lo cual aumentan las vulnerabilidades en estos archivos y se pone en riesgo la información.

En este documento se lanzará un planteamiento que minimizara estos riesgos y vulnerabilidades, mediante una solución que incluye una centralización de la información debidamente resguardada y también ciertos controles que ayudan a limitar las operaciones de hurto/robo por parte de los empleados y hasta de factores externos.

La metodología que se usara en esta monografía, es la de observación científica, mediante esta metodología y su investigación, llevara hasta el objetivo principal y la solución de la disminución de las vulnerabilidades de fuga, robo y daño de la información.

1. ANTECEDENTES

Es común que en las empresas se genere información mediante archivos de ofimática, esto se da gracias a los aplicativos de Word y Excel de la casa de software o fabricante Microsoft, en su gran mayoría, estos archivos a menudo son expuestos y atacados de diversas formas, gracias a su popularidad, la forma más común de ataque es por virus, también son robados, secuestrados, modificados o editados, consultados y enviados por correo sin autorización, estas prácticas se observan a menudo como una vulnerabilidad importante en las organizaciones, debido a que en el contenido reposa información muy importante e imprescindible, de la cual dependen negocios del ámbito empresarial, que normalmente se representan en dinero o también son los equivalentes a investigaciones, datos de valor tangible y no necesariamente económico asociado con el riesgo y control informático.

2. OBJETIVO DEL PROYECTO

2. 1. OBJETIVO GENERAL

Disminuir la vulnerabilidad de fuga, robo y daño de los archivos ofimáticos Word y Excel.

2. 2. OBJETIVOS ESPECÍFICOS

- Identificar los tipos de ataque, amenazas de los archivos.
- Recolectar información de ataques.
- Diseñar un documento de como disminuir este tipo de fuga, robo y secuestro.
- Contribuir a la minimización de riesgos de la información.

3. JUSTIFICACIÓN

Se pretende con este documento aumentar la seguridad en los archivos ofimáticos que contienen la información generada por una organización y así disminuir las vulnerabilidades de robo, fuga de información y ataques de virus a los archivos, que hoy en día deja muchas pérdidas económicas en las organizaciones y hasta incluso la quiebra, el objeto es disminuir la base de ataque e intentar concentrar los esfuerzos en seguridad informática a través de una aplicación en un servidor con seguridad y bajos riesgos de vulnerabilidad.

A continuación, se presenta una pequeña estadística del problema:

> Buenos Aires, Argentina – ESET, compañía líder en detección proactiva de amenazas, lanza el ESET Security Report 2016, informe que analiza el estado de la seguridad informática en Latinoamérica y presenta los resultados de encuestas realizadas a más de 3000 profesionales de distintas organizaciones. El reporte cuenta con datos de empresas de Argentina, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Guatemala, Honduras, México, Nicaragua, Panamá, Paraguay, Perú y Venezuela.
>
> En el informe se destaca que el 40% de las empresas encuestadas sufrieron un incidente relacionado con malware en el último año. Los países más afectados por códigos maliciosos son Nicaragua, que ocupa el primer lugar con el 58. 3%, seguido de Guatemala con el 55. 8% y Ecuador con 51. 9%. Asimismo, Argentina (29. 7%), Chile (29. 2%) y Venezuela (24. 1%) resultaron los países menos afectados por casos de malware en las empresas. En segundo lugar, con el 16% aparece el *phising* como uno de los incidentes de seguridad más frecuentes. A pesar de ser una técnica cada vez más conocida y relativamente fácil de detectar, logra su propósito a través de la aplicación efectiva de técnicas de Ingeniería Social. [1]

[1] ESET, ESET informa que el 40% de las empresas sufrió un ataque de malware [en línea], 2016 [revisado octubre 2017], Disponible en Internet: https://www. google. com. co/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjhqfO_47LXAhXJSyYKHZvaD-IQFgglMAA&url=http%3A%2F%2Fwww. eset-la. com%2Fcentro-prensa%2Farticulo%2F2016%2F40-empresas-sufrio-ataque-malware-eset-security-report%2F4290&usg=AOvVaw3AH_OJpk1dOODl2co-hLAX. [2016]

4. ALCANCE Y DELIMITACIÓN DEL PROYECTO

Este documento pretende informar al lector sobre un planteamiento para disminuir las vulnerabilidades en los archivos informáticos, tales como la fuga de información, el robo y los daños ocasionados a los archivos y secuestro.

Se pretende armonizar una idea, la cual genere una expectativa y guía para el diseño de un aplicativo que permita asegurar la información de forma centralizada, sin que la información esté expuesta a riesgos, se minimicen o se controlen.

Este documento no pretende diseñar, ni desarrollar un aplicativo.

5. MARCO REFERENCIAL

5*. 1 MARCO TEÓRICO.*

Dada la investigación implícita realizada se hará un recuento del marco referencial, exponiendo un marco teórico de los objetos y sus afectaciones.

En el mundo existen más de 400 millones de usuarios que hacen uso software de sistemas operativos de la casa de software Microsoft, estos usuarios también usan el complemento de herramientas de tipo ofimático de la misma casa de software llamado Office, este dúo de sistema operativo [Windows] y herramienta ofimática [office] son los más usados en el mundo y han sido blanco de ataques continuos con el pasar de los años.

En las organizaciones se genera una cantidad considerable de información, la cual es almacenada en los productos ofimáticos de Microsoft, como lo son en su gran mayoría documentos [Word] y hojas de cálculo [Excel], por lo tanto, se convierte en el blanco de ataques para los hackers, esto con diferentes motivos y razones.

Los ataques más influyentes de los últimos años son los de secuestro de la información a través de los Ransomware, el robo de la información copias de los archivos y entrega a la competencia, desapariciones por conveniencia y también el hurto.

En este documento se presentan distintos argumentos como las estadísticas, los conceptos de los elementos involucrados y hasta el actuar de los mismos con sus respectivas consecuencias.

El fenómeno ocurre en muchos de estos casos con el daño, robo o hurto de la información, que se debe a, que en muchas organizaciones no se tiene un adecuado uso racional de los elementos informáticos o tal vez la no información de los peligros de muchos de ellos junto con la irresponsabilidad de los usuarios, al ejecutar acciones que permitan vulnerar la seguridad implementada en las organizaciones.

Otro de los fenómenos más usuales son los ataques a través de los robos y hurtos de la información, en la mayoría de casos este ocurre desde adentro de las organizaciones, ya sea con motivos económicos o con motivos de deslealtad con la organización.

Sin embargo, controlar a los usuarios y sus responsabilidades no es muy factible, de hecho, se puede pensar en centralizar la mayoría de estas responsabilidades en un software y/o servidor, el cual permita minimizar los riesgos.

Hasta el momento no se ha planteado una solución funcional para minimizar estos riesgos o al menos intentar un control, para minimizar estos impactos siempre se ha hecho alusión a que los usuarios deben ser los “responsables” de los actos que puedan dar afectación a los problemas con los archivos informáticos, de lo que se deriva en el juicio de las personas.

5. 1. 1 Determinar el objeto, situación, caso. (que se va a observar)

Los objetos a determinar en este proyecto son los siguientes, los archivos de ofimática como Word, Excel.

Situación: De acuerdo con los datos del nuevo ESET Security Report, la aparición de programas maliciosos [virus, malware] es la principal causa de incidentes que sufren las empresas, aquí se habla esencialmente de Ransomware los cuales hacen mucho daño a las organizaciones, puntualmente a los archivos que no son recuperables como los ofimáticos como Word y Excel que contiene información muy importante en las organizaciones.

No solo los archivos con índices de perdidas ocasionan problemas si no también los hurtos corporativos y la fuga de información, de estos no existe mucha información, pero se tienen altos indicios de este fenómeno.

Los archivos que no importan, son los de sistemas operativos y programas los cuales son recuperables a través de reinstalaciones.

A continuación, se describirá la estructura de los archivos docx y xlsx.

5. 1. 1. 1. Estructura de Archivos de Microsoft Word.

Antecedentes

Desde la versión Word 2007, los archivos de Word tenían un formato de propiedad de Microsoft que se llamaba “Word Binary File Format”. Con este formato se manejaba toda la información del documento, textos, tablas, imágenes, datos con el formato, contenido con sus tablas, bibliografías, toda esta información estaba dentro de un mismo archivo, y esto pretendía a una estructura compleja del archivo, esto hacía que los archivos que puedan ser propensos a fallas. Por esta razón, el manejo de estas estructuras hace que aumente la complejidad para este tipo de archivos, Microsoft decidió cambiar las estructuras a formatos abiertos XML.

Para realizar un ejemplo vamos a desarrollar el siguiente proceso

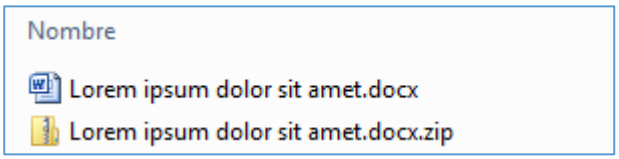
Para crear un documento que sirva de ejemplo, primero se debe abrir la aplicación Word, y escribe =lorem (20). Al pulsar enter, se generará automáticamente un texto con 20 párrafos, (El texto lorem está en latín).

Seguido se guarda el archivo en formato docx, se debe hacer una copia del archivo y sobre la copia se deberá renombrar el archivo a uno con extensión. zip.

Estructura del archivo

Como se ha dejado el mismo nombre con el nombre de archivo sugerido más la extensión, como se muestra en la figura 1.

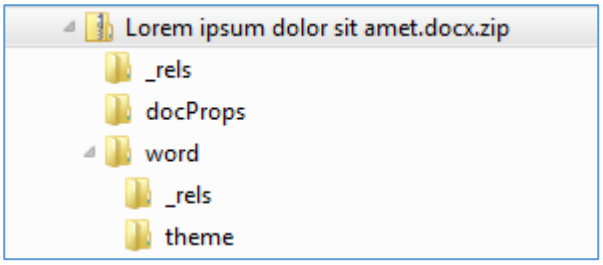
Figura 1 Archivo Word convertido en Zip.



Fuente: PEPEEEEEEE, (WIKI). El formato docx. [en Línea], 23 de julio de 2013 [revisado Octubre 2017], Disponible en Internet: https://answers.microsoft. com/es-es/msoffice/wiki/msoffice_onenote-mso_other/el-formato-docx/a3257c9d-fb20-4345-9c3a-885d1e76f34b.

Para ver la estructura o arquitectura interna del archivo docx, se debe dar click sobre el archivo del .zip, y se observará lo que enseña la figura 2 en forma de árbol:

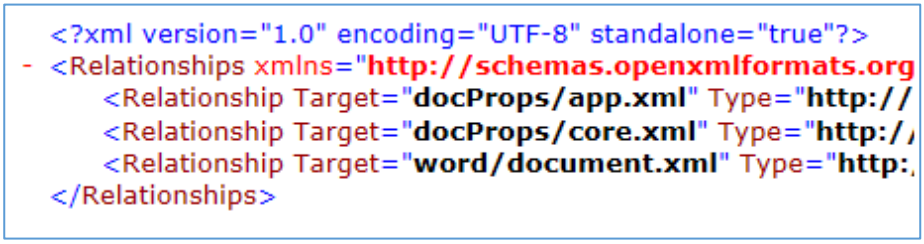
Figura 2 Archivo Word convertido en Zip.



Fuente: PEPEEEEEEE, (WIKI). El formato docx. [en Línea], 23 de julio de 2013 [revisado Octubre 2017], Disponible en Internet: https://answers.microsoft. com/es-es/msoffice/wiki/msoffice_onenote-mso_other/el-formato-docx/a3257c9d-fb20-4345-9c3a-885d1e76f34b.

Al abrir la carpeta llamada _rels, (de relationships) se encuentra un archivo de nombre rels.xml con el siguiente contenido, mostrado en la figura 3.

Figura 3 Contenido archivo XLS.

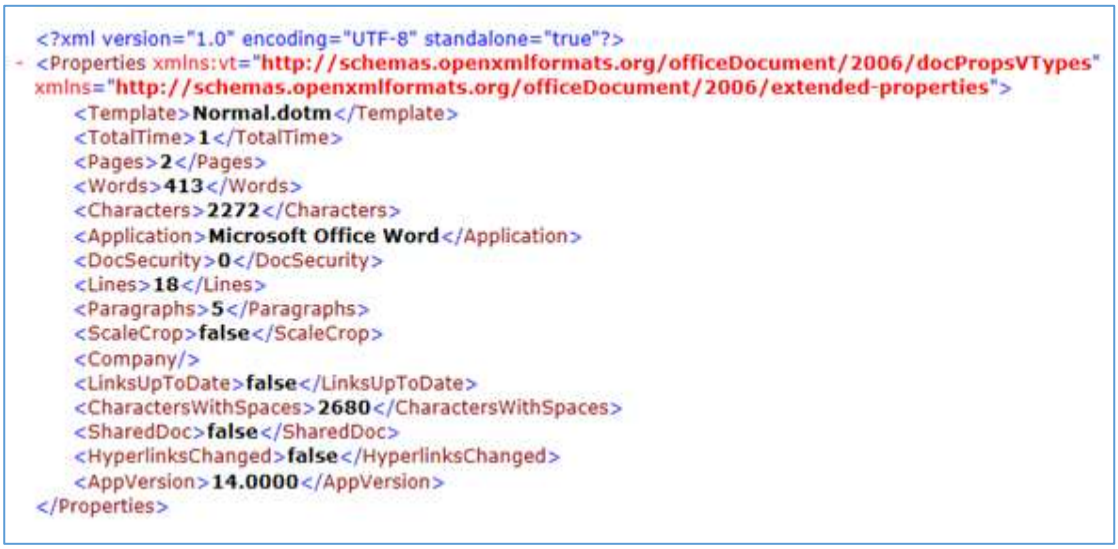


Fuente: PEPEEEEEEE, (WIKI). El formato docx. [en Línea], 23 de julio de 2013 [revisado Octubre 2017], Disponible en Internet: https://answers.microsoft. com/es-es/msoffice/wiki/msoffice_onenote-mso_other/el-formato-docx/a3257c9d-fb20-4345-9c3a-885d1e76f34b.

Cuando se abre el archivo se observa en el contenido que se relacionan tres archivos de tipo xml, dos en la carpeta docProps y uno en la carpeta Word (que se muestran en la figura 3).

El archivo app.xml, en la carpeta docProps (propiedades generales del documento) se tiene un resumen del documento también estructurado por .XML (la plantilla que se ha utilizado, el tiempo total de edición que se ha empleado en el archivo, número de páginas, palabras, caracteres y otros datos propios de la aplicación o del documento).

Figura 4 Contenido de archivo app. xlm.



Fuente: PEPEEEEEEE, (WIKI). El formato docx. [en Línea], 23 de julio de 2013 [revisado Octubre 2017], Disponible en Internet: https://answers.microsoft. com/es-

es/msoffice/wiki/msoffice_onenote-mso_other/el-formato-docx/a3257c9d-fb20-4345-9c3a-885d1e76f34b.

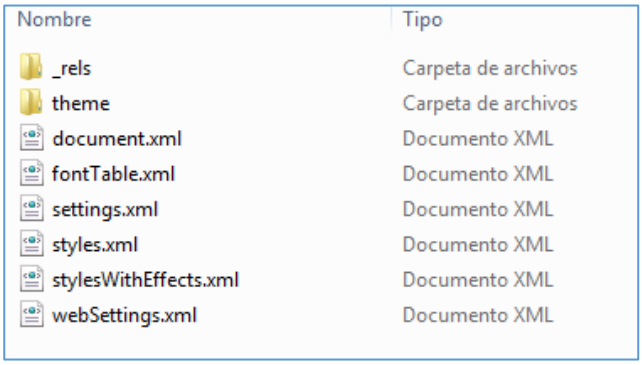
En el archivo llamado core.xml, ubicado también en la carpeta docProps, contiene los datos de metadatos, como nombre del autor del archivo, el último usuario que lo modifico, las fechas y horas de creación y hasta la última modificación (estos datos son propios del documento [metadato]).

Figura 5 Contenido de archivo core .xml.

Fuente: PEPEEEEEEE, (WIKI). El formato docx. [en Línea], 23 de julio de 2013 [revisado Octubre 2017], Disponible en Internet: https://answers.microsoft. com/es-es/msoffice/wiki/msoffice_onenote-mso_other/el-formato-docx/a3257c9d-fb20-4345-9c3a-885d1e76f34b.

En la carpeta siguiente llamada Word, se encuentra el contenido del documento y nuevamente encontramos la carpeta _rels y theme, también una serie de archivos xml.

Figura 6 Contenido de archivo Word . zip.



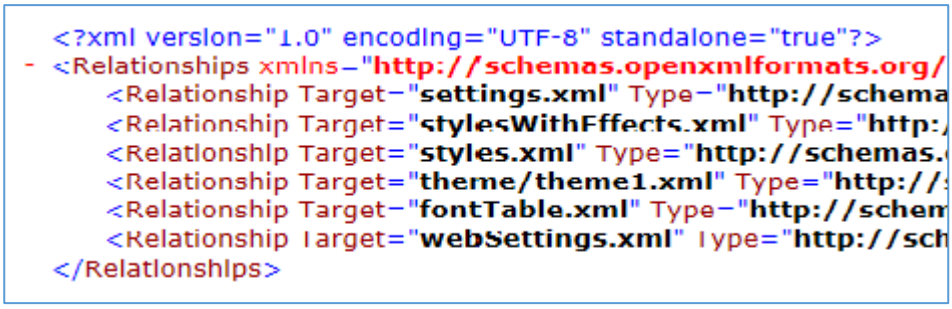
Fuente: PEPEEEEEEE, (WIKI). El formato docx. [en Línea], 23 de julio de 2013 [revisado Octubre 2017], Disponible en Internet: https://answers.microsoft. com/es-es/msoffice/wiki/msoffice_onenote-mso_other/el-formato-docx/a3257c9d-fb20-4345-9c3a-885d1e76f34b.

En la carpeta llamada _rels mostrada en la figura 6 aparece un archivo con el nombre document .xml. rels, establece las relaciones del archivo

document.xml con otros archivos de tipo .xml necesarios para armar el contenido y la estructura del documento o para el formato.

En el ejemplo este es el contenido observado de la figura 7.

Figura 7 Contenido de carpeta _rels y archivo documents.



Fuente: PEPEEEEEEE, (WIKI). El formato docx. [en Línea], 23 de julio de 2013 [revisado Octubre 2017], Disponible en Internet: https://answers.microsoft. com/es-es/msoffice/wiki/msoffice_onenote-mso_other/el-formato-docx/a3257c9d-fb20-4345-9c3a-885d1e76f34b.

En el contenido del archivo .xml de la figura 7 se encontrará si el documento tiene cabecera y pie, entonces habrá una relación con un archivo header.xml y footer.xml.

Si el contenido del documento tiene notas al pie o notas al fin, habrá una relación a un archivo footnotes.xml y endnotes.xml.
Si el contenido del documento tiene imágenes contendría relaciones a los archivos de las imágenes correspondientes, que constarían dentro de una carpeta llamada Media.

El contenido de cada uno de estos archivos .xml hace referencia a su nombre: El archivo settings.xml contiene los parámetros de configuración usados en el documento, en el archivo styles.xml están los estilos usados, en el archivo theme1.xml se encuentran los datos necesarios para definir el tema que se ha usado, en el archivo fontTable.xml, se encuentran las fuentes de las letras usadas (si se incrusta o modifica las fuentes en el documento, se pueden observar desde aquí), en el archivo webSettings.xml, se observa los parámetros del documento para la web. [2]

5. 1. 1. 2. Estructura de Archivos de Microsoft Excel.

Antecedentes

[2] PEPEEEEEEE, (WIKI). El formato docx. [en Línea], 23 de julio de 2013 [revisado Octubre 2017], Disponible en Internet: https://answers.microsoft. com/es-es/msoffice/wiki/msoffice_onenote-mso_other/el-formato-docx/a3257c9d-fb20-4345-9c3a-885d1e76f34b.

La extensión XLSX fue creada desde la versión 2007 del programa ofimático de Microsoft Excel. Entre tanto, con las versiones 2010, 2013 y 2016 llegan con propuestas de más funcionalidad, con el formato XML llega a convertirse en una poderosa hoja de cálculo simple y potente.

Como siempre, cuando se cambia de versionamiento, las versiones recientes siempre tendrán problemas con respecto a las anteriores las cuales van quedando obsoletas como lo es Excel 2007, 2003, etc. Por ejemplo, con Excel 2003 no se pueden abrir documentos de Excel 2016, por temas de cambio de estructura y archivos, a menos que se instale un paquete que proporcione la compatibilidad que debe existir para versiones nuevas de Microsoft Office, esto fue poco probable debido al cambio estructural, pero como ya se tenía mucha información se tuvo que crear una emulación para convertirlo y así mismo perder algunas funcionalidades de los archivos existentes. por lo tanto, si se posee una versión vieja de Excel como 2000, XP, 2003 o 2007 se debía instalar un paquete de compatibilidad de Microsoft office.

En las versiones anteriores a Microsoft office 2010 con extensión xls, se tenía una arquitectura de tipo binario, una estructura inmersa en sí misma y cerrada [caja negra] ahora los archivos poseen una estructura simple, organizada y poderosa como lo ofrece el XML y su conglomerado haciendo un archivo de extensión XLSX

A continuación, se observará un ejemplo de un archivo de Excel XLSX sencillo con solo 3 hojas como se muestra en la figura 8.

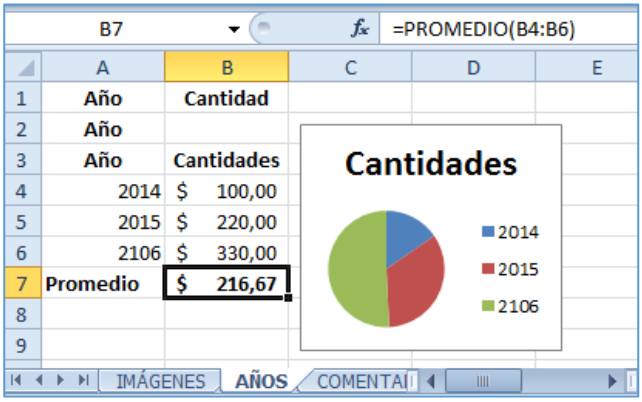
1. Una hoja llamada *IMÁGENES*, con algunos textos, con formato definido y 2 imágenes insertadas en la hoja:

Figura 8 Contenido celda Excel.

Fuente: PRIETO, Jesús. Lo que la extensión XLSX esconde. [en línea] 19 de junio de 2016 [revisado Marzo 2017], Disponible en internet: http://www. gonduana.com/lo-que-la-extension-xlsx-esconde/.

2. Una hoja llamada *AÑOS*, con una tabla y un gráfico mostrada en la figura 9:

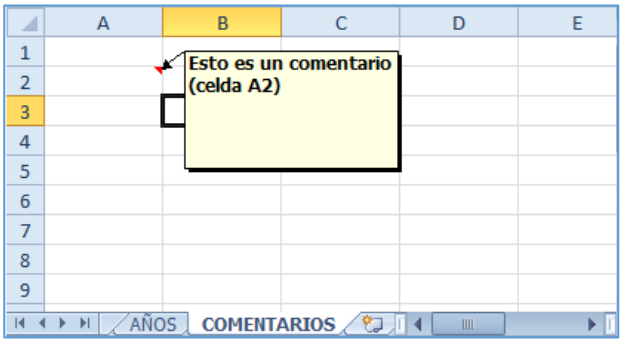
Figura 9 Contenido celda Excel tabla.



Fuente: PRIETO, Jesús. Lo que la extensión XLSX esconde. [en línea] 19 de junio de 2016 [revisado Marzo 2017], Disponible en internet: http://www. gonduana.com/lo-que-la-extension-xlsx-esconde/.

3. Una hoja llamada *COMENTARIOS*, con comentarios ingresados como se muestra en la figura 10:

Figura 10 Contenido celda Excel Comentario.

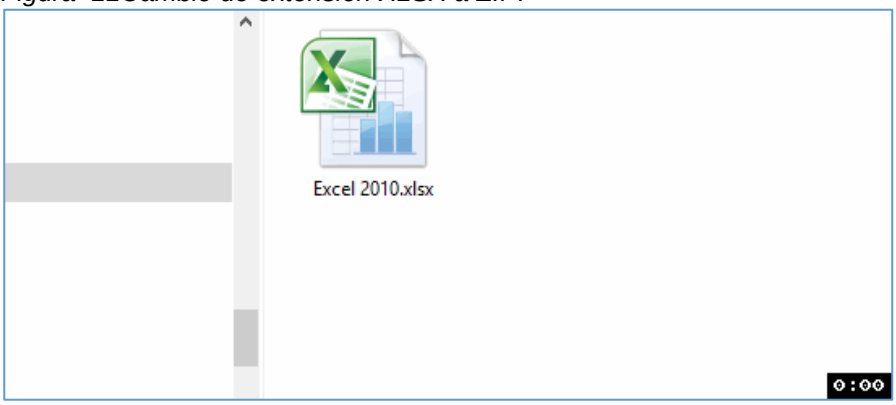


Fuente: PRIETO, Jesús. Lo que la extensión XLSX esconde. [en línea] 19 de junio de 2016 [revisado Marzo 2017], Disponible en internet: http://www. gonduana.com/lo-que-la-extension-xlsx-esconde/.

Se han incluido varios elementos en las hojas para que a continuación se pueda demostrar cómo se estructuran, en la nueva arquitectura planteada por Microsoft.

Se ubica el archivo en Windows Explorer, posteriormente se le debe cambiar la extensión del archivo de *.XLSX* a *.ZIP como se muestra en la figura 11*:

Figura 11Cambio de extensión XLSX a ZIP.

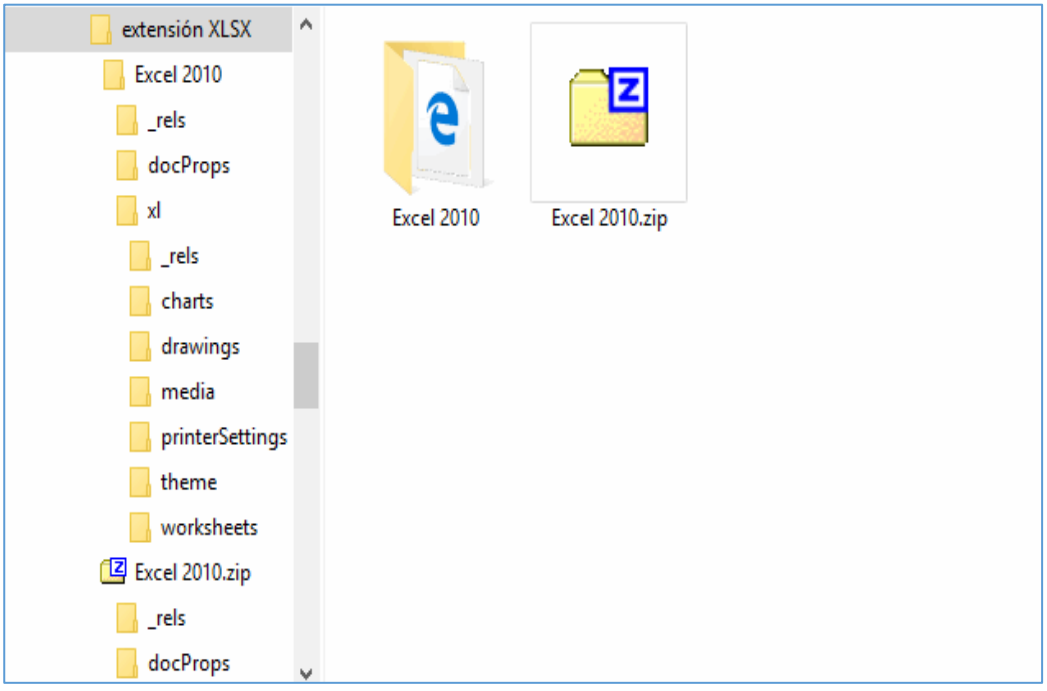


Fuente: PRIETO, Jesús. Lo que la extensión XLSX esconde. [en línea] 19 de junio de 2016 [revisado Marzo 2017], Disponible en internet: http://www. gonduana.com/lo-que-la-extension-xlsx-esconde/.

Ahora se puede abrir el archivo ZIP desde Windows Explorer o descomprimir desde cualquier otra herramienta de compresión.

Al descomprimirlo, se observará una estructura de directorios, como se muestra en la figura 12 y que posteriormente se explicará:

Figura 12 Contenido de Archivo Zip ya cambiado como Excel.



Fuente: PRIETO, Jesús. Lo que la extensión XLSX esconde. [en línea] 19 de junio de 2016 [revisado Marzo 2017], Disponible en internet: http://www. gonduana.com/lo-que-la-extension-xlsx-esconde/.

Se puede observar que el contenido hace parte de una estructura de carpetas con archivos de extensión XML, nuevamente tal como lo observábamos en Word.

En la carpeta *docProps* se encuentra la versión de Excel con la cual se generó el archivo, también en la carpeta docProps se observa un archivo importante de contenido y construcción que es el app.xml, que informa sobre el contenido en general de tipo .xml.

Cuando se abre el archivo app.xml, se observará código como el que se muestran en la figura 13.

Figura 13 Contenido de Archivo app.xml.

```
<?xml version="1.0" encoding="UTF-8" standalone="true"?>
- <Properties
xmlns:vt="http://schemas.openxmlformats.org/officeDocument/2006/docPropsVTypes"
xmlns="http://schemas.openxmlformats.org/officeDocument/2006/extended-properties">
    <Application>Microsoft Excel</Application>
    <DocSecurity>0</DocSecurity>
    <ScaleCrop>false</ScaleCrop>
  - <HeadingPairs>
    - <vt:vector baseType="variant" size="2">
      - <vt:variant>
          <vt:lpstr>Hojas de cálculo</vt:lpstr>
        </vt:variant>
      - <vt:variant>
          <vt:i4>3</vt:i4>
        </vt:variant>
      </vt:vector>
    </HeadingPairs>
  - <TitlesOfParts>
    - <vt:vector baseType="lpstr" size="3">
        <vt:lpstr>IMÁGENES</vt:lpstr>
        <vt:lpstr>AÑOS</vt:lpstr>
        <vt:lpstr>COMENTARIOS</vt:lpstr>
      </vt:vector>
    </TitlesOfParts>
    <Company/>
    <LinksUpToDate>false</LinksUpToDate>
    <SharedDoc>false</SharedDoc>
    <HyperlinksChanged>false</HyperlinksChanged>
    <AppVersion>14.0300</AppVersion>
</Properties>
```

Fuente: PRIETO, Jesús. Lo que la extensión XLSX esconde. [en línea] 19 de junio de 2016 [revisado Marzo 2017], Disponible en internet: http://www. gonduana.com/lo-que-la-extension-xlsx-esconde/.

Este es un archivo simple de XML, como se observa con suficientes etiquetas de apertura y de cierre de tipo XML, ahora se debe hacer el enfoque, hacia los siguientes ítems:

El primero, el nombre de las tres hojas de cálculo creada en el archivo de Excel llamadas: *IMÁGENES*, *AÑOS* y *COMENTARIOS*.

La segunda, es la etiqueta AppVersión, esta informa la versión del software de Excel, está se encuentra al final del XML, en este caso, se observa que es la versión 14 («14. 0300»), que corresponde a un Excel 2010.

A continuación, se exhibe la consulta de la siguiente tabla de versiones de [Office] Excel hasta la fecha:

Tabla 1. Versiones Office.

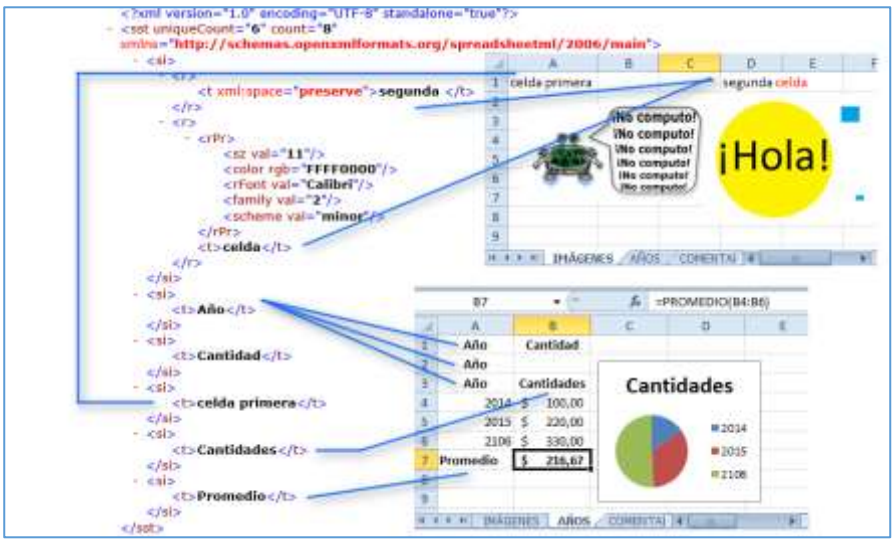
AppVersion	Versión
12	Office 2007
14	Office 2010
15	Office 2013
16	Office 2016

Fuente: El Autor

En la carpeta *xl* se observa el contenido de la hoja de cálculo, cuando la abrimos se encuentra el archivo sharedStrings.xml, aquí se observan los textos escritos en la hoja de cálculo. Es decir, en este archivo se guarda el contenido principal de la hoja de cálculo, distribuido por etiquetas de celdas y posiciones, respectivamente.

En la siguiente figura 14, se observa la comparación del contenido de este XML con 2 de las hojas y su ubicación en el archivo:

Figura 14 Contenido grafico de Xml.



Fuente: PRIETO, Jesús. Lo que la extensión XLSX esconde. [en línea] 19 de junio de 2016 [revisado Marzo 2017], Disponible en internet: http://www. gonduana.com/lo-que-la-extension-xlsx-esconde/.

A continuación, se detallará el contenido del archivo XML a fondo:
Primero, se localiza los textos de la primera celda y de la segunda celda. Estos textos no se encuentran en el mismo orden del archivo XML que en la hoja de datos, este solo intenta seguir el orden en el cual se escribieron, es decir si primero se escribió en la celda A1, luego en la celda A15 y por último en la celda A3, así mismo aparecerá en el archivo XML.

Otro caso que ayuda con la estructura es el caso de valores repetidos, en el archivo XML se encuentra el texto "*Año"*, que aparece 3 veces en la hoja o pestaña *AÑOS,* a partir de estos duplicados se da el nombre a otro tipo de archivo XML, llamado sharedStrings.xml, esto obedece a que Excel, por motivos de rendimiento, guarda una copia de cada cadena de texto distinta y no las duplicadas.

En otra parte de esta estructura de archivos XML se informa que esta cadena de texto "*Año"* se repite varios intervalos en unas celdas específicas y puntuales.

Por último, se puede apreciar que las cadenas de texto "*Cantidad",* "*Cantidades"* y "*Promedio" no se repiten, por lo tanto, permanecen como únicas*.

El tratamiento de los objetos de tipo comentario, también son ubicados en la carpeta xl, se almacenan en un archivo llamado comments1.xml, el contenido de uno de estos se observa en la figura 15.

Figura 15 Contenido de archivo comments1.xml.

Fuente: PRIETO, Jesús. Lo que la extensión XLSX esconde. [en línea] 19 de junio de 2016 [revisado Marzo 2017], Disponible en internet: http://www. gonduana.com/lo-que-la-extension-xlsx-esconde/.

En la figura 15 se observa los comentarios que posee el archivo de Excel en formato XML, aquí se informa su ubicación en la hoja de cálculo que incluye las coordenadas de la celda y el comentario como texto, incluso también se incluye los estilos y el formato de la información, si hubiese comentarios de otras hojas, Excel crearía un archivo adicional llamado comments2.xml, comments3.xml, y así sucesivamente; se crearía un XML por cada hoja con comentarios.

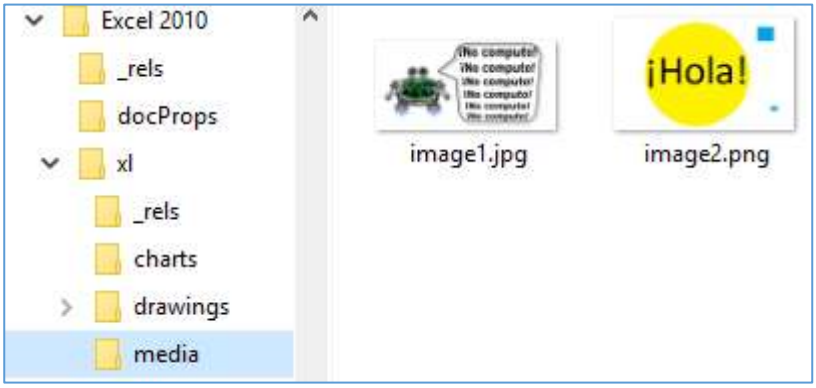
Nota importante: Las herramientas nuevas de traducción asistida, como Trados Studio o memoQ, abren las hojas de cálculo de tipo XLSX en su propia interfaz de usuario. Lo que hace en realidad es convertir la extensión XLSX a ZIP, abre el ZIP en una carpeta temporal, busca la estructura y aparta los archivos sharedStrings.xml y comments1.xml de la carpeta xl, extrae el texto y formato mediante un filtro especial de este software. Si se hace alguna modificación se genera inmediatamente en él .xml, por último, se crea un ZIP con la estructura de directorios, archivos cambian la extensión ZIP a XLSX para que pueda ser entregado al cliente en el formato origen.

Esto indica, que es posible traducir hojas de cálculo XLSX con estas herramientas o también que se puede desarmar los archivos para su revisión, validación u otros objetivos y volver a armar sin la necesidad de tener los aplicativos ofimáticos Word, Excel.

En este ejemplo de Excel los gráficos en la hoja número 2 "*AÑOS", en la estructura* se encuentra en la carpeta xl/drawings, también existen gráficos, cuya configuración (color, posición, tipo de gráfico) se indica más detalladamente en la carpeta xl/drawings.

En la carpeta *xl/media contiene todo el* contenido multimedia, si se abre la carpeta xl/media, se encuentran las dos imágenes insertadas en la hoja de cálculo de Excel, así como se muestra en la figura 16.

Figura 16 Contenido de Gráficos en carpeta.



Fuente: PRIETO, Jesús. Lo que la extensión XLSX esconde. [en línea] 19 de junio de 2016 [revisado Marzo 2017], Disponible en internet: http://www. gonduana.com/lo-que-la-extension-xlsx-esconde/.

Las imágenes están en el formato original con el cual se insertó (.JPG y .PNG, para el caso de la hoja llamada Año), con lo cual se describe lo siguiente:

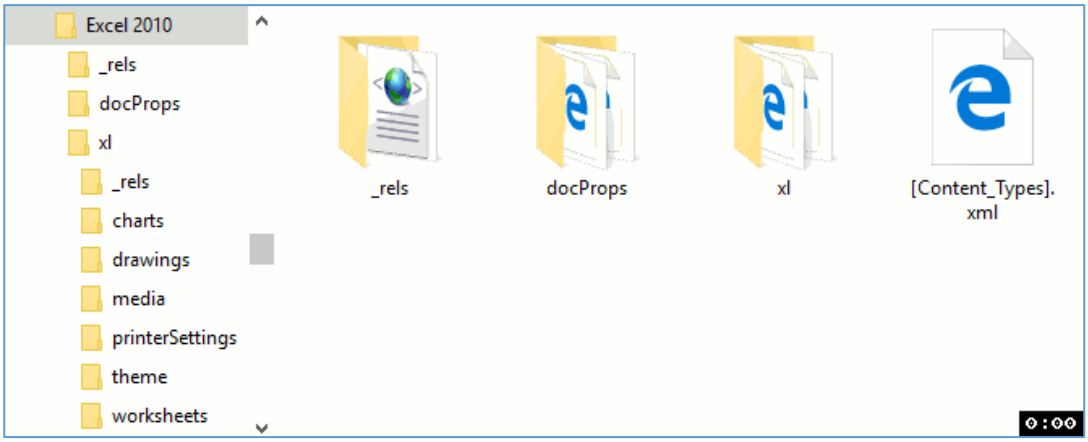
En el proceso de traducción de las imágenes la carpeta xl/media se encuentran todas las imágenes pertenecientes al archivo completo en la estructura es muy útil, esta separación como se muestra en la figura 17 de la carpeta xl/media así:

Si la hoja de cálculo contiene varias imágenes insertadas, estas pueden ser cambiadas si conservan el mismo nombre, el procedimiento de modificación completo sería el siguiente:

- Seleccionar las imágenes con texto traducible de esta carpeta xl/media.
- Con cualquier herramienta de software ocr, se extrae el texto de estas imágenes a un documento de texto, según el software.
- Traducir los textos de las imágenes.
- Con alguna herramienta de edición de imágenes (como Paint de Microsoft, Photoshop, etc.), se pueden editar y modificar estas imágenes e insertar el texto, figuras.
- Sin cambiar el nombre de archivo (image1, image2…), deja las imágenes traducidas en la misma carpeta xl/media.
- Posteriormente se cambia la extensión de ZIP a XLSX. [3]

[3] PRIETO, Jesús. Lo que la extensión XLSX esconde. [en línea] 19 de junio de 2016 [revisado Marzo 2017], Disponible en internet: http://www. gonduana.com/lo-que-la-extension-xlsx-esconde/.

Figura 17 Contenido Carpeta xl/media.



Fuente: PRIETO, Jesús. Lo que la extensión XLSX esconde. [en línea] 19 de junio de 2016 [revisado Marzo 2017], Disponible en internet: http://www. gonduana.com/lo-que-la-extension-xlsx-esconde/.

A continuación, se validará algunos conceptos de los virus que más impactan a estos archivos son.

Exploits: es un programa o procedimiento de código que se aprovecha de una vulnerabilidad que se llama agujero de seguridad en una aplicación o sistema operativo de tal forma que un atacante puede usarla en su beneficio.

El Ransomware: es un programa malicioso que al ser ejecutado en un equipo PC le ofrece al ciberdelincuente la oportunidad de secuestrar y bloquear el PC, esto generado desde una ubicación remota o automáticamente al ejecutar un programa malicioso, esto permite encriptar los archivos, tomando el control de toda la información (software, datos, fotos, aplicativos, etc.). El proceso para desbloquear el equipo PC y/o los archivos, lo anuncia a través del lanzamiento una ventana emergente o un aviso en el escritorio, al reiniciar el equipo, en la que se informa el pago de un rescate por la información secuestrada.

Existen dos tipos de Ransomware, uno el que bloquea el equipo PC y solicita rescate y el segundo encripta los datos y lo deja sin acceso interno.
De igual forma tiene como objeto ocultar los archivos uno dentro de otro archivo, esto se logra con un programa deseado o sebo para el usuario que lo invita a ejecutar o a hacer click en este, estos archivos van adjuntos en correos electrónicos, vídeos de páginas solicitadas o buscadas de dudoso origen o incluso en actualizaciones de sistemas y programas en principio confiables.

Una vez que ha ingresado en el equipo PC, el malware virus se activa o espera a cierto evento y provoca el bloqueo del sistema operativo, afectando aplicaciones, datos de todo tipo e inicia la encriptación, por ultimo ejecuta el mensaje de advertencia con la amenaza e informa la cuantía del “rescate” que se debe de pagar

para recuperar o restituir a su anterior estado toda la información. El mensaje puede variar en función del tipo de Ransomware al que enfrentamos.

> Para mejorar la percepción de seguridad en el ataque y el miedo de la víctima, en varias ocasiones se ofrece los datos del entorno del equipo, como la dirección IP, nombre del equipo, la organización proveedora de internet y hasta una fotografía desde la webcam, esto permitirá aumentar la sospecha de la amenaza y afianzar la certeza del ataque. [4]

Interpretado en otras palabras de la vida real, es como si una cerradura (para el ingeniero de sistemas sistema operativo o aplicación) tuviera un fallo en el diseño que accediera a generar llaves que la abrieran llamados (Exploits) fácilmente y poder así acceder al activo que se quiera proteger, realizando así actos delictivos.

Entre los usuarios existe una confusión con los exploits, los que se consideran un tipo de malware y/o virus, los malware aprovechan una vulnerabilidad para acceder a un equipo sin problemas de accesos permitido desde el mismo sistema.

De esta forma, se puede proporcionar los accesos necesarios para que pueda ejecutarse en un sistema e infectarlo aprovechando cualquier vulnerabilidad.

> Los medios de infección más frecuentes se encuentran a la mano, como los correos electrónicos, estos pueden ser Spam (Basura) o estar suplantados, regularmente usando técnicas de ingeniería social, engaños como cursos, rifas, paquetes gratis, actualizaciones, envío de facturas o cualquier otra cosa, también se hace la expansión de este malware por otros medios, como la descarga de antivirus / antimalware, drivers, ejecuciones similares de aplicaciones (phishing), actualizaciones, anuncios falsos y la instalación y ejecución sobre equipos de botnets y otros afectados por ejemplo el malware Zeus.
>
> O también en ocasiones la distribución de software falso producido por páginas de descargas ilegales, suplantadas, contenido multimedia protegido (como películas y series), pornografía, blogs infectados y otros. [5]

Virus: Son programas informáticos que ingresan al equipo de una persona sin que este se dé cuenta, con la finalidad de alterar la información, o infectar los archivos del sistema destruyendo los datos almacenados en el equipo, estos virus pueden

[4] PANDASECURITY. COM, ¿Qué es un Ransomware?. [en Linea] 15 de Noviembre de 2013 [Revisado Marzo de 2017], Disponible en internet: http://www. pandasecurity. com/spain/mediacenter/malware/que-es-un-ransomware/ p 39-40

[5] ALBORS, Josep. ¿Sabes qué es un exploit y cómo funciona? [en Linea] 9 de octubre de 2014 [Revisado marzo de 2017], disponible en internet: https://www. welivesecurity. com/la-es/2014/10/09/exploits-que-son-como-funcionan/. p 40- 42

replicarse a sí mismo y propagarse a otros equipos. No todos los virus son malignos, existen unos programas que son inofensivos y se identifican por ser molestos, espiar y enviar información al atacante, etc.

MÉTODOS DE INFECCIÓN

Hay muchas formas con las que un equipo PC puede exponerse a infecciones con un virus:

- ✓ Mensajes en redes sociales como Facebook o Twitter.
- ✓ Archivos adjuntos en correo electrónico.
- ✓ Sitios web dudosos o sospechosos.
- ✓ Ingreso de USB, DVD o CD con virus o programas maliciosos.
- ✓ Descarga de cualquier tipo de aplicación o programas de internet voluntariamente o inductivamente.
- ✓ Anuncios publicitarios falsos.
- ✓ Ataques mediante vulnerabilidades de los sistemas operativos, a falta de actualización o no descubiertos.

CÓMO INFECTA UN VIRUS EN UN EQUIPO.

1. El usuario instala voluntaria o involuntariamente un software infectado en el Equipo PC.
2. El archivo malicioso es alojado en la memoria ram del equipo PC, esperando algún tipo de evento para ejecutarse.
3. El virus infecta archivos que se esté usando en ese instante o también infecta masivamente otros archivos, alojados en unidades extraíbles.
4. Cuando el equipo PC se inicia, el virus se carga en la memoria RAM o como proceso o servicio y toma control de servicios del sistema operativo, aplicaciones o datos, lo que ya ha determinado la infección y también la propagación de este.

Existen varios tipos de virus, los cuales afectan archivos, rendimiento, equipos, redes y otros, para este caso no se detallarán en definición y funcionamiento, ya que de una u otra forma terminan infectando y atacando los archivos importantes para una organización.

Los robos y hurtos de información a las empresas es otro factor que afecta la funcionalidad, la economía y los procedimientos de las organizaciones.

5. 2 MARCO CONTEXTUAL

La solución se orienta para un ámbito general, no se particulariza como solución a un problema de una organización, si no que se propone en general, como método de realización de una mejora en la sistematización, y en la disminución de riesgos encontrados con la información, aprovechando que se puede centralizar los

archivos de forma ordenada y segura de esta manera se minimice las amenazas, se deben controlar los accesos y envíos de información, de esta forma se espera que la disponibilidad de la información se mantenga en las organizaciones y las organizaciones minimicen las perdidas.

La concentración de la información es importante ya que desde allí se concentraría las herramientas de seguridad y aseguramiento de los servidores.

5. 3 MARCO CONCEPTUAL

Los archivos ofimáticos como Word y Excel, son usualmente son atacados de diversas formas, copiados divulgados sin permiso, infectándolos con virus, como Ransomware, spyware, gusanos etc. Este último haciendo que sean el medio para transportar e infectar otros tipos de archivos, logrando como objetivo la no funcionalidad de archivos, perdida de información, secuestro de información, modificación de a la información, y también el daño a programas de software y equipos de cómputo.

En este documento se genera una sugerencia que permite minimizar los riesgos, mediante la centralización de la información de los archivos ofimáticos, acompañado de un conjunto de dispositivos de seguridad y buenas prácticas en seguridad informática orientadas tanto hacia los administradores como hacia los usuarios.

6. IDENTIFICACIÓN DE ATAQUES Y AMENAZAS DE LOS ARCHIVOS DE WORD Y EXCEL

6. 1. Analizar e interpretar los datos.

Del registro de los datos, se tiene el siguiente impacto de los Ransomware, este es alto en general, se dice que estos dejan perdidas estas perdías se calculan en un billón de dólares en el año de 2016 según Big-Brother-News publicado en marzo 24, 2017 solo en estados unidos, estas cifras son dadas por identificación y reporte de los incidentes.

Al no contar con el pago de un rescate, el costo relacionado con la pérdida de productividad de los empleados y la inactividad ocasiona pérdidas que se suman al daño financiero, adicionalmente el daño relacionado a la marca y a la reputación, incrementan la perdida; Esto se suma a las posibles consecuencias de carácter penal por incumplimiento de las normas. Algunos informes señalaron que el FBI calculo que en el primer segmento trimestral del año 2016 las pérdidas estuvieron alrededor de 209 millones de dólares, algo considerable comparado contra los 24 millones de dólares del año 2015.

Frente a estas cifras se puede determinar que la información es un frente importante de toda organización y que esta debe ser cuidada. Por lo tanto, como conclusión se debe crear una posible solución para minimizar este impacto global. [6]

6. 2. Robo/hurto de información.

El hurto de la información puede iniciar desde misma empresa o también como ataques directos en una organización, cualquiera que sea el medio o de donde provenga este, hará daño directo en la organización, tal como lo indica Monica Tilves a continuación en la investigación de HFS Research.

7 de cada 10 empresas han sufrido robos de datos a manos de los trabajadores.

Una investigación llevada a cabo por HfS Research y Accenture muestra “un panorama preocupante” en términos de seguridad.

---

[6] DIARIOTI. COM. El Ransomware en cifras y lo que las organizaciones deben saber. [en línea] 2016 [revisado Abril 2017], Disponible en internet: https://diarioti. com/el-ransomware-en-cifras-y-lo-que-las-organizaciones-deben-saber/98938.

Los ciberdelincuentes no son las únicas personas que pueden poner en peligro la seguridad de una empresa. En algunas ocasiones el enemigo se encuentra localmente, ya que los trabajadores también pueden terminar provocando la pérdida de información, de forma consciente.

Como señala: HfS Research en nombre de Accenture en el articulo “The State of Cybersecurity and Digital Trust 2016”

En un informe que ha realizado HfS Research en nombre de Accenture, la mayoría de las compañías ha sufrido el robo de información a manos de los trabajadores durante el último año (2016) o cuanto menos, han sido víctimas de un ataque, estas sería aproximadamente un 69% de ellas. En el caso de las firmas TIC y los medios de comunicación esta cifra se eleva al 77%.

Este hurto perpetrado desde el interior preocupa al 48% de las organizaciones, mientras que la infección por malware es la pesadilla hipotética de un 42% cuando se habla de riesgos a los que se pueden acabar enfrentando los negocios en el próximo año o año y medio y ocasionar hasta la quiebra inminente.

Además, más de la mitad de las empresas cree que los empleados actuales no serían capaces de prevenir problemas de seguridad. Posiblemente se podría detectar y actuar a posteriormente para repararlos, pero no para evitar que lleguen a suceder con toda la fuerza y consecuencias. A esto hay que añadir que 4 de cada 10 directivos de alto nivel reclaman más dinero para poder contratar expertos en seguridad y formar a los trabajadores.

“Los resultados de la investigación muestran un panorama preocupante “, valora Kelly Bissell, Senior Managing Director de Accenture Security. “Los líderes en seguridad creen que las amenazas no desaparecerán, sino que aumentarán y dificultarán la capacidad de las compañías de proteger los datos clave y restablecer la confianza en lo digital. Al mismo tiempo, mientras las compañías pretenden invertir en cibertecnologías avanzadas, no tienen suficiente presupuesto para contratar o formar a gente calificada para usar la tecnología de manera eficiente”.

“Para gestionar mejor este problema de seguridad, las compañías necesitarán trabajar conjuntamente con el amplio ecosistema de empresas existente (unidades de negocio, socios, proveedores y consumidores finales) con el fin de crear un entorno de confianza en lo digital”, dice Bissell. [7]

[7] TILVES, Mónica. 7 de cada 10 empresas han sufrido robos de datos a manos de sus trabajadores. [En línea] 8 de julio de 2016 [Revisado Abril de 2017], Disponible en internet: http://www. silicon. es/7-cada-10-empresas-robos-datos-trabajadores-2313410.

6. 3. Registrar los datos observados.

A continuación, se muestra algunos virus que afectan los archivos y están totalmente vigentes.

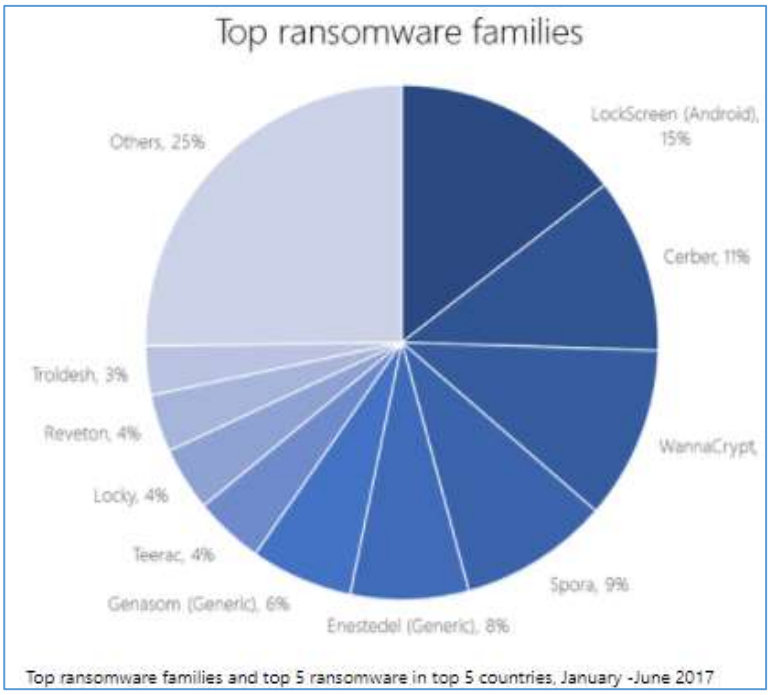
Tim Rains, Director de seguridad de Microsoft lanzado el blog Ransomware: "Entendiendo el riesgo en abril de 2016 que resume el estado de Ransomware y proporciona estadísticas, detalles y sugerencias preventivas para empresas y profesionales: nuestros Informe de inteligencia de la amenaza: Ransomware también incluye sugerencias sobre prevención y recuperación, estadísticas y datos."

Los últimos seis meses (entre diciembre de 2015 y de 2016 mayo) han visto el aumento de Tescrypt mundialmente. Crowti sigue siendo en la parte superior de la manada, Brolo y FakeBsod, para el periodo se encuentran Lockscreen, cerbec, wanacryp y spora repuntando los ataques.

El repunte de exxeroute también disminuyo, ahora en el 1% del top 10, de 7% durante los 6 meses anteriores.

A continuación, se muestra la familia de Ramsomware 2017 en la figura 18.

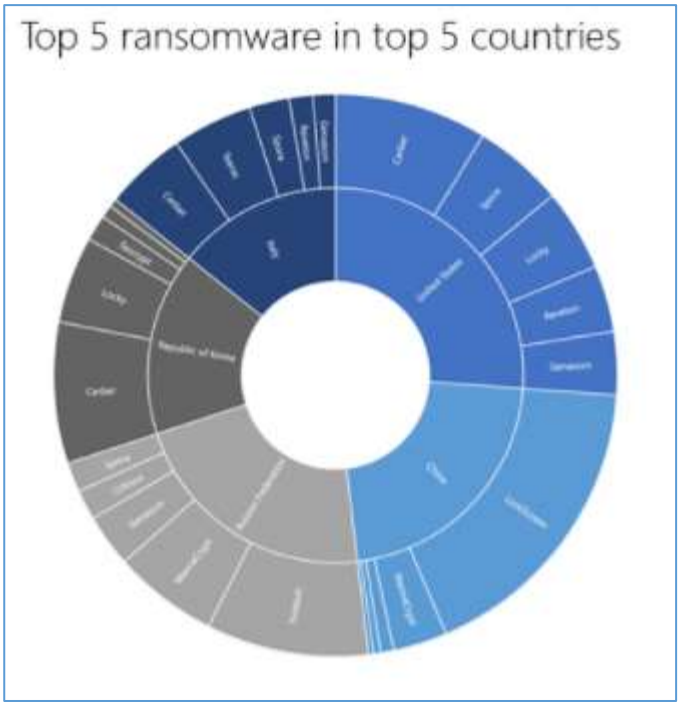
Figura 18 Ransomware familia 2017.



Fuente: Ransomware. [en línea] no posee fecha [Revisado Diciembre de 2017], Disponible en internet: https://www. microsoft.com/en-us/wdsi/threats/ransomware.

Para los 10 países con las detecciones de la mayoría, los Estados Unidos tiene un completo panorama de la mitad de todas las detecciones. Italia es segundo, seguido de cerca por Canadá, Turquía y el Reino Unido. Después de la distribución se extiende en todo el mundo.

Figura 19 Países con detección de Ransomware.



Fuente: Ransomware. [en línea] no posee fecha [Revisado Diciembre de 2017], Disponible en internet: https://www. microsoft.com/en-us/wdsi/threats/ransomware.

Las detecciones más grandes en los Estados Unidos fueron de Cerber, seguido por spora y Locky. Lockyscreen también fue frecuente en China, la figura 19 muestra la estadística. [8]

En cuanto a la perdida de datos para propósitos varios tenemos un informe:

"El Instituto Ponemon ha presentado su "Estudio sobre el coste de la Pérdida de Datos 2015: Análisis Global", patrocinado por IBM, el cual, tras analizar a 350 importantes empresas de 11 países, señala que la media del coste de la pérdida de datos es de 3,5 millones de euros por empresa. Esto supone un incremento del 23% en los dos últimos años.

[8] MICROSOFT. Ransomware. [en línea] no posee fecha [Revisado Diciembre de 2017], Disponible en internet: https://www. microsoft.com/en-us/wdsi/threats/ransomware.

El estudio también revela un incremento del 6% en el coste medio de pérdida o robo de archivos con información confidencial y sensible, siendo la industria sanitaria la que registra el mayor coste por robo de datos con una media que supera los 334 euros. Además, este coste ha supuesto para las empresas de distribución un incremento que va de los 105 dólares registrados el año pasado a los 151 dólares de este.

En Uruguay se data del robo de los archivos informáticos los cuales tenían una trascendencia de investigación de diez años, el robo tuvo actividad de tipo físico en la que se llevaron todo el material recaudado y que incluye una extensa investigación acerca de los desaparecidos durante la dictadura (1973-1985) [tomado de http://www.lateclaene.com/william-puente-ct5m]." [9]

[9] MÁRMOL, Patricia. El coste de la pérdida de datos alcanza los 3,5 millones de euros por empresa. [en línea] 28 de mayo de 2015 [revisado Abril 2017], disponible en internet: http://www. datacenterdynamics. es/focus/archive/2015/05/el-coste-de-la-p%C3%A9rdida-de-datos-alcanza-los-35-millones-de-euros-por-empresa.

7. RECOLECCIÓN DE INFORMACIÓN DE ATAQUES EN ARCHIVOS DE WORD Y EXCEL

7. 1. Determinar la forma con que se van a registrar los datos.

Los datos ya se encuentran registrados a través de estadísticas internacionales, los cuales informan de la existencia y de veracidad de los ataques, Microsoft presenta unas estadísticas en general, sobre los ataques de algunos de los Ransomware que afectan principalmente a los productos de ofimática, ya que es el software más usado del mundo en el procesamiento de datos.

También se pueden evidenciar relatos de robo de información en la cual no hay pérdida económica si no perdida investigativa que puede influir en un caso, decisión o determinación.

7. 2. Observar cuidadosa y críticamente.

A continuación, se muestra el comportamiento de algunos virus Ransomware

7. 2. 1. Ransom: Win32/Crilock. A

Comportamiento de la amenaza.
Instalación.
La amenaza podría ser descargada por otros malware.

Instala una copia de sí mismo como *%APPDATA%*\Roaming\{*azar* GUID}.exe, por ejemplo *%APPDATA%*\Roaming\{1400BEBE-1503-1236-2800-383F060F181A}.exe.

Hace los siguientes cambios en el registro para que se ejecute cada vez que inicie el PC:
Modifica en la subclave:
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
Establece valor: "CryptoLocker "
Con datos: "*%APPDATA%*\Roaming\{*azar* GUID}.exe", por ejemplo"*%APPDATA%*\Roaming\{1400BEBE-1503-1236-2800-383F060F181A}.exe "

Capacidad de carga.

Impide acceder al escritorio.
Como parte de la carga del equipo PC, esta amenaza muestra una página web de pantalla completa que cubre todas las otras ventanas y solo se muestra así

misma, haciendo inutilizable el PC. La advertencia pedirá pagar una cuota para recibir una clave generada aleatoriamente que "desbloqueará" los archivos y permitirá recuperar el acceso al PC “teóricamente”. El Ransomware muestra un reloj de cuenta regresiva, cuenta regresiva de 72 horas o similar y le ofrece las siguientes opciones de pago para pagar la "multa":

- Bitcoin
- cashU
- MoneyPak
- paysafecard
- Ukash

La llave que "abre" el PC es única; usted no podrá utilizar la clave de otra persona. Tenga en cuenta que estos sistemas de pago en línea no están asociados con esta amenaza de alguna manera.

Las siguientes figuras 20, 21, 22, 23 son algunos ejemplos de imágenes que muestra Crilock.A:

Figura 20 Aviso de Secuestro.

Fuente: MICROSOFT. Ransom:Win32/Crilock.A. [en línea] 15 de septiembre de 2017 [revisado Abril 2017], disponible en internet: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Ransom:Win32/Crilock.A

Figura 21 Aviso de Secuestro.

Fuente: MICROSOFT. Ransom:Win32/Crilock.A. [en línea] 15 de septiembre de 2017 [revisado Abril 2017], disponible en internet: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Ransom:Win32/Crilock.A

Figura 22 Aviso de Pago.

Fuente: MICROSOFT. Ransom:Win32/Crilock.A. [en línea] 15 de septiembre de 2017 [revisado Abril 2017], disponible en internet: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Ransom:Win32/Crilock.A

Figura 23 Método de Pago.

Fuente: MICROSOFT. Ransom:Win32/Crilock.A. [en línea] 15 de septiembre de 2017 [revisado Abril 2017], disponible en internet: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Ransom:Win32/Crilock.A

Cifrar archivos

El Ransomware cifra archivos en el PC que encuentra, en la búsqueda se encuentran unidades fijas y remotas, encriptando todo lo que encuentre. En la naturaleza, el malware se ha observado el uso de los algoritmos RSA y AES para este propósito.

Crilock.A cifra los archivos que encuentra en las unidades fijas y remotas con las siguientes extensiones:

- . 3fr
- . ccdb
- . ai
- . arw
- . bay
- . cdr
- . cer
- . cr2
- . crt
- . crw
- . dbf
- . dcr
- . der
- . dng
- . doc
- . docm
- . docx
- . dwg
- . dxf
- . dxg
- . eps
- . erf
- . indd
- . jpe
- . jpg
- . kdc
- . mdb
- . mdf
- . mef
- . mrw
- . nef
- . nrw
- . odb
- . odc
- . odm
- . odp
- . ods
- . odt
- . orf
- . p12
- . p7b
- . p7c
- . pdd
- . pef
- . pem
- . pfx
- . ppt
- . pptm
- . pptx
- . psd
- . pst
- . ptx
- . r3d
- . raf

- . raw
- . rtf
- . rw2
- . rwl
- . sr2
- . srf
- . srw
- . wb2
- . wpd
- . wps
- . x3f
- . xlk
- . xls
- . xlsb
- . xlsm
- . xlsx

7. 2. 2. Ransom: Win32/Trasbind. A

Comportamiento de amenaza
Instalación
Este troyano emite copias casi propias como estos archivos, lo que resulta en archivos críticos de sistema de Windows se sobrescriban e infecten el PC:

- *%windir%* *explorer. exe*
- *%windir%* *System32\taskmgr. exe*
- *%windir%* *System32\userinit. exe*
- *%windir%* *System32\dllcache\taskmgr. exe*
- *%windir%* *System32\dllcache\userinit. exe*

El troyano también puede infectar el PC con estos nombres:

- *%windir%* *System32\03014d3f. exe*
- *%APPDATA%* *22cc6c32. exe*

Cambiando el registro para que la copia se ejecute cada vez que se inicia Windows.

En la subclave:
HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon
Establece valor: "*Shell*"
Datos: "*%APPDATA%\22cc6c32. exe*"

Capacidad de carga
Le impide usar el PC.
El troyano le impide usar el PC, en su lugar, emite el mensaje de alerta diseñado para alarmar al usuario, tal como se muestra en la figura 24:

Figura 24 Aviso Secuestro.

Fuente: MICROSOFT. Ransom:Win32/Trasbind.A. [en línea] 15 de septiembre de 2017 [revisado Abril 2017], disponible en internet: https://www. microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan%3AWin32%2FTrasbind.A&ThreatID=-2147322034

7. 2. 3. Ransom: Win32/Cribit.A

Comportamiento de amenaza
Instalación
Trojan:Win32/Cribit.A se ubica en la carpeta %APPDATA% utilizando un nombre de archivo aleatorio de 5 a 15 caracteres aleatorio. Por ejemplo, un archivo que analizamos fue nombrado *%APPDATA%*\ylohf.exe.

También crea la siguiente entrada del registro para que se ejecute automáticamente cada vez que inicia Windows:
En la subclave: HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Establece valor: "Bitcomint "
Con datos: "*%APPDATA%*\ < *nombre de archivo de malware* >.exe"
Por ejemplo:

En la subclave: HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Establece valor: "Bitcomint "
Con datos: "*%APPDATA%*\ylohf.exe "
También emite otros archivos como parte del proceso de instalación como:

- bitcrypt.ccw - archivo de configuración de malware
- del.bat - archivo por lotes, que usa para ejecutarse a sí mismo; una vez que ha hecho la rutina maliciosa, utiliza otra vez este archivo eliminar a sí mismo para que no quede traza o rastro en el PC.

Capacidad de carga

Le impide ejecutar Task Manager y Registry Editor
Trojan: Win32/Cribit. A comprueba continuamente para ver si cualquiera de estos procesos se está ejecutando y si es así, los finaliza:

- taskmgr. exe (Task Manager)
- regedit. exe (Registry Editor)

Impide iniciar en modo seguro

Esta amenaza elimina estas claves del registro. Sin estas claves del registro y configuración, no puede reiniciar el PC en Safe Mode:

- HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network
- HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal

También ejecuta estos comandos:

<u><*system folder*></u> \cmd. exe" /K bcdedit /set {bootmgr} displaybootmenu no *-este comando impide que* Windows *muestra el* Windows Boot Manager <u><*system folder*></u>\cmd. exe" /K bcdedit /set {default} bootstatuspolicy ignoreallfailures *-este comando desactiva el* Windows System Recovery *al iniciar el PC*

Cifra archivos

Trojan:Win32/Cribit.A busca archivos con estas extensiones en todas las unidades de disco:

- *. abw
- *. arj
- *. asm
- *. bpg
- *. cdr
- *. cdt
- *. cer
- *. css
- *. dbt
- *. dbx
- *. dfm
- *. djv
- *. djvu
- *. doc
- *. docm
- *. docx
- *. dpk
- *. dpr
- *. frm
- *. gz
- *. jpeg
- *. jpg
- *. key
- *. lzh
- *. lzo
- *. mdb
- *. mde
- *. odc
- *. pab
- *. pas
- *. pdf
- *. pgp
- *. php

- *. pps
- *. ppt
- *. pst
- *. rtf
- *. sql
- *. text
- *. txt
- *. vbp
- *. wri
- *. xfm
- *. xl
- *. xlc
- *. xlk
- *. xls
- *. xlsm
- *. xlw
- *. xsf
- *. xsn
- *. cdx
- *. dbf
- *. js
- *. vsd
- *. xlsx

Para cada archivo que encuentre, codificara el archivo con AES key. El archivo cifrado tiene la extensión. bitcrypt o. bitcrypt2.

Trojan: Win32/Cribit.A imprime la nota de rescate como el archivo bitcrypt. txt en cada una de las carpetas que cifra [archivos].

Una vez que ha codificado todos los archivos del objetivo, abre la nota de rescate y cambia el fondo de escritorio a la siguiente (Observe que el texto es de diseño, como lo muestra la figura 25 a continuación):[10]

Figura 25 Aviso de Secuestro.

Fuente: MICROSOFT. Ransom:Win32/Cribit.A. [en línea] 15 de septiembre de 2017 [revisado Abril 2017], disponible en internet: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Ransom:Win32/Cribit.A

[10] MICROSOFT. Ransomware. [en línea] no posee fecha [Revisado Marzo de 2018] , Disponible en internet: https://www. microsoft. com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Ransom:Win32/Crilock. A

7. 2. 4. Ransom: Win32/Adslock. A

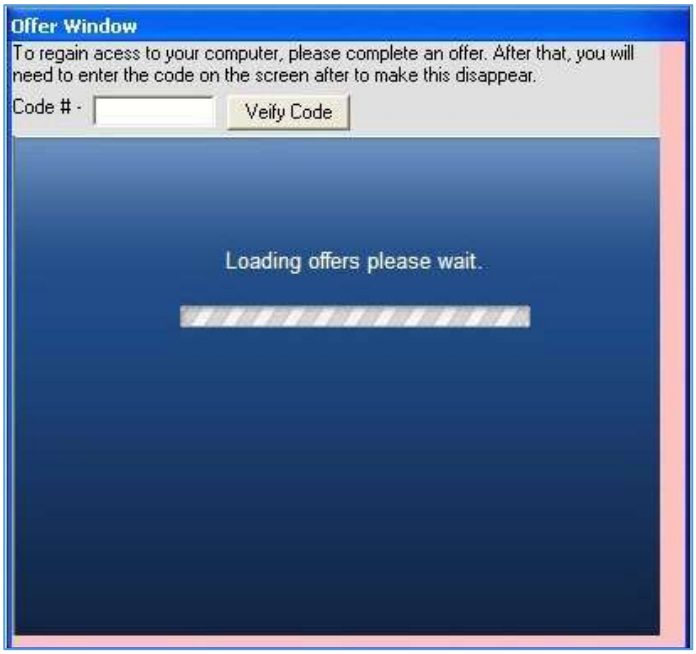
Comportamiento de amenaza Win32/Adslock. A
Esta amenaza es un programa malicioso diseñado para bloquear el escritorio del Pc y así obligar al usuario a completar una oferta que supuestamente desbloquee la pantalla.

Instalación
Se autocopia en la carpeta de inicio de Windows para que se ejecute automáticamente cada vez que un usuario inicia sesión o iniciar Windows.

Capacidad de carga
Realiza cambios de escritorio
La amenaza deshabilita al administrador de tareas, así como oculta la barra de tareas del sistema.

También intenta bloquear el escritorio y muestra una solicitud para completar una oferta para desbloquear la pantalla, como lo informa la figura 26 a continuación:

Figura 26 Aviso de Secuestro.



Fuente: MICROSOFT. Ransom:Win32/Adslock.A. [en línea] 15 de septiembre de 2017 [revisado Abril 2017], disponible en internet: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Ransom:Win32/Adslock.A

Detrás de la "Offer Windows", inicia la amenaza con un HTTP que solicita la siguiente página:

- watchhow. <removed>yi. am/lock/#1#1#0#YouAre<removed>jile#1#

El servidor responde con un mensaje que dice "You are Locked" y muestra imágenes no deseadas que implica que el usuario está viendo contenido inapropiado, como se muestra en la figura 27:

Figura 27 Aviso de Secuestro/Bloqueo.

Fuente: MICROSOFT. Ransom:Win32/Adslock.A. [en línea] 15 de septiembre de 2017 [revisado Abril 2017], disponible en internet: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Ransom:Win32/Adslock.A

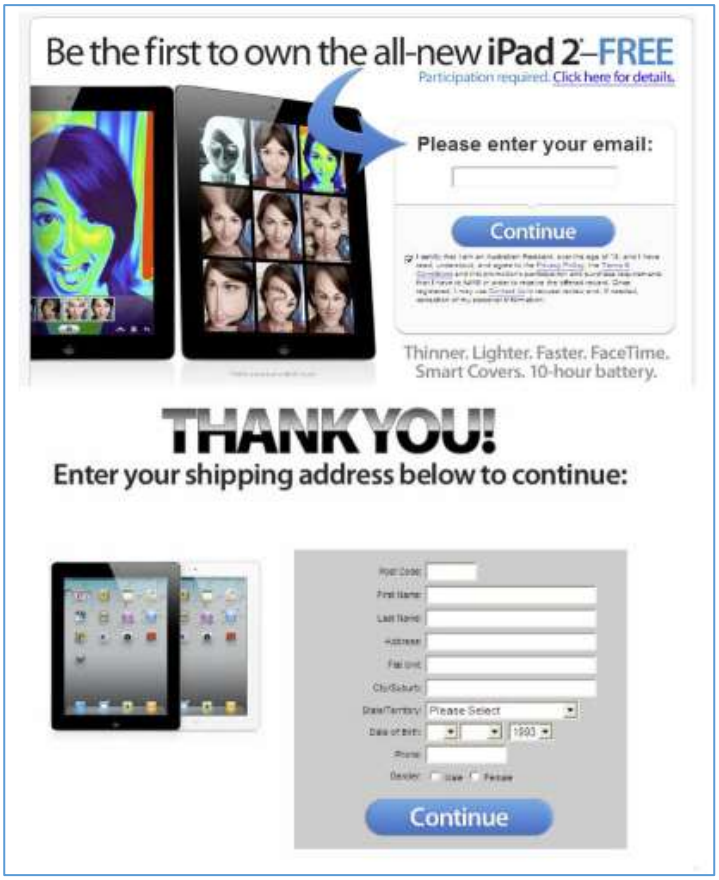
El mensaje induce que el usuario pueda completar cualquiera de las dos ofertas. Esto conduce a ver las promociones con ofertas que el usuario ha ganado un premio, como se informa en la figura 28:

Figura 28 Aviso de Enganche de secuestro.

Fuente: MICROSOFT. Ransom:Win32/Adslock.A. [en línea] 15 de septiembre de 2017 [revisado Abril 2017], disponible en internet: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Ransom:Win32/Adslock.A

Sin embargo, al usuario le requerirá una dirección de correo electrónico y el Personal identificable Information (PII) en Colombia la cedula, para reclamar el premio como se informa a continuación en la figura 29:

Figura 29 Enganche para el secuestro.



Fuente: MICROSOFT. Ransom:Win32/Adslock.A. [en línea] 15 de septiembre de 2017 [revisado Abril 2017], disponible en internet: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Ransom:Win32/Adslock.A

Muestra anuncios

La amenaza se conecta a los siguientes servidores, que son conocidos para servir este tipo de anuncios:

- *theabc<removed>photo. com*
- *wegetpaid. net*

Información adicional

Esta amenaza es generada por un causante, que es detectado como: Win32/Adslock. A. [11]

[11] MICROSOFT. Ransomware. [en línea] no posee fecha [Revisado Marzo de 2018] , Disponible en internet: https://www. microsoft. com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Ransom:Win32/Adslock. A

7. 2. 5. Ransom: Win32/Sofilblock. A

Comportamiento de amenaza

Instalación
Esta amenaza se copia a sí mismo como el siguiente archivo:
%AppData%\sopaps.exe
También crea la siguiente entrada del registro para que se ejecute cada vez que inicia Windows:
En la subclave: HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Establece valor: "ChpPrintUpdate "
Con datos: "%AppData%\sopaps.exe "
También puede crear los siguientes archivos, que pueden contener la clave de cifrado que puede descifrar los archivos:

- %AppData%\filesop.txt. block
- %AppData%\ok. txt.block

Capacidad de carga
Se conecta a determinados servidores
Puede conectarse a ciertos servidores para generar la clave de cifrado:

- 78. 47. 4. 76
- 176. 9. 237. 54

Cifra archivos
Utilizando la clave de cifrado, la amenaza encripta todos los archivos en el Equipo PC con cualquiera de las siguientes extensiones:

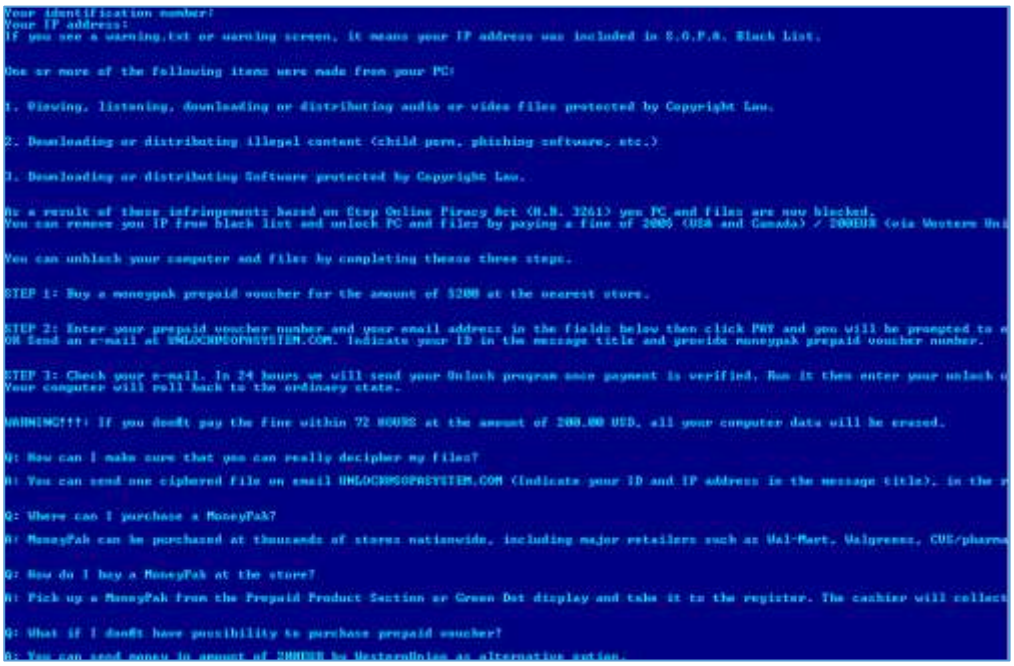
- abw
- arj
- asm
- bpg
- cdr
- cdt
- cdx
- cer
- chm
- css
- dbf
- dbt
- dbx
- dfm
- djv
- djvu
- doc
- docm
- docx
- dpk
- dpr
- frm
- gz
- gzip
- htm
- html
- jpg
- js
- key
- lzh
- lzo
- mdb
- mde
- odc
- pab
- pas
- pdf
- pgp
- php
- pps
- ppt
- pst
- rtf
- sql
- text

- txt
- vbp
- vsd
- wri
- xfm
- xl
- xlc
- xlk
- xls
- xlsm
- xlsx
- xlw
- xsf
- xsn

Se re nombran los archivos cifrados como "< nombre de archivo antiguo >. < vieja extensión >. block", por ejemplo, "C:\Samplefile. txt" a "C:\Samplefile. txt. block".

En cada carpeta con al menos un archivo encriptado, escribe un archivo "warning.txt", que contiene el texto siguiente de la figura 30:

Figura 30 Aviso de Secuestro.

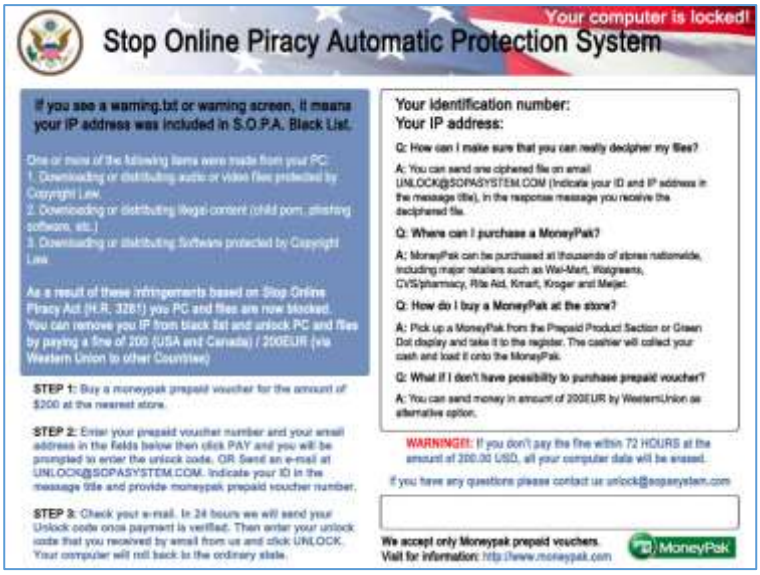


Fuente: MICROSOFT. Ransom:Win32/Sofilblock.A. [en línea] 15 de septiembre de 2017 [revisado Abril 2017], disponible en internet: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Ransom:Win32/Sofilblock.A

Bloquea el Equipo PC

La amenaza plantea como una institución legítima coacciona a los usuarios para pagar una cuota. Se impide acceder al escritorio y sustituye a la pantalla con una imagen similar a la informada en la figura 31:

Figura 31 Aviso de Secuestro.



Fuente: MICROSOFT. Ransom:Win32/Sofilblock.A. [en línea] 15 de septiembre de 2017 [revisado Abril 2017], disponible en internet: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Ransom:Win32/Sofilblock.A

Finaliza proceso

Para evitar terminar el proceso, termina los procesos "taskmgr.exe" y "regedit.exe" Se ejecutan, pero no se deja terminar los procesos modo oculto restringido. [12]

[12] MICROSOFT. Ransomware. [en línea] no posee fecha [Revisado Marzo de 2018] , Disponible en internet: https://www. microsoft. com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Ransom:Win32/Sofilblock. A

8. ESTRATEGIAS PARA LA DISMINUCIÓN DE FUGA, ROBO Y SECUESTRO EN ARCHIVOS DE WORD Y EXCEL

8. 1. ESTRATEGIAS PARA DISMINUIR EL ROBO, FUGA HURTO Y SECUESTRO.

Dentro de las estrategias para mitigar las problemáticas de hurto se sugiere la creación de una aplicación de la cual se darán algunas pautas, de igual forma se plantean otras estrategias posibles en seguridad informática.

La siguiente es la propuesta que se intenta aplicar a este problema, como medida de mitigación al problema:

8. 1. 1. PLUGINS

Es un programa que está en capacidad de adherirse al software deseado, para ello se debe entender las variables y el lenguaje que maneje el software base, para este caso Word, Excel, Windows, este plugins estará basado en las variables y objetos de programación divulgados para la operación y manejo del paquete ofimático de Microsoft, la forma de interactuar del plugins estará bajo la experticia del desarrollador.

8. 1. 1. 1. Infraestructura para el desarrollo del plugins

Descripción de la infraestructura:

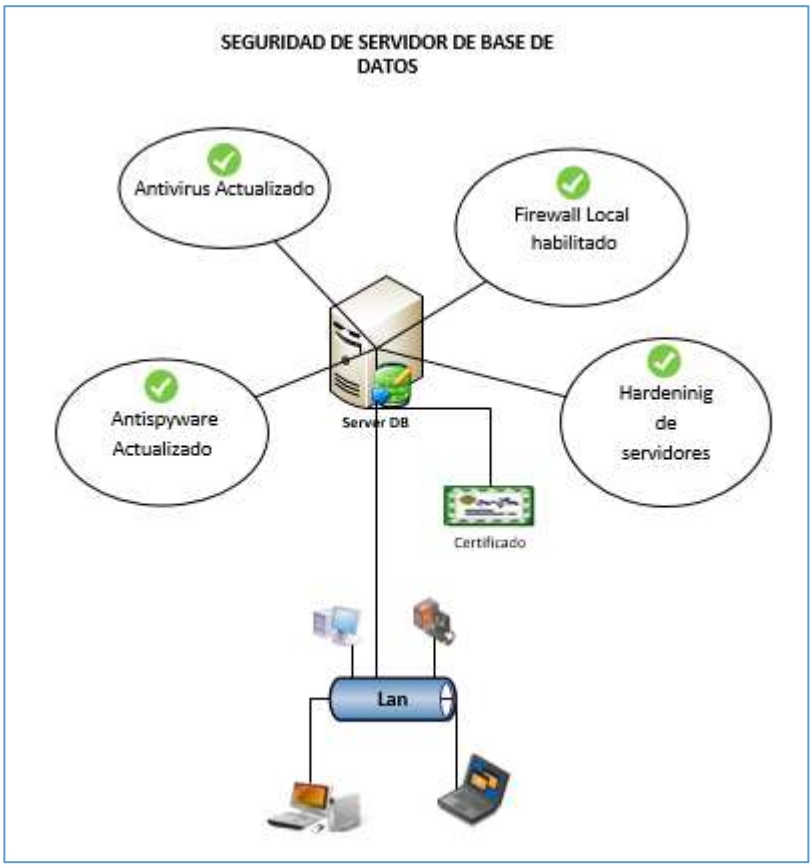
Requisitos de la infraestructura Servidor.

Para un mínimo [inicialmente con productos Microsoft, en una empresa pyme de máximo 30 usuarios, sin soporte de disponibilidad], se debería tener un servidor para la aplicación y base datos, dicho servidor debe contar con las siguientes características:

- 1 procesador de 6 núcleos.
- 8 Gb de memoria.
- Un disco de 200 GB para el sistema operativo.
- Disco duro de 700 GB para la base de datos [expandibles según proyección de la implementación] para los datos a almacenamiento.
- Una tarjeta de red de mínimo 1 GB

A continuación, se muestra en la figura 32 un esquema de infraestructura para el servidor de la aplicación y bases de datos.

Figura 32 Seguridad en servidor de base de datos.



Fuente: el autor.

El sistema operativo instalado debe ser mínimo Windows 2012 server versión standard, más la aplicación MS SQL server 2012 estándar.

El servidor debe contar con un antivirus instalado y actualizado diariamente, con un sistema de firewall local activo y con los permisos o reglas permitidas, permisos concedidos para puertos como es el caso de MSSQL server en el puerto 1433 asignado por defecto, File and printer sharing, icmp v4 o v6 y otros puertos por defecto activados para el antivirus, puertos para agentes de backup, etc.

Requisitos de la infraestructura Red.

El servidor debe estar bajo una infraestructura de red con cableado estructurado 100 Mb por segundo como mínimo, topología estrella con Switches que soporten

velocidades mínimas de 100Mb/s interconectados y administrables mínimo capa 3 con ámbitos de seguridad de Vlan.

También se recomienda que dentro del ámbito de seguridad se deben tener otros elementos mínimos como firewall perimetral, IDS/IPS, Antispam, servidores de antivirus, servidores de certificados, servidores de directorio activo, etc.

En el ámbito de red se debe trabajar con un dominio, el servidor de aplicación de seguridad de archivos ofimáticos debe estar unido al dominio, y por lo tanto debe tener una cuenta administradora para el aplicativo independiente, los clientes deben estar unidos al dominio, ya que por medio de este se harán las identificaciones de los usuarios en red.

Adicionalmente se debe contar con medidas básicas de seguridad como:

Los servidores de aplicación y de base de datos, que deben generarse bajo los lineamientos de seguridad respectivos para cada sistema operativo, puede ser a través de plantillas, esto consiste en limitar los puertos de firewall a usar solo los que sean usados, limitar los servicios, por ejemplo: eliminar/bloquear cuentas que no se necesiten como la de invitados, restringir el acceso a los usuarios por defecto o no autorizados a los servidores por defecto, ingresar con accesos certificados [firmar las comunicaciones], Configurar tipos de cifrado en kerberos, habilitar políticas de auditoria, etc.

Descripción del proceso.

El proceso inicia con varias entradas, una de ellas es cuando un usuario crea un documento nuevo, para esto el usuario debe tener instalado el plugins que se abrirá inmediatamente capturando los datos del usuario logueado y conectando directamente en el servidor al usuario, con esto el usuario estará en sesión directamente con el servidor de la aplicación, dados estos accesos el usuario puede abrir los archivos que se encuentren almacenados en el servidor y que sean de pertenencia o compartidos bajo los privilegios asignados previamente.

Posteriormente el usuario puede observar que el zoom del Word estará desactivado y tendrá un porcentaje más alto al 100% [esto minimizará la toma de información por medio de fotos u otros medios externos] el usuario puede iniciar a trabajar con el aplicativo y las restricciones dada anteriormente y administradas por el plugins.
El usuario puede obtener el documento que para entonces se guarde en la base de datos directamente, el almacenamiento de la información se hará mediante el plugins el cual a su vez se guardara temporalmente en el server e inmediatamente desarmara el archivo y lo almacenará [según opciones que el usuario haya guardado para mayor claridad se debe observar los títulos de estructura de los archivos Word o Excel]

Otra de las entradas del proceso es la apertura de un archivo enviado por correo electrónico, una vez recibido el correo electrónico y cuando el usuario intente abrir el archivo ofimático se activará el plugin y se desarmará en una tabla temporal y será revisado en primer lugar por el antivirus, posteriormente el documento será restringido para evitar la copia, la impresión, print screen.

A continuación, se muestran algunos flujogramas de la aplicación como se observa en la figura 40.

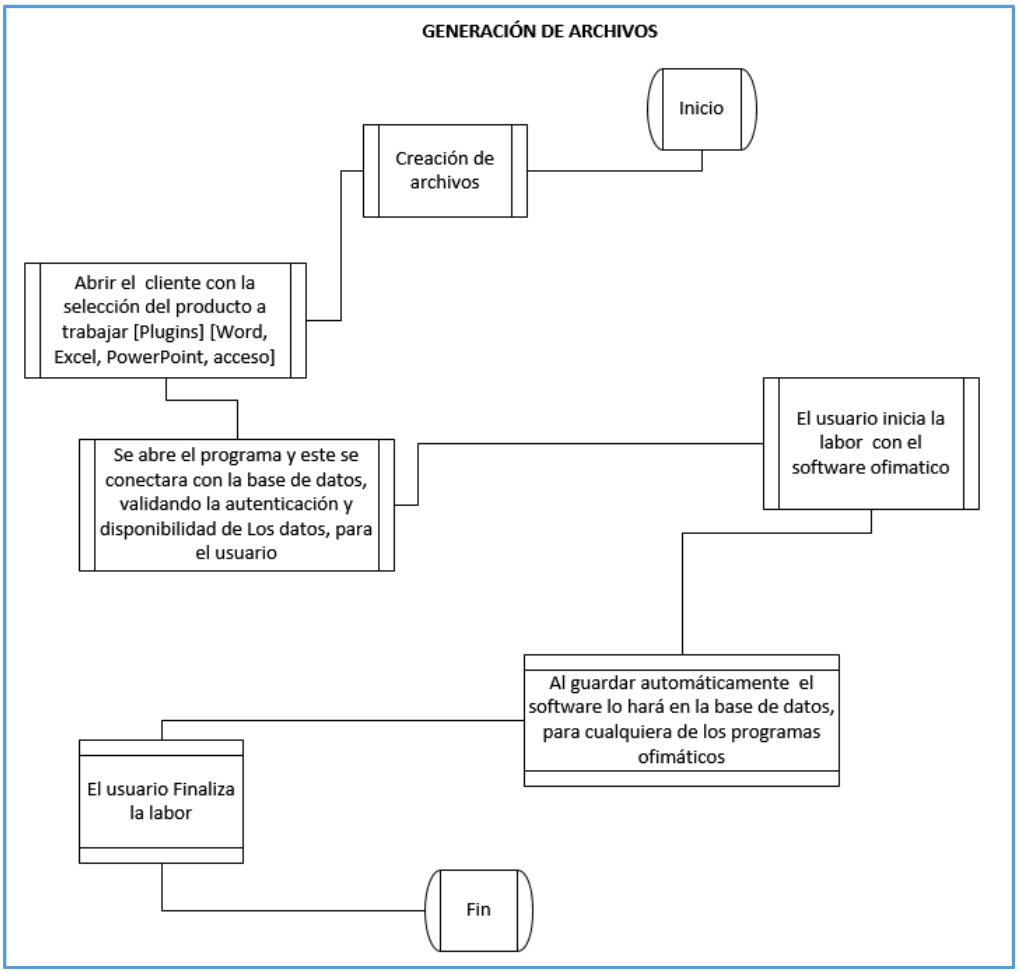
El usuario visualizara el documento con el zoom deshabilitado y superior a 100%.

Para todos los casos el plugins evitara que el usuario pueda copiar, imprimir, generar la acción de print screen o imprimir lo observado en pantalla, envío directo de archivos por correo, compartir los archivos.

A continuación, se muestra algunos de los flujogramas que se deben usar para el plugins.

En la figura 33 se muestra un flujo de trabajo para la generación de nuevos archivos que inician desde el cliente conectado al servidor hasta el almacenamiento.

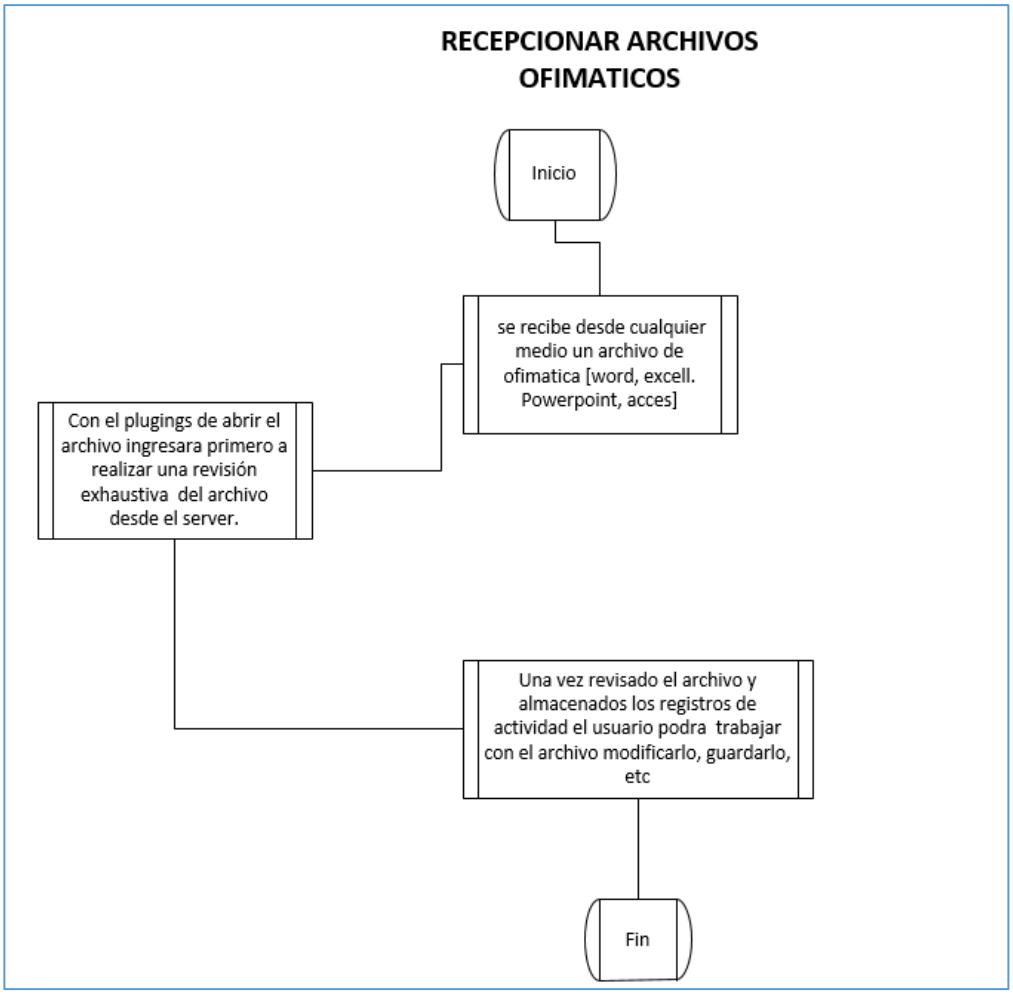
Figura 33 Flujo de trabajo con generación de archivo.



Fuente: el autor.

En la figura 34 se describe el ingreso de un archivo Informatico mediante otro medio de almacenamiento [opcional], el archivo será validado mediante el antivirus y se almacena la actividad que se realice con este.

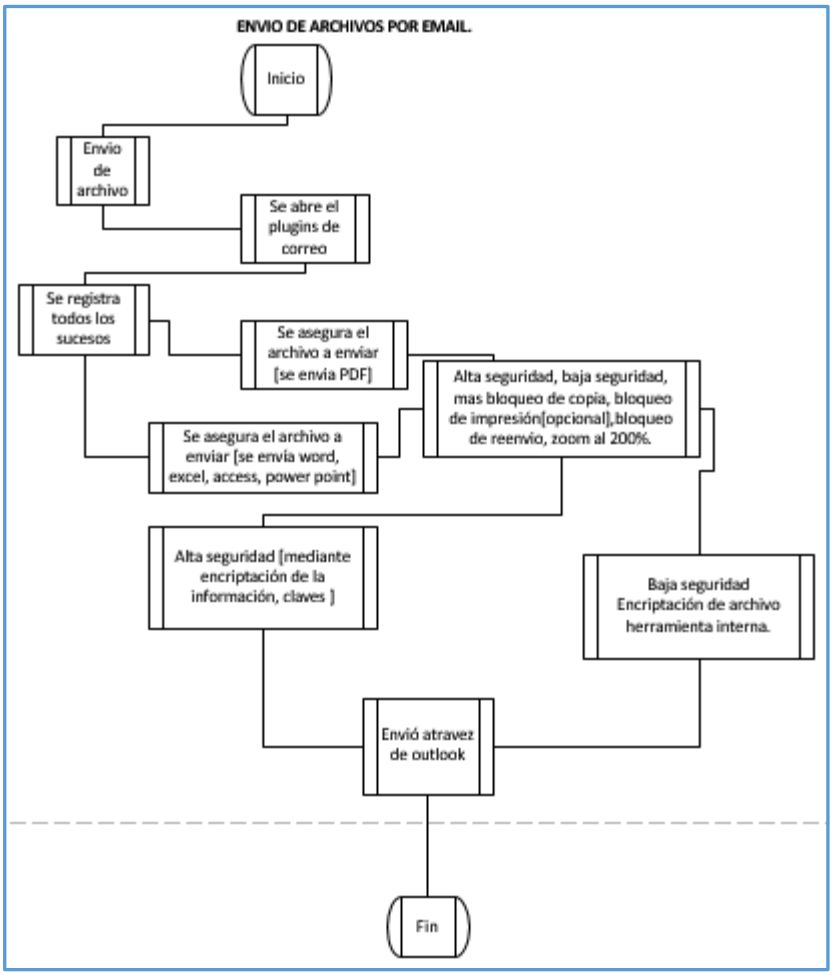
Figura 34 Solución trabajo con archivos recibidos.



Fuente: el autor.

En la figura 35 se describe el ingreso de un archivo Informatico mediante Outlook, al ejecutar el Word, Excel se activará el plugins, el archivo será enviado al servidor donde será validado por el antivirus y se almacenará la actividad que se realice con este.

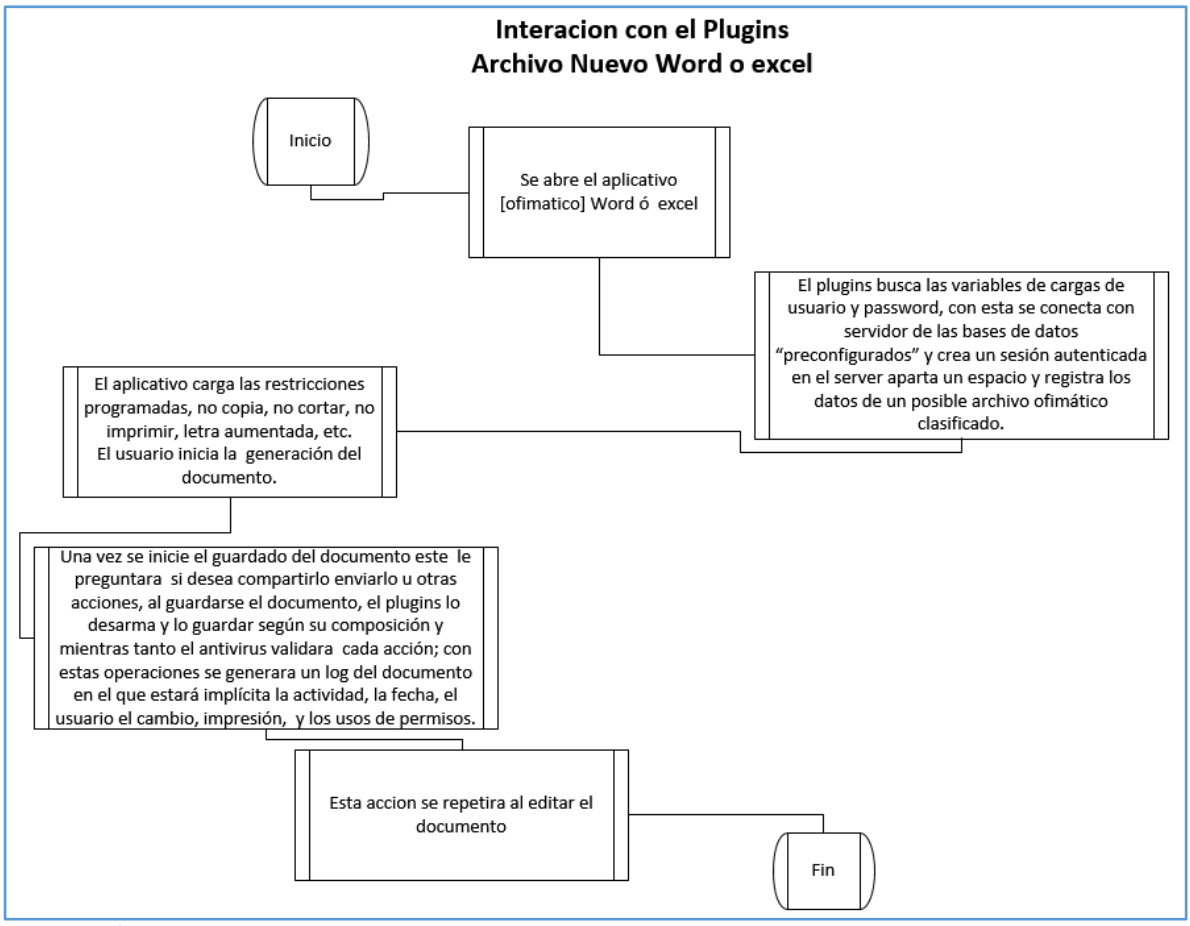
Figura 35 Solución de trabajo envío por correo electrónico, Aseguramiento.



Fuente: el autor.

En la figura 36 se observa el proceso de creación de un archivo ofimático nuevo, como se comporta la aplicación y su almacenamiento.

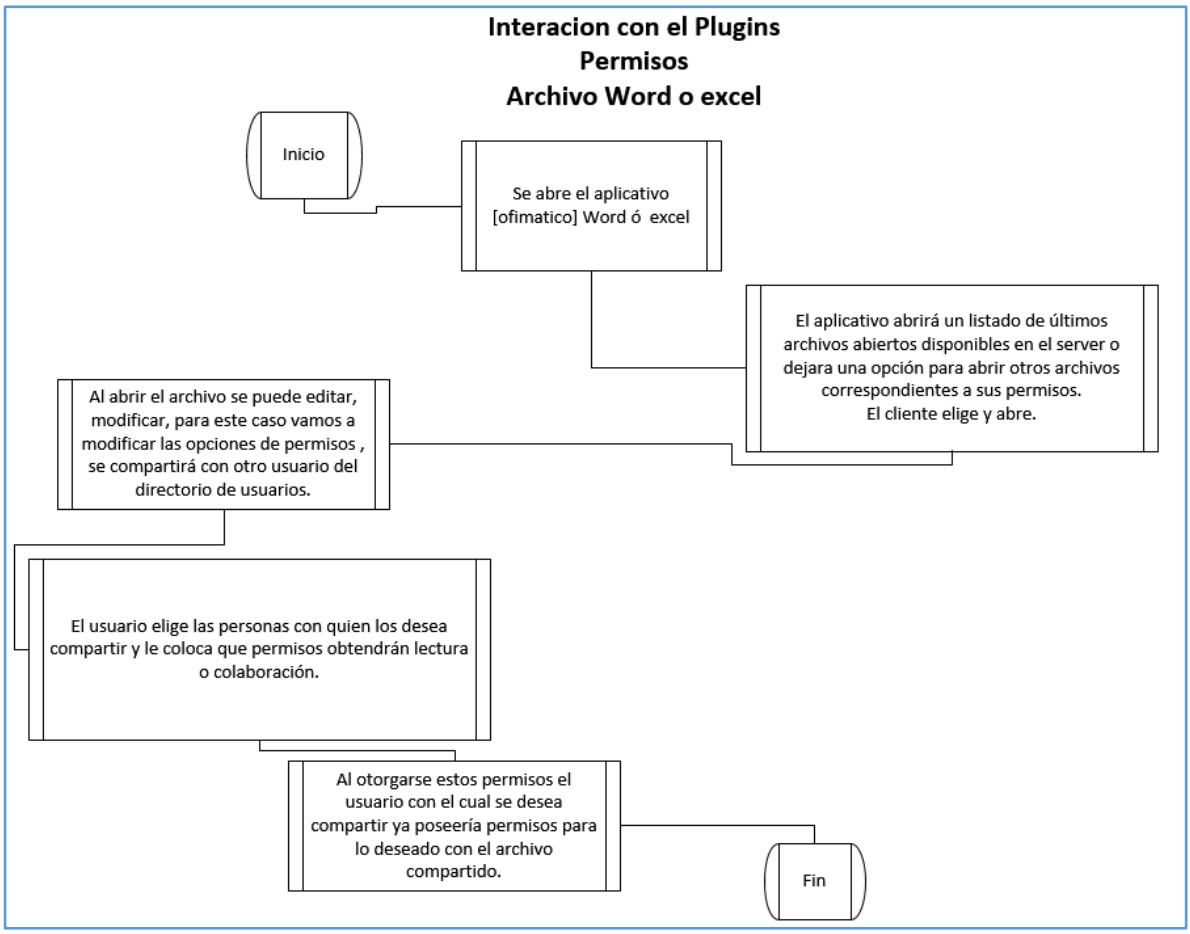
Figura 36 Interacción plugins archivo nuevo ofimático.



Fuente: el autor.

En la figura 37 se muestra el proceso de gestión de permisos y el proceso de consulta de datos.

Figura 37 Interacción plugins permisos archivo ofimático.



Fuente: el autor.

8. 1. 1. 2 Requisitos para el funcionamiento del plugin:

Requisitos Cliente.

Los clientes deben estar basados en productos Microsoft es decir el requisito mínimo Windows 8 profesional más office 2013 instalado, así mismo debe poseer el hardware suficiente para soportar la instalación y configuracion recomendada por Microsoft fabricante de Windows y office, adicionalmente el cliente debe tener instalado el plugins el cual hará la interface con el server.

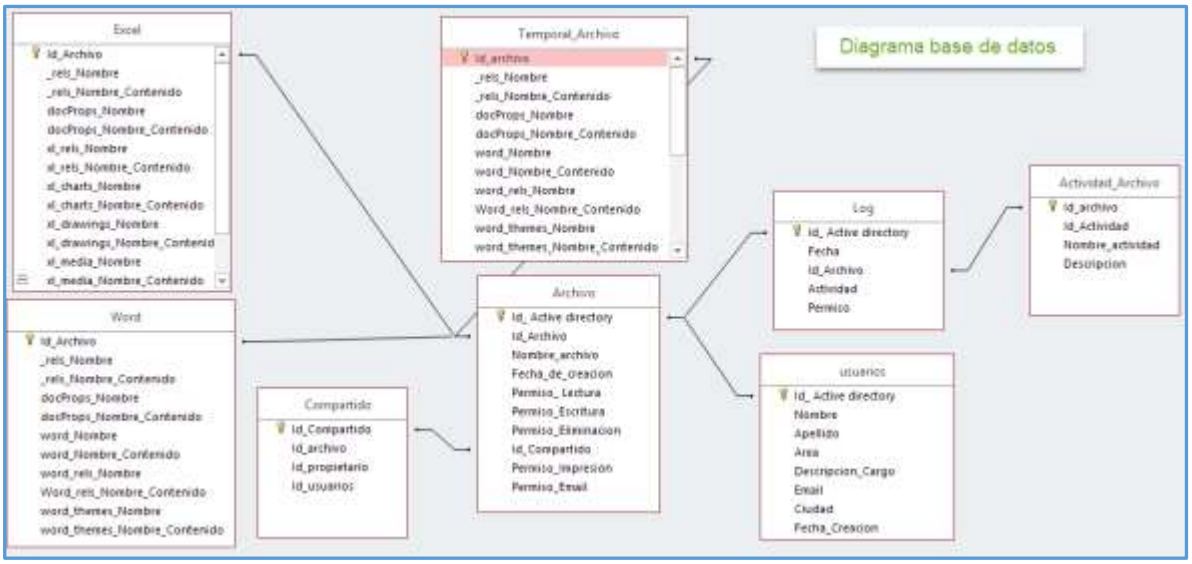
Restricciones de almacenamiento de OneDrive, google drive, USB, etc. ya sea a nivel físico o nivel wifi, bluetooth, únicamente se recibe información por correo electrónico desde ámbitos externos y a nivel interno a través del aplicativo.

Este servidor contara con atención centralizada en cuanto a las actualizaciones de seguridad antivirus, inspección de la composición origen (se desarmará el XML se revisará y se almacenara en el servidor, haciendo más eficiente la inspección y el almacenamiento de los archivos, no solo en el almacenamiento sino en el respaldo eficiente de la información.

Se debe tener una base de datos con todas las características de seguridad como antivirus, firewall local, certificados de aplicaciones, permisos, cifrado de la arquitectura de las tablas y otros, cabe anotar que la infraestructura debe tener los componentes de seguridad como ips/ids, Antispam, antivirus para cada máquina, firewall general, etc., por parte de los usuarios deben tener instalado y configurado el componente del plugins que conectara con la base de datos, otorgara permisos, visualizaciones y otras restricciones configuradas.

El desarrollo de la base de datos puede ser estructurada siguiendo el siguiente diagrama mostrado en la figura 38, la cual contiene tablas y los campos de almacenamiento de información.

Figura 38 Estructura general de la bases de datos.



Fuente: El autor.

8. 1. 1. 3. Acciones del plugins:

En el cliente se debe instalar un plugins que puede ser diseñado y escrito en cualquier software que sea compatible con Microsoft Windows y Office, preferiblemente en lenguaje .Net, este se encargará de que cualquier equipo que abra, cree, consulte o modifique un archivo ofimático se debe hacer desde el aplicativo que se comunicara con el servidor y allí se almacenara si es necesario

como única forma de consulta creación, modificación y eliminación, por lo tanto el plugins tendrá conexión directa a una sesión autenticada del usuario y a los archivos en el servidor de base de datos. Una forma de lograr estas tareas es apoyándose en las variables de sesión de Windows que permiten conocer la sesión del usuario como se muestra en el siguiente código:

Variables de la sesión Windows

Console. WriteLine("UserName: {0}", Environment. UserName)
los cuales sirven para capturar los inicios de sesión disponibles en ese momento ejemplo:

```
Imports System
Class Sample
  Public Shared Sub Main ()
    Console. WriteLine()
    Console. WriteLine("UserName: {0}", Environment. UserName)
  End Sub 'Main
End Class
```
[13]

Una vez tomado el usuario se debe almacenar para la creación de la sesión en la base de datos, esta también sirve para identificar los archivos del usuario en la base de datos.

Posteriormente se debe generar la conexión a la base de datos desde el cliente, este permitirá el ingreso, consulta, modificación y en algunos casos la eliminación de datos de los archivos propietarios, las conexiones a la base de datos pueden ser realizada como se aprecia en el siguiente código:

```
myConnectionString = "Provider=sqloledb;" & _
                     "Data Source=servidorsql;" & _
                     "Initial Catalog=nombre de la base de datos;" & _
                     "User Id=NombreUsuario;Password=contraseñaPrueba"
```

Cuando esté conectado se tendrá el acceso a los documentos propietarios, mediante consultas tipo select dentro del plugins y no visible para el usuario, estas consultas sirven para preguntarle a la base de datos si se tiene permiso para consultar otros archivos [caso de archivos compartidos, impresión de archivos, envió de archivos por correo electrónico]. El desarrollo de estas consultas se puede realizar teniendo en cuenta el siguiente código:

[13]Microsoft. Propiedad Environment. UserName. [en línea] Noviembre 2016 [revisado Abril 2018], Disponible en internet: https://msdn.microsoft.com/es-es/library/system. environment. username(v=vs. 110). aspx

```
Dim s As String = ("SELECT Archivo FROM Permiso_lectura")
myCommand = New OleDbCommand(s)
myCommand. ExecuteNonQuery()
```
[14]

El plugins también tiene la responsabilidad de:

Bloqueo de tecla Print screen: para el bloqueo de la tecla print screen se puede usar La siguiente función desarrollada en JavaScript y que es compatible con . net

```
function checkKeyPressed(e) {
    if (e. keyCode == "44") {
        alert("The print screen button was pressed. ");
    }
}
window. addEventListener("keyup", checkKeyPressed, false);
```

No existe copiado directo, se deshabilita los modos de copiado e impresión.

```
Private Sub Document_Open()
CommandBars("Standard"). Controls(3). Delete
CommandBars("Standard"). Controls(5). Delete
CommandBars("Standard"). Controls(7). Delete
CommandBars("Standard"). Controls(7). Delete
CommandBars("File"). Controls(4). Delete
CommandBars("File"). Controls(4). Delete
CommandBars("File"). Controls(4). Delete
CommandBars("File"). Controls(11). Delete
End Sub
```

Y el que sigue en el evento Close del mismo.

```
Private Sub Document_Close()
CommandBars("Standard").  Reset
CommandBars("File").  Reset
End Sub
```
[15]

Aumento de la letra mostrada [zoom] y bloqueo de la misma.
Validación de macros vía XML con descomposición del archivo recibido desde el server a nivel del antivirus.

Otras restricciones como de impresión, modificación, copiado, etc. en él envió de correos con archivos ofimáticos

Ingreso a través del aplicativo de los archivos informáticos de correo Outlook

Por defecto únicamente con la aplicación.

---

[14] Navés Solé, Jordi . [en línea] julio 28, 2014. [revisado Abril 2018], Disponible en internet: http://www. jnsoft. net/blog/connexion-base-datos-sqlserver-con-vb-net/

[15] Tomado de https://social. msdn. microsoft. com/Forums/es-ES/db3b8a32-3019-416d-a93a-89d5386bc37b/como-bloquear-el-copiar-en-word-usando-vb6?forum=vstoes

No hay compartido directo de archivos solo con la aplicación.
Compartido directo con permisos a través del aplicativo y la base de datos, se debe generar una consulta en las tablas para el archivo y el usuario depende de los permisos se dará acceso o no.

Para el caso de los archivos enviados a través de correo estos al iniciar desde el equipo se creará en el servidor una carpeta temporal que también se almacenará en la base de datos en la tabla temporal descomponiéndose en archivos para ser validados mediante el antivirus antes de ser mostrados a los usuarios finales, de esta forma se filtrará correctamente el archivo.

En la base de datos del server se almacenará cualquier operación que se pueda dar con los archivos ofimáticos, todo esto con el fin de auditar y registrar.

Con este planteamiento se contribuye a la disminución del riesgo e impacto a los archivos informáticos.

Para este ejemplo se toma el lenguaje. net para la generación del plugins como base a la manipulación a los archivos se hará con la base de datos, que en cualquier momento se debe hacer consultas para asignar o permitir operaciones con los archivos.

Se debe tener en cuenta la enumeración de los archivos que se tienen en el servidor para lo cual se debe hacer una conexión a la base de datos y allí consultar los archivos que posee el usuario, como pueden llegar a ser muchos solo se mostraran por carpetas de año a año o también la opción de los últimos 10 meses.

Con esta opción se podrá agregar, consultar, modificar o eliminar un documento.
Se podrá usar una consulta directa a la base de datos.

Existirá un módulo de permisos para generar los permisos al archivo abierto, permisos que será creados, modificados, eliminados y consultados aplicados a la base de datos como escritura consulta, impresión, enviado a correo electrónico, etc.

Al proponer este planteamiento se pretende minimizar el riesgo de ataques directos en contra de la aplicación de Word o Excel, con la mejor administración de los archivos por medio de un servidor y a si mismo proponer un manejo de la seguridad centralizado en un server, que actuara también como servidor de archivos protegiendo de ataques que se pueden minimizar y resguardar la información de una mejor forma.

Al otorgar permisos de operación a los archivos como de lectura, escritura y compartir se determina un propietario del archivo, al evitar un copiado, print screen e impresión se previene que la información salga de la organización sin control, al

igual que al aumentar en cierto modo la letra y el mantener los documentos guardados en una base de datos organizada y administrada, se evita la fuga de información y un posible riesgo con el ingreso de este tipo de archivos.

9. PAUTAS PARA MINIMIZAR LOS RIESGOS DE LA INFORMACIÓN EN ARCHIVOS DE WORD Y EXCEL

9. 1 Otras estrategias de mitigación para disminuir el robo, fuga hurto y secuestro

Otras estrategias que se pueden plantear para que se minimice el impactó de ataque a los archivos de ofimática en la organización son:

9. 1. 1. PROTECCION FÍSICA

A nivel de protección del hardware se puede tomar ciertas medidas que apoyan la labor de seguridad, entre otras se contempla: mantener el hardware como servidores, equipos de comunicación, equipos de seguridad, en un lugar cerrado con ciertas medidas de seguridad como puertas con llaves de seguridad, control de acceso biométrico y control humano, de tal forma que el acceso no sea directo y fácil, este se complementa con el control de acceso a las instalaciones de la organización que incluye todo el protocolo de acceso a empleados y visitantes.

En cuanto a las medidas para los servidores y los elementos de comunicación y almacenamiento se recomienda que se encuentren en un Datacenter que cuente aire acondicionado, electricidad ininterrumpida, debe existir un control de acceso (puede ser biométrico), sistemas contraincendios y se debe tener un registro de entradas y salidas de las personas que acceden a este espacio.

- En las comunicaciones se aconseja que los puntos de red estén asegurados ya sea deshabilitados y/o referenciados al funcionamiento por la Mac.
- Los equipos de los empleados deben contar con mecanismos de protección logica como es estar unidos a un dominio administrado, el cual exigirá un usuario y una contraseña como parte de acceso al sistema, se recomienda que no solo sea de acceso a los equipos sino también a cada una de las aplicaciones que funcionen en la organización, estas implementadas en un ambiente seguro como certificados y otros mecanismos.
- Como mecanismo de protección físico se recomienda que los discos duros de cada equipo deben estar encriptados, esto cubriendo el posible hurto de los equipos.

9. 1. 2 CIFRADO DE ARCHIVOS.

En los temas de envío y recepción de archivos por correo electrónico, se recomienda que en la operación la información sea tratada bajo parámetros de seguridad, como los certificados, en los cuales se protegen aspectos como la autenticación, confidencialidad e integridad de los datos transmitidos, generalmente se recomienda el montaje de los certificados públicos en cada uno de los buzones

de correo, con este mecanismo se garantiza los aspectos de seguridad antes nombrados ya sea de envío o recepción.

El certificado se puede adquirir con empresas certificadoras como digicert, commodo, good daddy, la implementación de este se puede hacer mediante el módulo de seguridad de Outlook, mediante los siguientes pasos:

En el menú File, click en Options > Trust Center.

En el menú de Microsoft Outlook Trust Center, hacer click en Trust Center Settings y posteriormente Email Security.

Se debe hacer click Import /Export para importar un certificado digital enviado por el proveedor, por ultimo buscar los servicios a usar como encriptar el mensaje, autenticar el origen, etc.

Usualmente los certificados usan RSA 2048/4096, pero se recomienda que se use algoritmos de encriptación ECC, el cual provee seguridad más fuerte y rendimiento con claves cortas.

9. 1. 3 PLANES DE CONTINGENCIA.

Se recomienda que en la organización se tenga un plan de contingencia, que consiste en planeación de reacción de ciertos eventos contemplados ya sean de carácter físico, lógico y humano, se recomienda que la implementación se realice según, standard for business continuity management [ISO 22301:2012] Disaster Recovery Institute International [DRII. org].

9. 1. 4 EVITAR EL USO DE SOFTWARE PIRATA.

Como medida preventiva de uso de software no autorizado se deben implementar controles sobre los equipos informáticos, este puede ser con software como System center configuration manager, herramienta de la casa Microsoft que se integra con las aplicaciones de la marca. Esta aplicación administra las máquinas de la red, aplicaciones, rendimiento, software, actualizaciones de forma centralizada, también permite hacer un inventario de las máquinas y el software comparado con una línea base, que informara al administrado si algún software fue instalado en un periodo dado.

Adicionalmente mediante el uso de un directorio activo se pueden implementar políticas para que los usuarios no puedan hacer instalaciones de ningún software sin permisos de los administradores de la red y los equipos.

9. 1. 5 IMPLEMENTACIÓN DE UN IDS.

Este es un componente de seguridad de tipo hardware o software que monitorea o supervisa una red en espera de actividades anómalas [alerta temprana] desde el exterior hacia un ámbito de red corporativo.

Un IDS está compuesto por los siguientes elementos: fuentes de recolección de datos reglas de contenido de datos, filtros, detectores de eventos anormales en el tráfico, dispositivo generador de informes y alarmas.

Dentro de los IDS a implementar se pueden considerar las siguientes opciones:

Snort: una de las ventajas es que es gratuito, plataforma bajo Linux, por ende, no cuesta, la implementación y el mantenimiento es más complejo para el funcionamiento se debe comprender muy bien las reglas y su funcionamiento, se recomienda la implementación con alta disponibilidad.

The bro: una de las ventajas es que es gratuito también ofrece alto rendimiento, es un analizador completo de protocolos que permite el intercambio de información en tiempo real, se basa en un análisis en eventos de archivos, la aplicación funciona a partir de la decodificación de capa de aplicación, detección de las anomalías de la red, coincidencia de firmas de ataques y análisis de conexión.

9. 1. 6 DISEÑAR UN SGSI Y UNA POLÍTICA DE SEGURIDAD

Un sistema de gestión de seguridad informática pretende aumentar la seguridad en la infraestructura minimizando los riesgos, amenazas, vulnerabilidades, mediante políticas, registros, procedimientos, manuales, documentación organizada y precisa de los activos de la información en la organización.

El objetivo de un sgsi es mantener la confidencialidad, integridad y disponibilidad de los activos, se recomienda usar estándar ISO 27000 con todas las recomendaciones para la implementación.

Un sgsi está diseñado para proteger los activos de una organización para nuestro caso los activos como lo son la organización, el Datacenter, servidor, la red, la información.

Dentro del sistema de gestión de la seguridad la información se puede implementar el PHVA el cual permite la evaluación y mejora continua, lo cual permitirá aprender de los eventos ocurridos y fortalecer la seguridad de la organización.

9. 1. 7. CAPACITACION AL PERSONAL.

Como parte de la estrategia de capacitación al personal se recomienda realizar las siguientes acciones para preservar la seguridad los datos, archivos, hardware y seguridad en general de la organización:

- Capacitar a los usuarios sobre el mejor uso de los correos, cómo prevenir infecciones y las consecuencias, temas de seguridad en claves o password, etc.
- No abrir archivos de correos sospechosos e informar al área de seguridad informática en caso de dudas.
- Generar capacitaciones y configuraciones idóneas en seguridad informática, sobre el manejo y buenas prácticas de las contraseñas.
- Las capacitaciones están contempladas dentro del SGSI, por tal motivo se debe informar al personal de la organización sobre las políticas de seguridad y las consecuencias de no cumplirlas.

9. 1. 8. ANTISPAM.

Se debe implementar una solución de Antispam, la cual se encarga de rechazar todo correo que tenga una reputación inadecuada para circular en el correo electrónico de una organización, esto permite mitigar los ataques mediante este medio de comunicación, para lograr este objetivo se debe mantener el aplicativo de Antispam actualizado y correctamente configurado, los Antispam recomendados son:

- Trend micro, este sistema es de amplia configuración con administración dedicada, que provee múltiples configuraciones y hasta retenciones de correo, para el caso de mantenimientos si así se desea, también se acompaña de el par como lo es el antivirus para correo y el antivirus para equipos y servidores que lo ayudan a complementar en las tareas de protección.
- Office 365 es otro sistema es el que provee las plataformas de correo como Office 365, este es un sistema automático administrado y suministrado por Microsoft.

9. 1. 9. ACTUALIZACIÓN SISTEMA OPERATIVO Y ANTIVIRUS.

Consiste en mantener los sistemas operativos actualizados, para este caso se hace referencia a los sistemas operativos Windows ya sea en versiones Windows 7, 8, 8. 1, 10, las actualizaciones se encuentran publicadas con el proveedor de la casa de fabricación “Microsoft”, así como todos los productos instalados, también se debe tener un programa de protección de virus, este puede ser comercial, como:

- Symantec End point Proteccion: proveedor comercial con muchos años de experiencia en el mercado, posee tecnologías de revisión exhaustiva en busca de código malicioso y comportamientos.
- Comódo: es un software gratuito que permite brindar máxima protección a los virus conocidos, malware y spyware, posee una tecnología AutoSandBox, etc.

9. 1. 10. NAVEGACIÓN EN INTERNET.

Se debe capacitar a los usuarios en mantener precaución con las páginas web consultadas, ya que existen muchas páginas que son peligras y pueden infectar los equipos y en algunas ocasiones se informan de daños o infecciones que logran engañar a los usuarios.

9. 1. 11. FIREWALL.

Es usado como un mecanismo de seguridad perimetral que se encarga de evitar ataques externos e internos en la infraestructura, el firewall se debe mantener actualizado en sus bases de datos de riesgos, en el caso del firewall se pueden usar cualquiera de tipo comercial, se propone los siguientes:

- Cisco asa: ofrece protección multicapa, tiene alto rendimiento y bajo consumo de hardware.
- Check point catalogado como el mejor por el cuadrante de gartner, aunque aún tiene serias falencias, es flexible, completo cuando se adquiere con la Suit, es cotoso entre la franja de los firewalls, pero se obtiene un gran producto.
- Exinda ofrece alto rendimiento, aprovecha el ancho de banda del ISP, es más rápido que el promedio de firewall comerciales, mejora el desempeño de las aplicaciones.

9. 1. 12. COPIAS DE SEGURIDAD.

Las copias de seguridad es otra de las medidas que se pueden tomar, si se hacen Backups se puede garantizar que la información se puede recuperar y el tiempo de perdida es corto, la toma de las copias de seguridad debe hacerse con intervalos de menor tiempo posible y lo más importante las copias deben ser probadas, documentando la metodología de recuperación, así mismo el tiempo de recuperación en caso de ataque puede ser corto y tener un alto grado de confiabilidad.

Para este caso se puede generar la copia de seguridad con la herramienta que tiene por defecto Microsoft SQL la cual mediante configuración se programa para que se genere el backup y luego este sea tomado por cualquier herramienta de grabado en cinta, ejemplo Backup exec. [herramienta que consta de una agente con el cual se

encarga de tomar una backup y grabarlo en cinta, también se puede hacer con el agente correspondiente de SQL], se recomienda que la cinta este encriptada y adicionalmente se almacene bajo las recomendaciones de D. R. P. [Disaster Recovery Plan] en la que dice que la cinta debe ser guardad a 400 km de la organización, que lo debe hacer una organización experta en el almacenamiento de este tipo de medios y bajo la seguridad requerida por ejemplo “4GS”, todo esto con la intención de poder a futuro contar con un medio confiable y la información disponible.

CONCLUSIONES.

Existe una gran afectación de entes externos hacia los archivos informáticos generados por la ofimática, en la representación Word y Excel, los cuales tiene información que es de vital importancia para las organizaciones.

La afectación en una gran parte obedece a temas de índole económico o financiero.

En otras ocasiones las afectaciones son de tipo judicial, afectando procesos y perjudicando a la justicia.

La identificación de los ataques es esencial para el estudio y objetivos de los ataques, ayudan a tipificar un comportamiento el cual se puede prever o advertir a los usuarios en general.

El diseño de este documento genera una iniciativa como la minimización de estas vulnerabilidades en los archivos y permite fortalecer la operación diaria de una organización.

Como parte de la minimización de las vulnerabilidades se debe contar con otras ayudas que fortalecen aún más la seguridad en general de una organización. Como solución final se debe elaborar un método o hacer un desarrollo el cual minimice las operaciones negativas con los archivos, evitando generación de indisponibilidad de los archivos y la información.

RECOMENDACIONES

En la manipulación de los archivos informáticos tratados en este documento se sugiere que los usuarios mantengan una serie de capacitaciones en temas de seguridad informática, en los que aprenderán a prevenir las infecciones de los archivos informáticos.

Para el caso de la administración de los sistemas informáticos se aconseja seguir muy detalladamente los estándares de seguridad informática, los cuales ayudan a minimizar los riesgos de infecciones a nivel digital.

Para posteriores investigaciones al respecto se recomienda estar al tanto de otros tipos de ataques e infecciones que puedan vulnerar la astucia de los usuarios o también vulnerabilidades de los sistemas informáticos.

GLOSARIO

Virus informático: Son programas o software que tienen como objetivo modificar el funcionamiento del computador, red, información o datos contenida en él.

Malware: Es un tipo de software que tiene como objeto infiltrarse y averiar una computadora o sistema de información, todo esto sin que el usuario se entere.

Ransomware: Es un tipo de programa informático que secuestra y/o restringe el acceso a los equipos informáticos o a los archivos del sistemas o datos infectado, el fin es pedir un rescate a cambio de quitar estas restricciones.

Archivo: Es un conjunto de bits que son almacenados en un dispositivo, un archivo es identificado por un nombre y una extensión la cual obedece a una identificación y ejecución del mismo.

Word: Es un programa de informática orientado al procesamiento de textos, fue diseñado y creado por la casa de software Microsoft y está integrado en el paquete ofimático llamado Microsoft Office

Excel: Es un programa de informática orientado al procesamiento de hojas de cálculo, fue diseñado y creado por la casa de software Microsoft y está integrado en el paquete ofimático llamado Microsoft Office

Seguridad: Es el medio que permite concentrar los esfuerzos en reducir los riesgos y permitir que los procesos tengan un estado aceptable de funcionamiento, este también es inherente a cualquier actividad, el riesgo nunca es eliminado totalmente, solo es minimizado.

Vulnerabilidad: Son errores en la arquitectura del software que permiten realizar desde un ámbito externo acciones sin permiso que perjudicaran el software del equipo o la información.

Robo de información: Es el acto de extraer ilegalmente información [conocimiento (intangible)] de un medio magnético, con el fin de perjudicar al propietario o generador de la información.

Secuestro de información: Consiste en encriptar la información encontrada en un equipo ingresando password de con larga contraseña [imposible de des-encriptar rápidamente] y para la cual el secuestrador solicita un pago a cambio de la contraseña de des encriptación.

Plugins: Es la inserción de un programa Informatico a otro añadiendo una funcionalidad o nueva característica.

BIBLIOGRAFÍA

BALESTRINI A, Mirian. (2001). “Como se elabora el proyecto de Investigación”. BL Consultores Asociados. Servicio Editorial. Caracas, Venezuela. P 34-76

ECURED. CU. Observación Científica. [en línea] 30 de mayo de 2017 [revisado Abril de 2017], Disponible en internet: https://www. ecured. cu/Observaci%C3%B3n_cient%C3%ADfica.

ELTIEMPO. COM. Ataque-cibernetico-afecta-redes-de-74-paises. [en línea] 2016 [revisado Abril de 2017], Disponible en internet: http://www. eltiempo. com/tecnosfera/novedades-tecnologia/ataque-cibernetico-afecta-redes-de-74-paises-87390.

FERNÁNDEZ, Sandra. ¿Qué es un virus informático? Definición y tipos. [en línea] 14 de Octubre de 2015 [revisado Abril de 2017], Disponible en internet: http://www. valortop. com/blog/virus-informatico-definicion-tipos.

GCFAPRENDELIBRE. ORG. ¿Qué es un virus informático? [en línea], no posee fecha [revisado Abril de 2017], Disponible en internet: https://www. gcfaprendelibre. org/tecnologia/curso/virus_informaticos_y_antivirus/los_virus_informaticos/1. do.

HERNANDEZ , Roberto. (1998). “metodología de la Investigación”. McGraw-Hill Editores. México.

PAREDES, ANTONIO. 40% de empresas sufrió ataques de malware. [en línea] 2016 [revisado Abril de 2017], Disponible en internet: http://prensa. tecnologia21. com/215/40-empresas-sufrio-ataques-malware.

PROCESOS DE PMBOOK, [en línea] 19 de Febrero de 2016 [revisado Abril de 2017], Disponible en internet: https://medium. com/administrador-de-proyectos/los-47-procesos-del-pmbok-5-sin-tener-que-memorizar-befddee74024

TAMAYO y TAMAYO, Mario. (1996). “El proceso de la investigación científica”. Limusa Noriega Editores. México. P 46-68

NORMA TÉCNICA COLOMBIANA - NTC 1486, [en línea] Agosto de 2008 [revisado Abril de 2017], Disponible en internet: http://www. unipamplona. edu. co/unipamplona/portalIG/home_15/recursos/01_general/09062014/n_icontec. pdf

ANEXOS

Anexo A. Resumen RAE

RESUMEN ANALÍTICO ESPECIALIZADO - RAE	
1. Título.	PLANTEAMIENTO DE SEGURIDAD PARA LA MINIMIZACIÓN DE FUGA, ROBO Y DAÑO DE LA INFORMACIÓN EN ARCHIVOS OFIMÁTICOS
2. Autor:	Omar Dimian
3. Edición	N/A
4. Fecha	Fecha: Diciembre de 2018.
5. Palabras Claves,	Virus, Ataque, Ofimática, Planteamiento, Ramsomware.
6. Descripción.	Esta monografía genera un planteamiento como solución a los diversos ataques informáticos a los archivos ofimáticos generados día a día en las empresas, como solución se muestra un diseño que pretende disminuir estos ataques y minimizarlo.
7. Fuentes.	Esta monografía se usan 19 referencias bibliográficas extraídas en su mayoría de enlaces de internet. DIARIOTI. COM. El Ransomware en cifras y lo que las organizaciones deben saber. [en línea] 2016 [revisado Abril 2017], Disponible en internet: https://diarioti. com/el-ransomware-en-cifras-y-lo-que-las-organizaciones-deben-saber/98938 MICROSOFT. Ransomware. [en línea] no posee fecha [Revisado Marzo de 2018], Disponible en internet: https://www. microsoft. com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Ransom:Win32/Sofilblock.A PANDASECURITY. COM, ¿Qué es un Ransomware? [en Linea] 15 de Noviembre de 2013 [Revisado Marzo de 2017], Disponible en internet: http://www. pandasecurity. com/spain/mediacenter/malware/que-es-un-ransomware/ p 39-40

	ECURED. CU. Observación Científica. [en línea] 30 de Mayo de 2017 [revisado Abril de 2017], Disponible en internet: https://www. ecured. cu/Observaci%C3%B3n_cient%C3%ADfica.
8. Contenidos.	En este documento se expone el bien conocido problema mundial de los ataques a los archivos de ofimática, es decir a los archivos de su gran mayoría generados por aplicaciones de Word, Excel, PowerPoint, quienes a lo largo de su existencia y también por su masificación son objeto de ataque con el objetivo de vulnerar la información que allí reposa, esta información puede ser de carácter económico investigativo, informativo, financiero, gerencial, etc. Los ataques generados a estos archivos son de tipo hurto, modificación/alteración de su contenido, secuestro, exposición de la información sin autorización, etc. El documento expone una posible propuesta de solución a los ataques a los documentos ofimáticos basados en Office, aplicación que se ha generado desde la casa matriz Microsoft y que genera los archivos .docx, xlsx, . pptx y de estos sacamos ventajas como el poder descomponer un archivo ofimático y darle un orden en una base de datos propuesta, también se pueden inspeccionar cada uno de estos elementos de posible software o programación mal intencionada. En el documento se exponen propuestas de un diseño en el que se incluye la intervención de un servidor con una base de datos que administrara y almacenara de forma se segura todos los documentos generados por una organización. El core adicional del diseño consiste en la generación de una plugins que se instalara en el cliente, este plugins interviene con ajustes puntuales hacia cada aplicativo como lo es Word, Excel, PowerPoint y Outlook, que consisten el evitar mediante la programación las copias, bloqueos de las teclas printscreen y también por software se hará el aumento del tamaño de las letras [evita la toma de fotos con mucha información], para ciertos permisos la impresión, modificación y envío del documento a correos no autorizados o también la notificación de aviso de envío para documentos calificados con alta importancia, adicionando alta seguridad con un compartido seguro de los archivos entre las personas deseadas.

	El ambiente ofimático será controlado por permisos y desde las aplicaciones mismas se otorgarán credenciales de directorio activo o similar unificadas para el acceso automático, tal como se pude ver hoy en día con un ambiente empresarial.
9. Metodología.	La metodología utilizada para la monografía es la observación científica y técnica usada en el análisis y procesamiento de los datos usado es el análisis cualitativo. La población de muestra se hace a través de las estadísticas tomadas de la casa Microsoft, quien con su plataforma de Windows defender preinstalada en todos sus sistemas operativos Windows puede tomar estos datos y procesarlos, dado para cualquier tipo de cliente empresarial, educativo y home. La población de Ramsomware que se pueden tomar para la muestra son todos los malware que pueden afectar los archivos office, pero los que más representación debido a su gran número de ataques y efectividad de los mismo, se tienen para la muestra son los siguientes: Win32/Crilock. A, Win32/Cribit. A, Win32/Adslock. A, Win32/Sofilblock. A, para el periodo de septiembre de 2017.
10. Conclusiones.	Mediante el análisis a la problemática de los ataques informáticos sufridos en contra de la información en los archivos ofimáticos en ambientes Microsoft, podemos asegurar una solución que ayuda a minimizar los intentos de ataque a los archivos ofimáticos y los altos impactos que esto significa para una entidad.
11. Autor del RAE.	Omar Dimian