UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE CIENCIAS Y SISTEMAS

MAESTRÍA EN GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

CICLO ACADÉMICO 2013- 2015

Informe Final de Tesis para optar al Título de

Máster en Gestión de la Seguridad de la Información

"ANÁLISIS DE AMENAZAS RELACIONADAS A LOS METADATOS Y CORREO ELECTRÓNICO, E IMPLEMENTACIÓN DE UN APLICATIVO COMO HERRAMIENTA PARA DISMINUIR EL RIESGO DE UN ATAQUE EN EL QUE SE EMPLEEN ESTOS ELEMENTOS."

Autores:

Ing. Norman Ariel Altamirano López

Ing. Félix Rafael Sequeira Jiménez

Tutor: Msc. Evelyn Aragón Espinoza

Managua, Nicaragua. Julio, 2016

Dedicatoria

Esta tesis se la dedico primeramente a Dios, quien me mantuvo firme aun en la enfermedad y diferentes luchas de la vida. Me dio fortaleza para continuar y no darme por vencido.

A mi madre quien a lo largo de su vida se ha esforzado como ninguna otra, para que todos mis hermanos y yo tengamos un gran ejemplo de entrega, amor y unión.

A mí amada esposa por su gran apoyo incondicional, comprensión y sus dulces palabras de aliento que me permitieron seguir hacia adelante.

A mi hermano menor, el cual con sus palabras me abrieron la mente para tomar la decisión de continuar desarrollándome académicamente.

A mi familia, por estar siempre atentos y dispuestos a ayudar ante cualquier dificultad o necesidad de cualquiera de los miembros.

Ing. Norman Ariel Altamirano L.

Dedicatoria

Primeramente le agradezco a Dios por haberme permitido la culminación de estudios del programa de la maestría de Gestión de la Seguridad de la Información (MGSI), a él le dedico la culminación de este estudio.

Les agradezco a mi madre y padre que siempre ha sido el pilar fundamental de mi educación y en mi vida, gracias a su amor y apoyo.

Les agradezco a mis hermanas por su apoyo, amor y el ánimo que me brindan para que siga superándome.

Ing. Felix Rafael Sequeira J.

Presentación

Con el surgimiento del internet, el avance del software y la tecnología, se les proporciono a las personas la capacidad de compartir grandes cantidades digitales de información a través de la nube, correo electrónico, etc. Gran parte de esta información contiene incrustados datos, conocidos como metadatos, los que indirectamente revelan más información de la que deberían, siendo un potencial riesgo. Además de ello, con el uso del correo electrónico se ha creado un medio de propagación de amenazas y flujo de información privada.

Por tanto, el presente documento suministrara de una aplicación que permitirá eliminar los metadatos de ciertos archivos, brindara protección ante correos electrónicos provenientes de dominios maliciosos y evitara que se envíen correos a direcciones sin autorización o que sean potenciales amenazas. Además de proporcionar un análisis del impacto que puede ocasionar el uso de metadatos y correo electrónico en la seguridad de las personas.

Índice

1. Introducción

En el mundo tecnológico en que vivimos, gran parte de las personas disponen de equipos computacionales y servicios de comunicación, lo que les ha permitido la creación y distribución de archivos y el envío y recepción de mensajes a diferentes partes del planeta. Aunque es una ventaja disponer de estos medios, también podrían ser utilizados para generar potenciales amenazas sino se utilizan adecuadamente.

Con las diferentes técnicas de engaño que utilizan los atacantes y el desconocimiento de los usuarios ante la tecnología, resulta fácil aprovecharse de esta debilidad para cometer delitos o recopilar información privada de una organización o persona.

Este hecho es de suma relevancia, ya que las personas por desconocimiento estarían facilitando información interna y privada, ya sea de su localización, estructura interna de la organización, usuarios que editaron los archivos, etc. lo que podría ser utilizado para cometer algún tipo de delito. También, debido a la astucia con que los atacantes elaboran sus ataques, estos han desarrollado métodos ya sea para propagar virus, correos masivos publicitarios o como medio para realizar engaños y cometer fraudes o robos. Inclusive, empleados que desean enviar correos a direcciones personales o no autorizadas, tienen la facilidad de hacerlo, debido a que no siempre se establecen mecanismos de fuga de información en las organizaciones.

Contar con herramientas de protección para evitar estos acontecimientos e implementar mecanismos, prácticas y políticas de seguridad es de gran importancia, ya que en un ambiente tecnológico donde la seguridad no sea tomada seriamente, se estaría dando acceso sin restricciones a cualquier ataque. El éxito que se logre no será solamente de la astucia del atacante, sino

de la falta de mecanismos y conocimientos en materia de seguridad que el usuario haya implementado.

Aunque las inversiones en elementos de seguridad en algunos casos son altas, pero muy necesarias, es importante realizar un análisis del beneficio de contar con ella, ya que las pérdidas económicas tienden a ser aún mayores que los gastos relacionados a la adquisición de hardware, software o capacitación para evitar el daño tanto a los datos como equipos, ya sea de las organizaciones o personas individuales.

Además, la seguridad es un área que debe trabajar conjuntamente con el usuario, sin embargo este último no siempre tiene conocimientos suficientes de protección, ya que quien hace uso de la tecnología, no siempre es un profesional en el ambiente informático. Por ello, este documento abordara tres aspectos fundamentales, como son: la protección de la información oculta en archivos que es enviada principalmente por correo electrónico, el filtro de correos electrónicos recibidos y enviados y por último el escaneo de dominios perteneciente a los correos electrónicos, esto con el propósito de detectar si son de fuentes maliciosas.

Esta investigación estará enfocada en analizar qué tipo de información contiene los metadatos, como pueden ser utilizados para llevar a cabo un ataque, que tan riesgoso puede ser para las personas u organizaciones no eliminar los metadatos, que tan difícil puede ser extraer este tipo de información de los archivos, la manera en que se usa el correo electrónico para realizar un ataque, las técnicas existentes que hacen uso del correo electrónico, los diferentes métodos para reducir el riesgo de ser víctimas de ataques, el impacto económico y social de los ataques y la razón por la cual se debe contrarrestar.

Por tal motivo, para evitar enviar información adicional en los archivos digitales, disminuir ser víctimas de ataques o engaños por medio de correos electrónicos,

brindar un aseguramiento extra en la comunicaciones y aumentar el conocimiento de las personas. Se pretende desarrollar una herramienta por medio de la cual se eliminen los metadatos de los archivos antes de que sean enviados por correo electrónico, se bloquee la entrada y salida de correos provenientes de direcciones consideradas sospechosas y se permita la administración de cuentas de correos confiables. Además de proporcionar un análisis de las técnicas de ataque empleadas haciendo uso de metadatos y correo electrónico, el impacto que puede ocasionar y qué medidas tomar para disminuir el riesgo.

2. Definición de la problemática

Existen dos problemas a tratar en esta investigación, primeramente nos referiremos a los metadatos, lo cuales en términos digitales consisten en datos que sirven para describir grupos de datos a los que podríamos llamar objetos informáticos (Baca, 1999), también se podría definir como datos sobre datos (Caplan, 1995). El problema radica principalmente en que al momento que se crea un archivo digital, a esta se indexan los metadatos, agregando información adicional, la cual podría contener si se tratase de una foto, marca, modelo y sistema operativo del dispositivo con que se tomó la foto, también fecha, hora y ubicación geográfica del momento en que se tomó la fotografía (Pérez, 2014).

Con estos datos y un poco de análisis se podría saber que vulnerabilidades afectan el equipo o utilizar algún sistema de información geográfica para ubicar las coordenadas geográficas y localizar el lugar de origen de la foto. Pero aún hay otro inconveniente, debido a que esta información esta oculta, no todos las personas tienen conocimiento de su existencia y por desconocimiento publican o comparten información sin saber que están facilitando datos sensibles que podrían traerles graves consecuencias.

El segundo problema en que nos concentraremos es en el que se vincula al correo electrónico, la mayoría de personas que hacen uso de internet tienen creadas por lo menos una cuenta de correo, ya sea comercial o corporativa. Aquí radica otro inconveniente, debido a que la mayoría de los sitios web para dar acceso a ciertos recursos solicitan a los usuarios registrarse, pidiendo como requisito datos personales, entre los que se encuentra su cuentas de correo, además de ello existen empresas o personas que tienen como función la recopilación de estas direcciones para diferentes propósitos.

El objetivo principal de hacer esto es tener una base de datos de correos, a los cuales se les puede brindar servicios, productos o ser objetivos de ataques. Ya con esta información en manos de otros, las personas pasan a ser potenciales víctimas, ya sea de envíos masivos de correos basuras, fraudes como phising, etc.

Si ambos problemas se mezclan, el impacto sería doble, ya que si se envía un archivo adjunto sin haber eliminado sus metadatos a una dirección sospechosa o maliciosa, se estaría además de estar siendo víctima del correo, proporcionando información sensible con lo cual el atacante podría elaborar algún método para realizar un ataque más sofisticado, como escalar privilegios en los sistemas de la organización, expandir su ataque a otros usuarios, comprometer cuentas, robar credenciales de usuarios, vigilar, incrustar virus, en fin, gran cantidad cosas que afectarían a las personas u organizaciones.

3. Justificación

Los usuarios que hacen uso de equipos tecnológicos, ya sean para generar archivos en diferentes formatos como para comunicarse a través de correos electrónicos, en su mayoría tienen un conocimiento nulo de lo que se refiere metadatos, la manera en como eliminarlos y el objetivo de estos. Además, debido a las diferentes técnicas de engaños existentes, las personas se vuelven

presa fácil para caer en trampas detalladamente diseñadas con el objetivo de robar información o cometer fraudes empleando correos electrónicos.

En la actualidad existen diversos software que se encargan de eliminar los metadatos de los archivos, sin embargo esto requiere para el usuario aprender a manejar la aplicación, ejecutarla siempre que desea enviar un archivo por correo electrónico, además de los costos relacionados que involucra. También en cuanto al correo electrónico, hay dos aspectos a abordar, el primero se refiere al correo proveniente de direcciones maliciosas y spam, para el cual existe lo que se conoce como el filtro anti-spam el que por lo general viene incorporado en los software de corres electrónicos. Para este tipo de correos los proveedores de antivirus y empresas desarrolladoras de software de seguridad entre sus soluciones integran esta característica y el escaneo de direcciones maliciosas, el otro aspecto es el envío interno de correo a cuentas confiables o autorizadas, para ello existen también software especializados para la administración. En ambos casos es necesarios contar con software de terceros, lo que también requiere conocimiento de la aplicación, administración y costos.

Además, contar con una herramienta que incorpore todos estos elementos en una sola aplicación aún no se ha pensado, sino que existen solamente sistemas individuales que ejecutan estás funciones. Siendo así la intervención humana es mayor, lo que indica que el margen de éxito de un ataque aumente y la información oculta que es enviada contiene datos sensibles sin tratarlos adecuadamente.

Así que con esta investigación se aspira llegar a proporcionar de una herramienta que integre estas tres características, evitar recibir correos maliciosos, evitar enviar archivos o correos a cuentas sin autorización y eliminar los metadatos de los archivos antes que sean enviados por correo electrónico. También realizar un análisis de cómo afecta el uso de metadatos y correo electrónicos a los usuarios, cuando son empleados para un ataque.

Contar con esta herramienta será de gran beneficio para los usuarios u organizaciones, debido a que facilitara una capa de aseguramiento en sus actividades diarias, sin realizar ninguna tarea adicional, ya que de manera transparente se ejecutarían procesos de protección al eliminar información confidencial o extra de los archivos y determinar si las direcciones a las que se envía o reciben correo son confiables. Esto ayudara al usuario a enviar archivos adjuntos solamente con información de la cual está consciente y clara de su contenido, teniendo así un control total sobre sus datos. Además, dará la confianza de que la cuenta de correo electrónica a la que se envía o recibe correos han sido analizadas y pueden ser utilizadas sin el temor de ser víctimas de algún tipo de ataque. También, con la administración de las cuentas de correos electrónicos se evitaría que se envíen correos a direcciones ya sean personales o ajenas a los procesos de las compañías, evitando así la fuga de información a través de este medio.

Al usar esta aplicación no solo se estaría eliminando metadatos o filtrando correos, sino que se estaría dando a las personas de un medio a través del cual se pueden defender contra potenciales amenazas o ataques, se reduciría el riesgo a vulnerabilidades asociadas a la fuga de información sensible oculta en los documentos, se protegería la imagen y reputación de las personas u organización al evitar revelar información sensible, se podría evitar el impacto de pérdidas económicas derivado del uso mal intencionado de metadatos o por ser víctimas de ataques por medio de correo electrónico, inclusive al contar con el análisis del impacto y amenazas que puede ocasionar el uso de metadatos y correos electrónicos, las personas tendrán mayor conocimiento, pudiendo así aplicar sus propios métodos para asegurar su identidad e información. Pensando en el usuario como el eslabón más débil en la cadena de seguridad, se brindaría con esta investigación los puntos principales para detectar una amenaza, los aspectos que se deben tomar en cuenta para saber cuándo un correo es auténtico, conocer como los atacantes se aprovechan de la información y la

manera de actuar ante algún ataque. Inclusive medidas de seguridad a implementar para asegurar sus equipos y datos.

La importancia de contar con una herramienta de protección y que el usuario tenga conocimientos de seguridad, son aspectos fundamentales para disminuir que un ataque informático tenga éxito. Siendo esto el objetivo de la seguridad, evitar ataques y proteger la información y su propietario.

4. Objetivos

4.1. General

Implementar una herramienta que permita eliminar los metadatos de ciertos archivos (.docx y .jpg) antes de que sean enviados por correo electrónico, la administración de cuentas confiables y bloqueo de correos electrónicos provenientes de direcciones maliciosas. Además de proporcionar un análisis del impacto y amenazas que pueden ocasionar en la seguridad de las personas el uso de metadatos y correos electrónicos.

4.2. Específicos.

- Analizar la estructura de los metadatos.
- Investigar los mecanismos de extracción de metadatos existentes.
- Examinar que tan útiles son los metadatos para elaborar un ataque.
- Investigar de qué manera puede ser utilizado el correo electrónico para elaborar un ataque.
- Analizar las técnicas existentes de ataques que emplean el correo electrónico.
- Analizar el daño que puede ocasionar a las personas un ataque en el que se emplean los metadatos o correo electrónico.

- Investigar de qué manera se podría disminuir ser víctimas de ataques donde se haga uso de metadatos o correo electrónico.
- Desarrollar una aplicación que cumpla las funciones de eliminar los metadatos de los archivos digitales, bloque el correo electrónico proveniente de url maliciosas y administre las cuentas de correos.

5. Marco Teórico

En la actualidad prácticamente toda aquella persona que haga uso de un equipo de cómputo genera diversos tipos de archivos, los cuales comparten ya sea a través de correo electrónico, redes sociales, blog, entre otros. Pero las personas solamente tienen control de la información visible, ya que hay datos que el usuario desconoce que están ahí, conocidos como metadatos.

Los metadatos consisten en información adicional que no está directamente visible en los ficheros y que tienen gran importancia debido a que al hacer uso de ellos se puede etiquetar, catalogar, describir y clasificar los archivos, pero podrían conllevar a cierto riesgo de seguridad. (Lamarca, 2013).

Tal como el caso del documento que presento Tony Blair que fue primer ministro del Reino Unido y cuyo archivo contenía información sobre Irak, Saddam Hussein y armas de destrucción masiva, el cual afirmó que no lo habían editado. Sin embargo, la información de los metadatos demostró como personas de su equipo lo había copiado y editado. Poniendo en duda, la autenticidad de la información. (Molist, Meyssan, 2003).

Tomando otro ejemplo, encontramos que el malware conocido como flame se aprovecha de los metadatos, donde uno de sus módulos msglu32 está centrado totalmente en ellos, buscando incluso los datos GPS de las fotografías para ubicar la posición del equipo infectado.(Symantec Security Response, 2012)

Algo muy importante que contienen estos metadatos además de los ejemplos presentados, es que en ellos se almacenas las rutas del archivo, usuarios que lo editaron, sistema operativo en el que se trabajó, correos electrónicos, etc. Estos datos utilizando una herramienta como Foca, se pueden extraer en cuestión de segundos y de manera organizada. (Pacheco, F., Jara, H., 2009). Realizando un análisis de la información se podrían diagramar topologías de red, llevar a cabo ataques dirigidos a personas específicas, explotar vulnerabilidades del software utilizado, en fin un sin número de cosas que son posibles ejecutar.

Es impresionante lo que se puede realizar solo con un poco de información y el impacto que puede ocasionar a una persona, organización o país. Si un archivo que contiene metadatos cae en manos de personas maliciosas con cierto grado de conocimiento respecto al tema, este podría ocasionar un gran daño. Ya que este tipo de datos sería un insumo para realizar una etapa de reconocimiento en la que el atacante recopila toda la información necesaria para encontrar vulnerabilidades, conocer su objetivo, formular ataques, entre otras.

Las empresas desarrolladoras se han dado cuenta de lo riesgoso que pueden ser los metadatos, por lo que han creado sistemas para la eliminación de estos, tales como metashield, un software especializado en proteger los entornos documentales mediante el análisis y tratamiento de los metadatos. (Eleven Path). También Microsoft office incorpora entre sus características la eliminación de metadatos a partir de la versión 2007 (Microsoft Support). Inclusive, herramientas como MetaClean, MetaStripper, Doc Scrubber, entre otras, se encargan de eliminar los metadatos.

El inconveniente que surge con estas herramientas es que se necesita recurrir a un recurso adicional para la limpieza de los archivos, lo que implica que el usuario debe aprender a usar una nueva aplicación y estar siempre alerta de utilizarla antes de enviar algún archivo. Además, en la mayoría de los casos requiere costos adicionales por la compra de software.

Es importante emplear buenas prácticas de seguridad para mantener la confidencialidad e integridad de las personas u organizaciones, se debe tratar en la mayor medida de lo posible evitar proporcionar información adicional, estableciendo mecanismo para mejorar la seguridad.

Otro tema a abordar es sobre las amenazas que se pueden generar a través de correos electrónicos, en 2013 existían aproximadamente 3,899 millones de cuenta de correo electrónico con una proyección al 2017 de 4,920 millones solo en cuentas comerciales, si se incluye las cuentas corporativas los datos oscilan de 929 millones en el 2013 a 1,138 millones al 2017. (The Radicati Group, inc., 2013)

Estas cifras son sumamente inmensas y aumentan exponencialmente a medida que pasan los años. Al existir este considerable mercado, las compañías y delincuentes han implementado una seria de técnicas para llevar a cabo sus objetivos. Entre estos se encuentra, técnicas como el spam, phishing, correos con ficheros adjuntos maliciosos (virus, gusanos, troyanos). (Universidad de Jaen, 2013), entre otros.

Estos correo llegan a la bandeja de entrada de los usuarios provenientes de direcciones que son consideradas por algunos antivirus como sospechosos, el problema radica en que aunque se cuente con una solución, solamente se tendría el servicio que esta empresa brinda y si aún no tienen identificado la url como sospechosa, fácilmente puede llegar a la bandeja del usuario y ser víctimas de engañado. Además de que un solo software no garantiza completamente la seguridad.

Como se ha mencionado existen diversas cantidades de métodos para realizar algún tipo de ataque o fraude mediante correo electrónico, para evitar esto las empresas, principalmente de antivirus se han enfocado en la implementación de herramientas anti spam, anti phishing, para proteger a los usuarios. Pero para

obtener altos niveles de seguridad, se necesita adquirir diferentes módulos de los antivirus y realizar la respectiva compra de la licencia. Empresas como panda, sophos, kaspersky y eset han implementados estas soluciones que ayudan en gran manera a la seguridad.

También en el ámbito de las comunicaciones por medio del correo electrónico, tenemos el flujo de información o archivos que son enviados internamente hacia direcciones ajenas a los asuntos de la compañía, lo que implica un riesgo, ya que se estaría proporcionando información confidencial a otros.

Algunas empresas implementan algo conocido como lista blanca o lista confiable de correos electrónicos, donde se crean las cuentas considerados confiables, a las cuales los usuarios si tienen permitido estar en comunicación. Básicamente podría definirse como un filtro de correos electrónicos confiables y no confiables. Ambos aspectos relacionados con el tema del correo electrónico son importantes tomarlos en cuenta, por una parte disminuir que un ataque tenga éxito al reconocer direcciones maliciosas, evitando que el correo proveniente de ellas logre llegar a la bandeja de entrada de los usuarios y por otra parte que la información interna sea suministrada a destinatarios autorizados, dando de esta manera confianza en que los archivos o las comunicaciones establecidas sean enteramente para tratar temas de negocios o personales, desvinculando así el riesgo de utilizar este medio para robar o extraer información, comprometer sus cuentas o propagar virus.

Sin embargo, algo importante que recalcar es que aunque soluciones o políticas de seguridad sean implementadas en las organizaciones, hay que tener muy en cuenta que es complicado evitar un ataque si el personal no cuenta con la educación ni la disposición. (Delgado, 2013). Prácticamente debido a las malas prácticas de las personas es que estos tienden a ser las principales víctimas. Dando como ejemplo que una persona para descargar algún contenido de la web debe proporcionar sus datos personales, entre los que se incluye el correo

electrónico, desde el momento en que los facilita, se estaría colocando en una posición vulnerable. Ya que lo que hace es suministrar su información que luego puede ser utilizada para generar un ataque.

El usuario juega un papel muy importante en su seguridad, debido a que aunque se cuenten con las mejores herramientas para asegurar las comunicaciones e información, el atacante es consciente de que por falta de formación en materia de seguridad, el usuario no suele estar muy sensibilizado con las posibles amenazas o el riesgo que supone. (Arroyo, 2014).

Si las organizaciones o personas se empeñan en asegurar sus equipos y comunicaciones, proporcionando niveles óptimos contra ataques. El atacante podría empelar técnicas de ingeniería social, mediante la cual podría obtener información sensible de los sistemas de información de la empresa, suplantar la identidad, obtener credenciales de acceso, entre otros.

Por tanto, las personas además de disponer de una herramienta que les ayude a evitar un ataque, deben contar con los elementos necesarios para identificarlos y así actuar adecuadamente para disminuir el riesgo de ser víctima de ello. A través de la experiencia y de la implementación de métodos de seguridad, se han pensado diferentes mecanismos para asegurar la información de las personas y su confidencialidad, sin embargo no se han integrado en una sola solución. Al integrar las tres características mencionadas anteriormente, como son la eliminación de información adicional en los archivos, bloquear la mayor cantidad de direcciones de correo electrónico maliciosas y realizar la administración de cuentas confiables, se proporcionaría de un valioso elemento a las personas u organizaciones, para aumentar así sus niveles de seguridad, evitando ser objetivos de un ataque, robo, flujo de información confidencial, etc.
Pero no solamente se debe abordar esta problemática desde el software. Sino también desde el usuario, quien a como se ha mencionado es el más débil en lo que a seguridad se refiere, debido al poco conocimiento que posee. Por ello, se

facilitara un análisis de los diferentes elementos que generarían una amenaza y que medidas son las más recomendables a tomar para evitarlas, relacionado a metadatos y correo electrónico.

6. Hipótesis

Debido al poco conocimiento de los usuarios en cuanto a la información adicional de los archivos digitales y a las diversas técnicas de engaños que se utilizan por medio del correo electrónico, las personas fácilmente tienden a ser víctimas de ataques. Por tanto para disminuir el riesgo de una amenaza y aumentar la confidencialidad de los datos, se deberá contar con una herramienta que proporcione estas características de seguridad, además de un análisis de las amenazas relacionadas.

1. Metadatos

Con el surgimiento del internet se dio lugar a una inmensa diversidad de fuentes y documentos a los cuales las personas de casi todas partes del mundo pueden acceder. Pero debido a las enormes dimensiones que posee esta red de redes, resulta complicado y sumamente difícil extraer conocimiento alguno. Por tanto para agilizar y facilitar la búsqueda en tan extraordinario universo de archivos, fue necesario establecer mecanismos para catalogar, etiquetar, describir y clasificar los recursos. Siendo estos mecanismos llamados metadatos.

A lo largo de este capítulo se abordaran temas relacionados a su historia, definiciones, objetivos por el cual fueron creados, estándares existentes y estructura.

1.1. Historia

El termino metadato está mayormente relacionado a la era de la información digital, sin embargo la generación de metadatos data de siglos atrás (Vásquez). “Tradicionalmente, los especialistas en información sobre el patrimonio cultural, tales como administradores de museos, bibliotecarios y archiveros, han usado el término metadatos con referencia a datos sobre indexación y catalogación creados por ellos mismos para ordenar y, en general, hacer más accesible esa información”. (Baca, 1999, p. 6).

Durante el tiempo cuando el internet no existía, los bibliotecarios utilizaban sus propios métodos de clasificación de referencias, asignando ya sea fichas de autor, año de publicación, titulo, descripción, entre otros atributos que proporcionaban información preliminar del libro sin necesidad de tenerlo físicamente o leerlo. (Lamarca, 2013). A esto se le podría dar el nombre de metadatos, ya que contienen datos de una fuente de información.

Desde que se da la creación del internet, este empezó a tener gran aceptación por la sociedad y toda la información se comenzó a migrar a formatos digitales. Pero debido a la inmensa cantidad de recursos disponibles, fue necesario establecer mecanismos para catalogar, describir y clasificar estos datos con el fin de buscar y acceder a ellos. (Lamarca, 2013). A partir de esta idea de incorporar metadatos en los archivos digitales es como se agrega información adicional a imágenes, documentos ofimáticos, música, entre otros.

1.2. Que son los metadatos

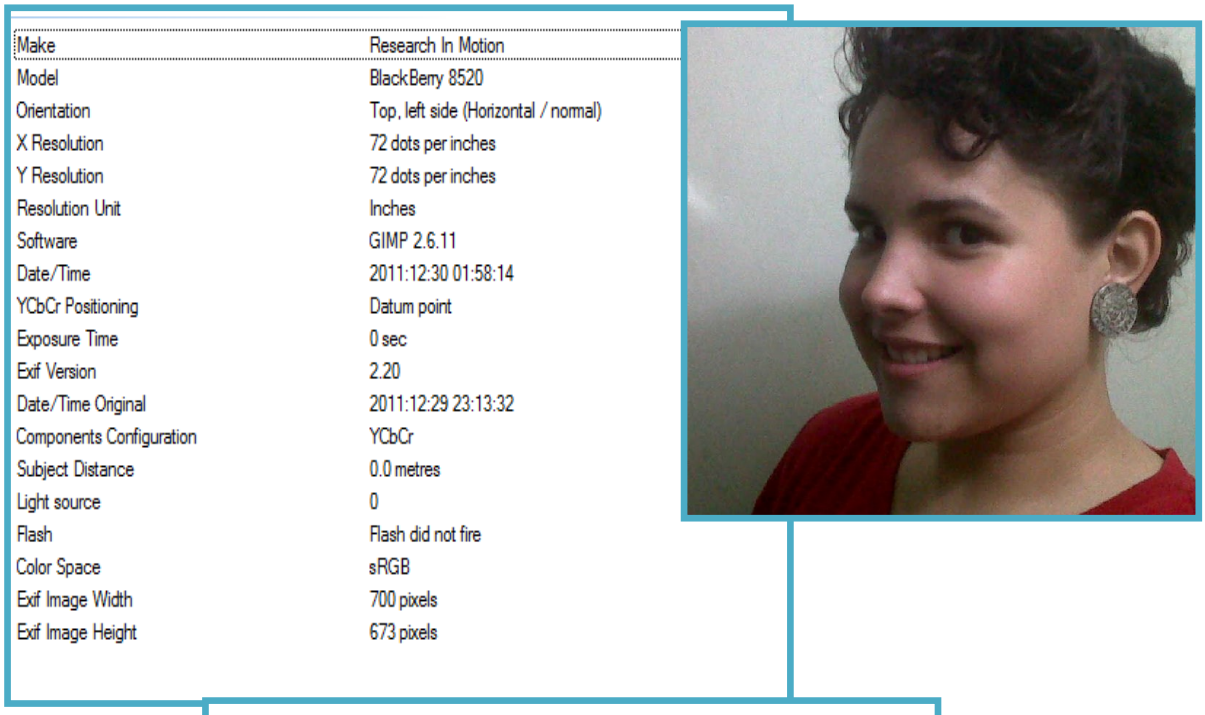
Se reconoce a Jack Myers, en la década de los años 60, como el origen del término “metadatos. (Miller, 1996). Este surge ante la necesidad de recuperar fundamentalmente información electrónica. Esto es, los metadatos funcionan como elemento de enlace en la búsqueda en tanto describen el contenido y localización de la información, una función muy parecida a la de los catálogos con la distinción del formato del documento y del procedimiento automatizado. Los metadatos son también, al igual que la descripción bibliográfica, una forma de organizar la información para su recuperación. (Pérez, 2006).

El término que mayormente se utiliza para definir los metadatos es nada más que “datos sobre datos” (Baca, 1999, p. 1). Es decir, información estructurada que describe a otra información y que nos permite encontrarla, gestionarla, controlarla, entenderla y preservarla. Aunque también pueden referirse al contexto, procesamiento y el uso de los recursos. (Baca, 1999, p. 6).

Otra definición que se puede dar a los metadatos es que son datos con sentido propio, que proporcionan información o documentación sobre otros datos manejados dentro de una aplicación o ambiente. Los metadatos pueden incluir información descriptiva sobre el contexto, calidad y condiciones o características de los datos. (Taylor, 1999).

A como se puede observar, en la diferentes definiciones planteadas hay cierto aspecto en común, el cual es que los metadatos describen un recurso de información, el cual coincide con los propósitos de esta investigación. Para entender mejor este concepto, se plantea un pequeño ejemplo:

Se procedió a descargar una imagen de la web y empleando una herramienta de extracción de metadatos, se explicara de una mejor manera en que consisten los metadatos.



Make	Research In Motion
Model	BlackBerry 8520
Orientation	Top, left side (Horizontal / normal)
X Resolution	72 dots per inches
Y Resolution	72 dots per inches
Resolution Unit	Inches
Software	GIMP 2.6.11
Date/Time	2011:12:30 01:58:14
YCbCr Positioning	Datum point
Exposure Time	0 sec
Exif Version	2.20
Date/Time Original	2011:12:29 23:13:32
Components Configuration	YCbCr
Subject Distance	0.0 metres
Light source	0
Flash	Flash did not fire
Color Space	sRGB
Exif Image Width	700 pixels
Exif Image Height	673 pixels

Figura 1. Metadatos de foto en formato .jpg

A como se observa en la figura 1, en el lado izquierdo se encuentra varios textos que hacen referencia a fecha, software, modelo de celular, etc. con que fue tomada la foto de la parte derecha. A esto es lo que se le conoce como metadatos, en si la foto ya es un información en sí, pero sus atributos o características tales como las citadas anteriormente hacen referencia a otro tipo de datos estructurados que dan una breve descripción de la fotografía.

1.3. Utilidad de los metadatos.

A como se ha tratado en puntos anteriores los metadatos consisten en datos que describen un objeto informático. Sin embargo aún no se ha proporcionado su utilidad.

Básicamente los metadatos como principal función que tienen es ampliar con información adicional el contenido del recurso del que forma parte con el fin de mejorar la calidad y efectividad de las búsquedas realizadas, no solo a la hora de realizar una búsqueda de un archivo perdido en nuestro sistema operativo, sino también para el posicionamiento web, utilizado en gran manera para la conocida web semántica.

Aunque también existen otras funciones como puede ser la de clarificar y gestionar con mayor facilidad los documentos o la de mejorar los estudios estadísticos entre otras muchas.

De forma clara y a modo de ejemplo práctico, los metadatos pueden ser utilizados para clasificar los archivos de música por álbum o autor, para que los buscadores web nos muestre las páginas web que mejor se ajustan a la búsqueda realizada o para que el buscador de Windows nos muestre únicamente las fotos realizadas entre dos fechas concretas. (Stevez, 2013).

Realmente el uso que se les da a los metadatos es muy amplio y van desde la recuperación de información, pasando por la descripción y catalogación de documentos, su uso por parte de robots y agentes de software, comercio electrónico, firmas digitales, derechos de propiedad intelectual; valoración, evaluación y clasificación de contenidos; trabajos bibliométricos e informétricos de todo tipo, etc. (Lamarca, 2013).

Si se analiza más a fondo cada una de las diferentes utilidades de los metadatos y la manera en como simplifica las tareas, resulta sumamente útil disponer de ellos.

1.4. Normas o estándares de metadatos

A pesar de que los metadatos son elementos que intentan organizar la información electrónica fundamentalmente la contenida en Internet, sin su normalización, el intercambio internacional y el control informativo mundial es prácticamente imposible. (Pérez, 2006).

Para resolver este inconveniente se han desarrollado diversas normas, que a continuación se presentan como un breve contenido de su descripción. Para ampliar el conocimiento por parte del lector, se puede hacer uso de los enlaces de cada uno.

1.4.1. Metadatos para la descripción:

- **DC: Dublin Core Metadata Initiative.**

Es un conjunto de quince elementos de información que se pueden usar para describir una amplia gama de recursos en el Internet, lo que permite una forma simple de descubrimiento interdisciplinario de recursos. Estos elementos son:

Contributor, Coverage, Creator, Date, Description, Format, Identifier, Language, Publisher, Relations, Rights, Source, Subject, Title y Type. (Dublincore, 2013).

- **METS: Metadata Encoding and Transmission Standard.**

Ofrece un medio flexible para codificar metadatos descriptivos, administrativos y estructurales para un objeto digital y expresar las complejas relaciones entre estos tipos de metadatos. Brinda un estándar útil para el intercambio de objetos

digitales entre repositorios. Además, METS permite asociar objetos digitales con comportamientos o servicios

Un documento METS consta de siete secciones:

Cabecera METS, Metadatos Descriptivos , Metadatos Administrativos, Sección Archivo, Mapa Estructural, Enlaces Estructurales y Comportamientos. (Eito, 2011).

- **MODS: Metadata Object Description Schema.**

Es un esquema de metadatos descriptivo que se deriva del MARC 21 (protocolo de identificación para el intercambio de información que permite estructurar e identificar los datos de tal forma que puedan ser reconocidos y manipulados por computadora) y que intenta permite crear la descripción de recursos originales o seleccionar los registros existentes en MARC 21. Utiliza el lenguaje y la sintaxis XML. (MODS, 2014).

- **EAD: Encoded Archival Description.**

Se trata de un proyecto internacional que desarrolla pautas para el mercado de textos electrónicos (novelas, obras de teatro, poesía, etc.) y se enfoca al campo de las humanidades. Básicamente es una estructura de datos y no un estándar de contenido de los datos. También es un formato de comunicación de datos basado en la sintaxis SGML / XML. En algunos entornos, la descripción de archivos se creará y mantendrá el uso de tecnologías como bases de datos relacionales u orientados a objetos, y EAD será utilizado principalmente como un mecanismo de transferencia. (EAD, 2012).

- **TEI: Text Encoding Initiative**

Comprende la descripción bibliográfica del documento codificado, la descripción de la codificación, la descripción del perfil o información no bibliográfica como

lenguas, fechas y otros y la descripción de las modificaciones del documento electrónico. (TEI, 2015).

1.4.2. Metadatos para la industria y el comercio electrónico

- **UDEF: Universal Data Element Framework.**

Es una estrategia de identificación de metadatos entre la industria, diseñada para facilitar la convergencia y la interoperabilidad entre el comercio electrónico y otras normas. El objetivo de la UDEF es proporcionar un medio de identificación en tiempo real de la equivalencia semántica, como atributo de los elementos de datos en formatos de documentos e-business y de integración. (Barry & Associates, inc).

1.4.3. Metadatos para multimedia

- **MPEG-21: Multimedia Framework**.

Metadatos para colecciones de vídeo, álbumes musicales, etc. (MPEG)

- **MPEG-7: Multimedia Content Description Interface.**

Metadatos para contenido audiovisual, esto es, para describir contenido multimedia (MPEG).

1.4.4. Metadatos generales:

- **W3C Semantic web activity**

Se trata de formatos comunes para la integración y combinación de datos procedentes de diversas fuentes, donde en la Web original concentran principalmente en el intercambio de documentos. También se trata de la lenguaje para la grabación de cómo los datos se refiere a los objetos del mundo

real. Eso permite que una persona o una máquina, empezar en una base de datos y luego pasar a través de una serie interminable de bases de datos que no están conectados por medio de cables, pero llegan a ser de la misma cosa. (W3C, 2013).

A como se ha planteado anteriormente, existe una gran cantidad de estándares desarrollados para metadatos con diferentes propósitos, abordar cada uno a detalle seria elaborar extensos documentos explicativos, pero para propósitos de esta investigación solo se hizo mención de algún de ellos.

2. Extracción de metadatos

Teniendo la breve explicación de metadatos abordada en el capítulo anterior, lo siguiente que se debe realizar es obtener los conocimientos necesarios de técnicas o herramientas para extraer esta información.

Actualmente en el mercado del software existe una gran variedad de aplicaciones comerciales y gratuitas que permiten extraer los datos ocultos de archivos de distintos formatos (pdf, docx, xlsx, etc.). Sin embargo hay algunos atributos que se obtienen que resultan un poco difícil de entender.

Por ello, para contar con las habilidades necesarias de extracción e identificación, en este capítulo se abordaran temas relacionados a herramientas en el mercado que tienen como objetivo la obtención de los metadatos, se analizaran y proporcionaran los conceptos de los diferentes tipos de datos que arrojan el análisis de los archivos.

2.1. Herramientas de extracción de metadatos

A continuación se presentan una serie de herramientas enfocadas en la extracción de metadatos, algunas de las cuales serán utilizadas para demostrar

el procedimiento de extracción y por medio de la cual se podrá apreciar el tipo de datos que se obtienen.

- **FOCA**

Utilizada principalmente para encontrar metadatos e información oculta en los documentos que examina. Estos documentos pueden estar en páginas web, y con FOCA se pueden descargar y analizar. Estos documentos se buscan utilizando tres posibles buscadores que son Google, Bing y Exalead. La suma de los tres buscadores hace que se consigan un gran número de documentos.

También existe la posibilidad de añadir ficheros locales para extraer la información EXIF de archivos gráficos. (Eleven Paths, 2015).

- **Grampus**

Es un proyecto multiplataforma que se divide en cuatro módulos: Forensic Grampus, Anti-Forensic Grampu, Grampus y Anti Grampus. Enfocados en analizar y extraer metadatos, eliminar o modificarlos. Pudiendo utilizar archivos individuales o extraídos de la web. (Sanko, 2013).

- **Metagoofil**

Es una herramienta de recopilación de información diseñada para la extracción de metadatos de documentos públicos (pdf, doc, xls, ppt, docx, pptx, xlsx). La herramienta lleva a cabo una búsqueda en Google para identificar y descargar los documentos en el disco local y luego extraer los metadatos. Con los resultados genera un reporte con los nombres de usuario, las versiones de software y servidores o nombres de máquina. (Google)

- **Jhead**

Esta aplicación se concentra en archivos gráficos como jpg, pudiendo extraer y modificar los metadatos de estos. (matthias, 2015).

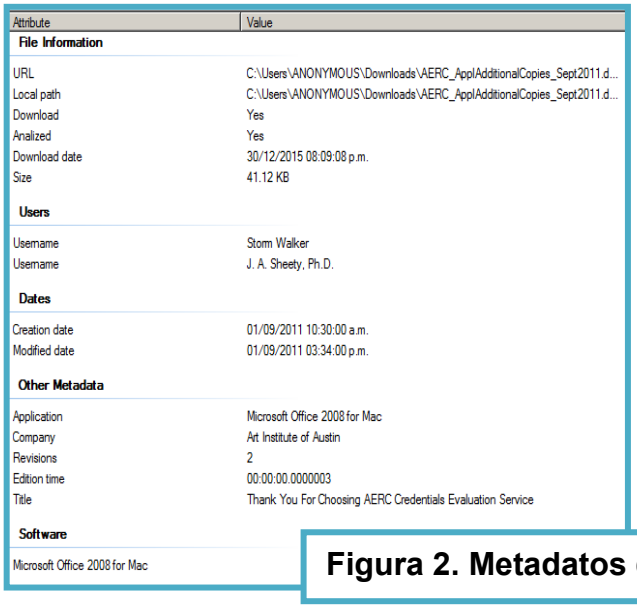
La cantidad de herramientas para extracción de metadatos es inmensa, además de las abordadas se pueden listar hachoir-metadata, ExifTool, Pinpoint Metaviewer, Exif reader, Metapicz , Exif Data, entre otras. Básicamente todas estas aplicaciones tienen como objetivo principal extraer los datos ocultos de diferentes tipos de archivos, tales como xlsx, pdf, docx, pptx, jpg, png, entre otros formatos de archivos existentes.

2.2. Metadatos obtenidos de los archivos

Para elaborar el análisis y extracción de metadatos en los archivos, se empleara la herramienta foca. Dando inicio con los archivos docx, xlsx, pdf e imágenes jpg. El lector puede emplear la aplicación para otros archivos con diferentes formatos.

- **Metadatos de archivos DOCX**

Se descargó un archivo docx del siguiente sitio web http://www.aerc-eval.com, nombrado AERC_ApplAdditionalCopies_Sept2011. A este se le procedió realizar el análisis de metadatos, lográndose obtener la siguiente información mostrada en la figura 2.



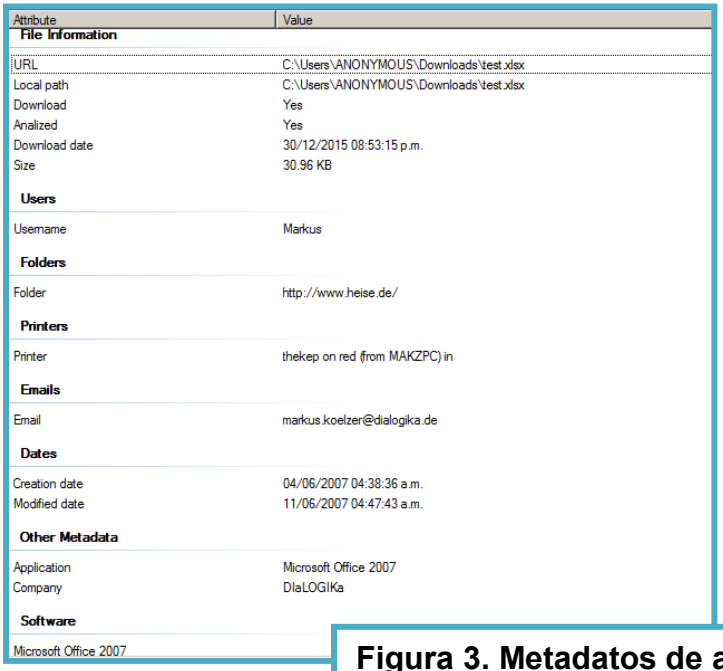
Attribute	Value
File Information	
URL	C:\Users\ANONYMOUS\Downloads\AERC_ApplAdditionalCopies_Sept2011.d...
Local path	C:\Users\ANONYMOUS\Downloads\AERC_ApplAdditionalCopies_Sept2011.d...
Download	Yes
Analized	Yes
Download date	30/12/2015 08:09:08 p.m.
Size	41.12 KB
Users	
Username	Storm Walker
Username	J. A. Sheety, Ph.D.
Dates	
Creation date	01/09/2011 10:30:00 a.m.
Modified date	01/09/2011 03:34:00 p.m.
Other Metadata	
Application	Microsoft Office 2008 for Mac
Company	Art Institute of Austin
Revisions	2
Edition time	00:00:00.0000003
Title	Thank You For Choosing AERC Credentials Evaluation Service
Software	
Microsoft Office 2008 for Mac	

Figura 2. Metadatos de archivo

Del análisis de metadatos al archivo antes mencionado se obtuvo cierta información que es importante destacar. Donde, File Information son datos de ubicación del archivo, fecha en que se descargó y tamaño. En cuanto a users se puede apreciar que hubo dos personas que revisaron el archivo Storm y J. A Shetty, además se presenta la fecha en que se modificó y creo. También la aplicación con la cual fue creado el archivos como es Microsoft office 2008 for mac, compañía a la que pertenece, cantidad de revisiones y la hora en que se editó.

- **Metadatos de archivos XLSX**

Al igual que para archivos docx, se procedió a descargar un documento xlsx de http://dev-builds.libreoffice.org/tmp/ nombrado test. Siendo escaneado y obteniendo la información mostrada en la figura 3.



Attribute	Value
File Information	
URL	C:\Users\ANONYMOUS\Downloads\test.xlsx
Local path	C:\Users\ANONYMOUS\Downloads\test.xlsx
Download	Yes
Analized	Yes
Download date	30/12/2015 08:53:15 p.m.
Size	30.96 KB
Users	
Username	Markus
Folders	
Folder	http://www.heise.de/
Printers	
Printer	thekep on red (from MAKZPC) in
Emails	
Email	markus.koelzer@dialogika.de
Dates	
Creation date	04/06/2007 04:38:36 a.m.
Modified date	11/06/2007 04:47:43 a.m.
Other Metadata	
Application	Microsoft Office 2007
Company	DIaLOGIKa
Software	
Microsoft Office 2007	

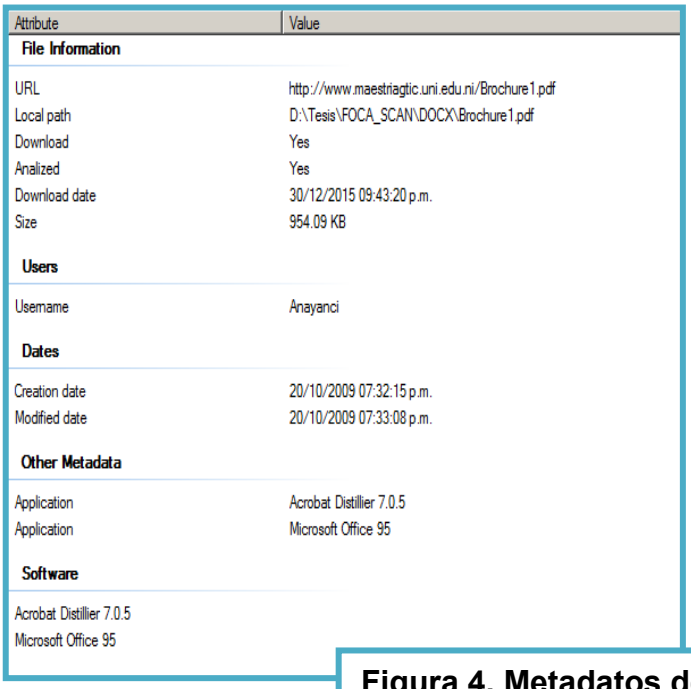
Figura 3. Metadatos de archivo .xlsx

Los metadatos obtenidos son parecidos a los docx del escaneo anterior, pero con unas cuantas diferencias, este archivo contiene información de una folder que apunta a una url relacionada, además de una impresora en red MAKZPC y

por último se logró obtener la dirección electrónica del usuario que creo el documento.

- **Metadatos de archivos PDF**

Prosiguiendo con nuestro análisis de metadatos, se descargó un documento pdf de http://www.uni.edu.ni/ nombrado Brochure1. Siendo escaneado y obteniendo la información mostrada en la figura 4.



Attribute	Value
File Information	
URL	http://www.maestriagtic.uni.edu.ni/Brochure1.pdf
Local path	D:\Tesis\FOCA_SCAN\DOCX\Brochure1.pdf
Download	Yes
Analized	Yes
Download date	30/12/2015 09:43:20 p.m.
Size	954.09 KB
Users	
Username	Anayanci
Dates	
Creation date	20/10/2009 07:32:15 p.m.
Modified date	20/10/2009 07:33:08 p.m.
Other Metadata	
Application	Acrobat Distillier 7.0.5
Application	Microsoft Office 95
Software	
Acrobat Distillier 7.0.5	
Microsoft Office 95	

Figura 4. Metadatos de archivo .pdf

Básicamente los metadatos obtenidos son muy parecidos a los de los demás escaneos, pero se logra demostrar como también los archivos pdf contienen información oculta.

- **Metadatos de archivos JPG**

Para realizar la extracción de metadatos de imágenes, se descargó una fotografía del siguiente link http://i.blogs.es/a243c1/fotografia/original.jpg, presentando la siguiente información mostrada en la figura 5.

Attribute	Value
Exif Makernote	
Make	Nokia
Model	Lumia 625
Orientation	Top, left side (Horizontal / normal)
X Resolution	72 dots per inches
Y Resolution	72 dots per inches
Resolution Unit	Inches
Software	Windows Phone
YCbCr Positioning	Center of pixel array
Exposure Time	595/500000 sec
F-Number	F 2.4
ISO Speed Ratings	100
Exif Version	2.20
Date/Time Original	2013:10:21 17:57:04
Date/Time Digitized	2013:10:21 17:57:04
Components Configuration	YCbCr
Shutter Speed Value	1/840 sec
Aperture Value	F 2.4
Exposure Bias Value	0
Metering Mode	Average
Light source	0
Flash	Flash did not fire, Auto
FlashPix Version	1.00
Color Space	sRGB
Exif Image Width	2592 pixels
Exif Image Height	1456 pixels
Exposure Mode	Auto exposure
White balance mode	Auto white balance
Digital Zoom Ratio	1
Scene Capture Type	Standard
Compression	JPEG (old-style)
Thumbnail Offset	33202 bytes
Thumbnail Length	7706 bytes
Thumbnail Data	[7706 bytes of thumbnail data]
GPS Makernote	
GPS Version ID	2 2 0 0
GPS Latitude Ref	N
GPS Latitude	39°28'49.039
GPS Longitude Ref	W
GPS Longitude	6°20'16.214
GPS Altitude Ref	Sea level
GPS Altitude	386 metres
GPS Measure Mode	3-dimensional measurement
GPS DOP	18

Figura 5. Metadatos de archivo .jpg

Hay muchos datos de bastante interés que se pueden apreciar en este escaneo, primeramente se observa el modelo y marca del equipo con que fue tomada la fotografía como es un Nokia Lumia 625, el sistema operativo que es Windows Phone y un dato muy importante que es la ubicación geográfica. Además de otro tipo de información, que brinda características de cómo fue tomada la foto.

A como se ha visto en los diferentes tipos de archivos analizados se ha podido extraer algún tipo de información sensible que podría conllevar a un riesgo de seguridad, ya sea a empresas o individuos. Simplemente con una simple herramienta y unos pocos archivos se puede tener un amplio conocimiento de un objetivo.

3. Metadatos como instrumento para realizar ataques.

Para realizar un ataque informático se deben desarrollar 5 etapas de las cuales dependerá el éxito del ataque, estas fases son reconocimiento, escaneo, ganar acceso, mantener el acceso y cubrir la huellas (Mamani, 2013).

El primer paso es el reconocimiento, aquí es donde los metadatos son mayormente utilizados, ya que la información que proporcionan permite al atacante conocer como está estructurada la organización, el personal interno, el software que utiliza, entre otros datos que sirven de insumo para llevar a cabo las siguientes etapas.

Con el objetivo de conocer como los metadatos son utilizados para lograr realizar un ataque, se analizara en este capítulo el tipo de información que revelan lo metadatos, la manera en que puede ser utilizada y presentaran algunos ejemplos de ataques que tuvieron éxitos donde se utilizaron los metadatos.

3.1. Más allá de los metadatos

Los metadatos en algunos casos revelan información muy sensible y no eliminarlos es un problema de seguridad, hasta tal punto que pueden llegar a comprometer la privacidad del individuo y abrir las puertas a que un ataque tenga éxito.

La facilidad con que se obtienen los archivos en diferentes formatos y la poca precaución de empresas y personas en cuanto a la eliminación de los metadatos, es un debilidad que los hackers utilizan para realizar sus ataques o pruebas de seguridad (Bautista, 2013).

Para demostrar como de un simple archivo se puede obtener gran cantidad de información, se procederá a hacer uso de los diferentes archivos escaneados en el capítulo anterior y analizara que tanto conocimiento se puede obtener.

- El documento en Word de la figura 2 demuestra algunos datos importantes, primeramente encontramos que hay dos usuarios que editaron este archivo, lo que podría indicar que dentro de la organización se encuentran dos equipos que están asignados a estas dos personas o también pudo haber sido compartido por usb u otro medio, ya sea para su revisión o aprobación. Además al tener los nombres y apellidos de los usuarios se podría conocer la dirección de correo electrónico, debido a que se posee el dominio de donde fue descargado. Otro dato sobresaliente es el software que utilizaron para crear el archivo, como se observa es Microsoft Office 2008 for mac, ahora sabemos que estas personas que crearon y editaron el archivo tienen equipos mac, con los cuales trabajan y tienen instalado un software de Microsoft Windows. Y por último se observa el nombre de la compañía Art Institute of Austin, posiblemente sea el lugar donde se originó el archivo y no del sitio donde se descargó.

- El documento en Excel de la figura 3 es un poco más interesante que el anterior, en este se puede apreciar el usuario que creo el archivo y fácilmente se obtiene su correo electrónico, ya con estos datos se puede determinar la nomenclatura que utilizan en la empresa para asignar cuentas de correo a sus usuarios, el nombre de la organización dialogika tampoco coincide con la dirección de donde se descargó, por lo que este archivo también se originó en otro sitio y está almacenado en un servidor diferente. Además se observa que dentro de la organización poseen al menos una impresora que está en red y por último el software con que se creó el archivo es Microsoft Office 2007, con lo que se podría argumentar que el sistema operativo del equipo es un Windows.

- Sobre el documento en PDF de la figura 4, aunque la información es similar a la de los demás archivos en cuanto a usuario y fecha de creación o edición, hay un aspecto importante el cual es el software utilizado, fácilmente se observa que utilizaron Microsoft Office 95 para crear el archivo y posteriormente lo exportaron empleando Acrobat Distillier 7.0.5. Al igual que el Excel también podría decirse que el sistema operativo es Windows 95 o talves superior.

- El siguiente archivo de la figura 5, se trata de una imagen en formato jpg. La cantidad de información que se obtuvo es bastante detallada, fácilmente se reconoce que el equipo con que se tomó la es un celular Nokia modelo Lumia 625, el cual corre el sistema operativo Windows Phone, esta foto fue tomada sin el flash, por lo que se realizó durante el día. También hay un dato importante y es que se logra obtener la ubicación geográfica en donde fue tomada la fotografía, con lo que se podría saber la procedencia de la imagen.

Con estos simples archivos se ha podido demostrar la relevancia que tienen los metadatos en la seguridad, fácilmente se puede obtener información con solo realizar un pequeño análisis y aprovecharse de esto es solo el comienzo de hasta donde se puede llegar.

3.2. Como aprovecharse de los metadatos

En puntos anteriores se ha tratado la utilidad que tienen los metadatos, ya sea para catalogar o agilizar búsquedas. Esta es la parte positiva de contar con ellos, sin embargo al ser información en algunos casos privada y sensible, se vuelven un medio a través del cual se podrían crear amenazas y hasta explotar alguna vulnerabilidad en los sistemas.

Para seguir demostrando que tan riesgoso es no eliminar los metadatos de los documentos digitales, se utilizaran nuevamente los archivos anteriores. De esta

manera se plantearan algunas técnicas con las cuales se podría aprovechar esta debilidad en la seguridad.

El escaneo de los documentos docx, xlsx y pdf lo agruparemos como uno solo, ya que la estructura de metadatos obtenida es similar entre ellos, mientras que los datos de la foto serán analizados individualmente. A continuación se definen los atributos obtenidos y algunas técnicas que los atacantes podrían emplear para lograr sus objetivos.

- **Usuario**

Los documentos escaneados tienen el nombre de los usuarios en sus metadatos, para aprovecharse de ello podría hacerse uso de ingeniería social y teniendo muy en cuenta que el usuario es el eslabón más débil en la cadena de seguridad, se vuelve un blanco fácil.

La mayoría de las personas utiliza su nombre para registrarse en diferentes sitios web, proporcionan sus correos electrónicos, número telefónicos, contraseñas, direcciones, nombres de amigos de trabajo, etc. Este es un error que muchos cometen, ya que no todo los sitios en internet brindan los niveles de seguridad adecuados, haciendo que la información pueda ser vista por cualquiera. Al realizar una investigación exhaustiva y luego de que se haya recopilado información extra del objetivo, podría llevarse a cabo ataques más elaborados como llamadas telefónicas, envió de correos con virus adjuntos o algún método para engañar al usuario y así recopilar más datos o encontrar un punto de acceso.

Si el usuario cometió el error de relacionar a sus compañeros de trabajo, ya sea en alguna red social o grupos de amigos, fácilmente se podría crear un esquema de quienes integran la compañía y así ampliar el espacio de búsqueda. Al tener mayores puntos donde buscar, la probabilidad de encontrar algún fallo o vulnerabilidad es mayor.

- **Compañía**

Otro punto importante que contienen los metadatos es el nombre de la compañía, es importante mencionar que el sitio web de donde se descargaron los archivos aparentemente en algunos casos no tiene relación con la empresa que indican los metadatos. De ahí se podría argumentar que de una u otra manera ambas compañías está relacionada, ya sea en los negocios o sistemas compartidos.

Nuevamente se debe realizar un trabajo investigativo ahora empleando el nombre de la compañía, teniendo como objetivo recolectar más información. Entre la técnica para recopilar se podría navegar en el sitio web de la empresa, buscar contactos, números telefónicos, direcciones, correos electrónicos. Es más, al tener los números telefónicos, sencillamente se podría realizar una llamada y preguntar por el autor del archivo y de esa manera saber a qué empresa pertenece.

Actualmente en el mercado existen diversas herramientas que automatizan el proceso de recopilación de información de los sitios web, con lo cual se vuele más rápido y sencilla esta tarea.

- **Aplicaciones**

El contar con el nombre de sistemas operativos, aplicaciones y versiones en los metadatos, es un gran error en seguridad, ya que se vuelve información muy sensible que puede ser aprovechada, permitiendo lograr los objetivos del atacante.

Al conocer el sistema operativo, se podría pensar en la infraestructura que posee la empresa, pudiendo tener algún servidor que aloja los servicios relacionados a una sola plataforma o algunos otros programas comunes que son instalados en esos sistemas.

Fácilmente desde el momento que se conoce los sistemas internos, empieza la tarea de buscar vulnerabilidades que ya hayan sido descubiertas y si el administrador no tomo las medidas adecuadas para actualizarlas, podrían ser explotadas, otorgando diferentes privilegios al que realiza el ataque. En esta etapa nos encontraríamos en la fase de ganar acceso, debido a que se estaría realizando un proceso de ataque directo.

Anteriormente a esto, se encuentra la fase de escaneo, esta etapa es un poco más invasiva que la de reconocimiento ya que lo se busca es información mas privada del objetivo, con el fin de lograr obtener algunos otros puntos de accesos. Algunos administradores utilizan la técnica de proporcionar falsos positivos como método de engaño, para que los atacantes se enfoquen en cierta plataforma operativa, cuando en realidad se está utilizando otra. Sin embargo al disponer de la información de los metadatos, se podría tener otra perspectiva y mayor seguridad en lo que se está obteniendo, teniendo mayores márgenes de éxitos y menos pérdida de tiempo.

Este tipo de técnica de buscar vulnerabilidades y explotarlas, aplica también para las aplicaciones, no solamente para sistemas operativos. Además, se podría pensar en utilizar algún otro software como virus específicamente creados para un sistema específico y que otorgue de cierta manera acceso al equipo.

- **Correo electrónico**

Aunque en el proceso de realizar una búsqueda de información se pueda lograr obtener los correos electrónicos, los metadatos en ocasiones ahorran esa tarea, como sucede con uno de los archivos escaneados.

Al contar con el correo electrónico, se puede conocer el tipo de nomenclatura que utiliza la compañía para asignar direcciones a sus empleados, teniendo esto se podría utilizar la ingeniería social para sacar provecho de ello y el ataque no

estaría dirigido a un solo usuario sino a todo los miembros de la organización, de así desearlo. Además, como antes se ha mencionado, se enviaría un archivo adjunto que contenga algún virus, el cual podría brindarnos una puerta trasera de llegarse a ejecutar.

De acuerdo al perfil del usuario del que se desea obtener información, se podría redactar correos, solicitando ciertos datos o tratando de establecer alguna relación que permita poco a poco ir estableciendo comunicaciones, para que en el momento oportuno se ejecute el ataque sin que el usuario tenga sospecha.

- **EXIF**

Los metadatos EXIF de las imágenes cubren una amplia cantidad de información que caracteriza la foto. Estos datos incluyen la marca, el modelo y el sistema operativo que utiliza.

Sin importar la plataforma en la que corran los sistemas operativos, si no se actualizan tienden a presentar vulnerabilidades que poco a poco van surgiendo, las cuales pueden encontrarse en la web, en la mayoría de las veces con sus respectivos exploit. Además, al presentarse tanto la marca como el modelo del equipo se podría formular ataques basados en hardware.

Inclusive la ingeniería social podría aplicar utilizando estos datos, al conocer la marca y modelo, se podría proporcionar una conexión wifi gratuita para que al momento que se conecte un usuario con estas características de teléfono, intercepte los paquetes, recolectando así información específica de una determinada persona.

- **GPS**

Posiblemente este sea el tipo de metadato obtenido de las cámaras más sensibles y riesgosas en lo que respecta a la seguridad humana, ya no enfocándonos más en sistemas, sino en las personas físicamente.

En la información proporcionada por el GPS se incluye la ubicación geográfica de donde se tomó la foto en cualquier parte del mundo y con una precisión métrica. Si una persona publica o sube una foto a la web, solamente con tener estos datos de localización y utilizando algún sistema de información geográfica, en cuestión de segundos puede ubicarse su posición. Si hay fotos continuas de diferentes lugares, se podría crear un mapa de rutas en los sitios que anduvo la persona y si es rutinaria la trayectoria, en cualquier momento el atacante la podría interceptar o darle seguimiento. O también, se podría saber en qué momento sale de la casa, pudiendo cometer así algún robo.

Es impresionante como los metadatos proporcionan tanta información y la cantidad de técnicas que pueden ser aplicadas para sacar el mejor provecho de ello. Publicar archivos con metadatos es un grave riesgo en la seguridad, que podría traer grandes consecuencias a las personas u organizaciones.

3.3. Acontecimientos exitosos empleando metadatos.

Después de haber analizado un poco el mundo de los metadatos y como no eliminarlos es un riesgo para las organización e individuos. Se presentan algunos ejemplos en los cuales el factor de éxito obtenido fue gracias a que se disponían de los metadatos.

- Hawk Carlise, comandante de las fuerzas aéreas del ejercito de los Estados Unidos, localizo la ubicación exacta de un cuartel general del Estado Islámico gracias al selfie que había publicado en Internet uno de los miembros de la organización. 22 horas después de que se descubriera la fotografía se había confirmado la ubicación exacta y lanzado un ataque militar que acabó con la base (Everstine, 2015).

- El fundador de la compañía McAfee se encontraba escondido tras huir de las fuerzas de seguridad, que lo habían declarado "Person of Interest", pero invitó a un periodista a entrevistarle. Este publicó una fotografía con un teléfono iPhone4S, la cual contenía información del GPS en sus metadatos, dejando en claro que estaba en Guatemala. (Maligno, 2012).

- La Unidad de Delitos Económicos y Fiscales (UDEF) que investiga la trama Gurtel, acreditó que 200.000 € en tres facturas hechas en Excel eran falsas porque a pesar de tener meses de distancia entre unas y otras, en los metadatos todas se pudo ver que habían sido creadas con una diferencia de 3 minutos entre ellas. (Zafra, 2012).

- La novia de un defacer publico una fotos en Facebook que contenía información GPS de dónde se había tomado, esto llevó al FBI a detener al delincuente. (Salaberry, 2012).

- El caso de Alex Tapanaris saltó a las noticias. En pleno momento de popularidad de anonymous, una de las notas de prensa de AnonOps mostraba en los metadatos un nombre Alex Tapanaris. Ese nombre apuntaba a un diseñador gráfico, del que analizando los metadatos de su web se podía leer un nickname t4pan. De ahí, a dar con su persona y acabar detenido fue cuestión de poco tiempo.(ITProPortal, 2010).

En estos ejemplos se demuestran como los metadatos son utilizados para revelar información oculta, con lo cual se podrían realizar investigaciones para dar con un criminal o formular ataques, esto en dependencia de las intenciones de quien manipule los documentos. Por ello es importante que dentro de nuestras medidas de seguridad antes de publicar cualquier tipo de archivo, estos vayan limpios de metadatos, ya que son un riesgo tanto para la organización como el individuo.

4. Correo electrónico

El correo electrónico es uno de los principales medios de comunicación que utilizan las personas y empresas en el mundo, debido a que es sumamente útil su crecimiento ha sido inmenso. Según estudios para el 2017 se estima una proyección de 4,920 millones solo en cuentas comerciales y 1,138 millones en cuentas corporativas. (The Radicati Group, inc., 2013).

Estos datos corresponden solamente a direcciones de correo electrónico, quiere decir que la cantidad de tráfico o correos que se intercambia a diario es muchísimo mayor. Por tal motivo, las compañías y los delincuentes lo han visto atractivo, tanto como medio de propaganda, ventas, ofrecer servicios o para llevar a cabo ataques, propagación de virus, robos, entre otros. Lo que afecta la seguridad del individuo como tal.

De acuerdo al estudio realizado por McAfee en el primer trimestre del 2015, se presentan cifras estadísticas muy altas de las amenazas en la que está involucrado el correo electrónico y las diferentes técnicas de ataques relacionadas. (McAfee, 2015). A como se muestra en los siguientes gráficos.

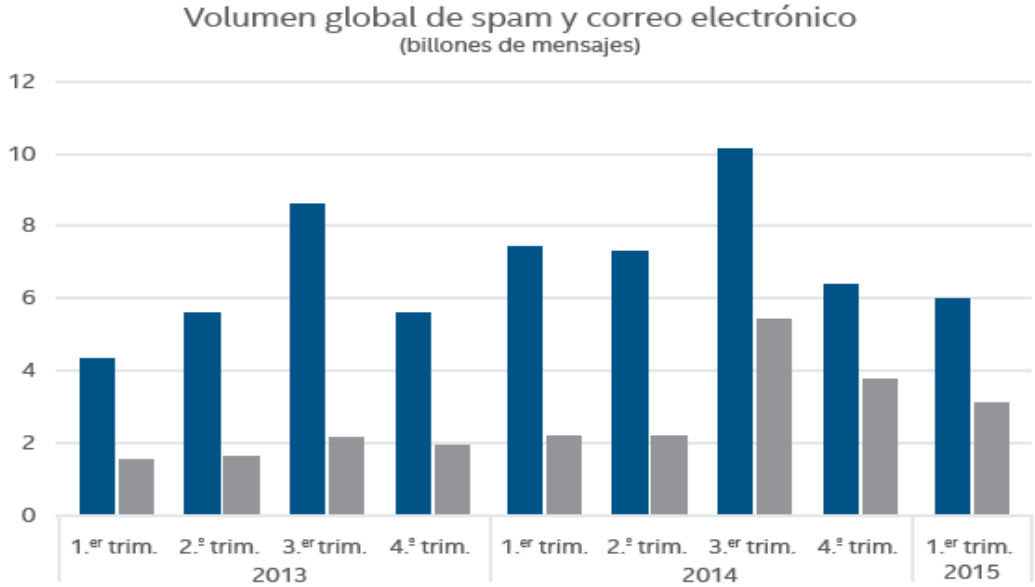


Figura 6. Fuente: McAfee Lab, 2015

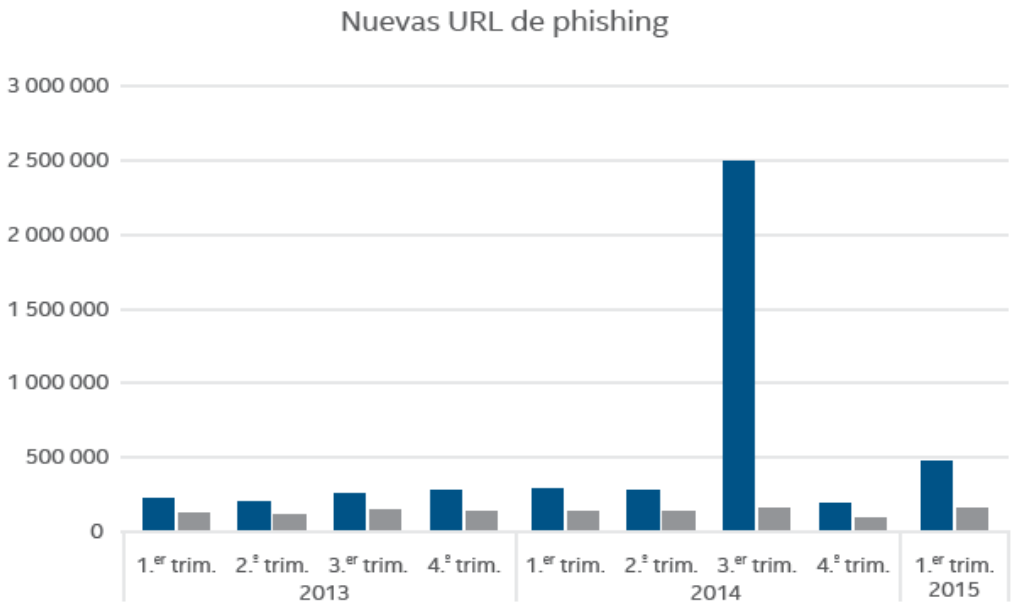


Figura 7. Fuente: McAfee Lab, 2015

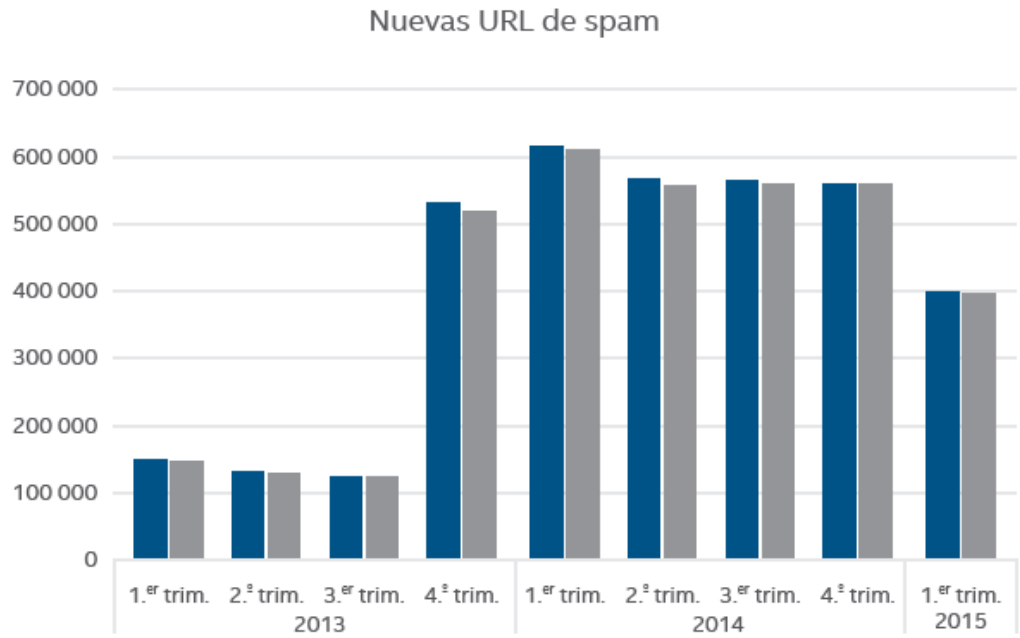


Figura 8. Fuente: McAfee Lab, 2015

Sin duda alguna estas cifras son bastante abrumadoras. Para disminuir estas amenazas se han creado gran cantidad de herramientas, sin embargo los atacantes logran traspasar esta seguridad y consiguen alcanzar sus objetivos. Con el fin de tener un mejor conocimiento sobres estas amenazas y comprender así mejor su actuar, en este capítulo se analizara como puede ser utilizado el

correo para elaborar un ataque, las técnicas que se utilizan y las razones por la cuales tienen éxito.

4.1. Elaboración de un ataque haciendo uso del correo electrónico

Los delincuentes antes de elaborar un ataque se toman cierto tiempo para analizar e investigar su objetivo. A como anteriormente se mencionó ejecutan una etapa de reconocimiento, en la que se trata de recopilar la mayor cantidad de información con el fin de lanzar el ataque más adelante. (Berrio).

Dentro de estos datos que son recopilados se pueden encontrar direcciones de correo, las cuales una vez que están en manos de los criminales pueden ser usadas para diferentes fines, aunque también podría tratarse de un recolector de direcciones de correo electrónico. En la actualidad existe una gran cantidad de sitios que para descargar un archivo, ver alguna publicación o video, solicitan que se facilite el correo electrónico, esto tiene como principal tarea crear base de datos de correos, para luego utilizarlas para generar propaganda, venta de servicios, propagación de virus, engaños, entre otros. Inclusive en la web hay herramientas como Email Extractor que buscan y extraen correos electrónicos de varias fuentes.

Como se ha demostrado el primer punto que se emplea para la elaboración de un ataque es la recopilación de las cuentas electrónicas. Al contar con esta información lo siguiente que se realiza es investigar a las potenciales víctimas para luego formular ataques a dos grupos objetivos distintos:

- El primero grupo se centra en un objetivo específico, en el cual el ataque es dirigido ya sea a una persona o entidad, del que se tiene cierta información privada o personal. De esta manera el correo electrónico es personalizado, la información que contiene está relacionada a los intereses de la víctima y por ser algo conocido, este tiende a confiar y ser engañado con más facilidad.

- El segundo grupo está enfocado en correos masivos, en este caso debido a que no se conoce información de la víctima, se envían correos con información muy general y nada personalizado, pero debido a la cantidad correos generados, hay bastante probabilidad de que el ataque sea exitoso.

Finalmente cuando ya se cuenta con la dirección del correo electrónico y se establece el tipo de objetivo al que se va a realizar el ataque. Se procede a emplear los diferentes ataques existentes, tales como spam, phishing, hoax, ingeniería social, entre otras que serán abordadas en el siguiente acápite.

4.2. Amenazas en el correo electrónico

En internet existen todo tipo de trampas y técnicas bien diseñadas para obtener algún beneficio de los usuarios y actualmente la mayor parte de estas amenazas llegan en forma de correo electrónico. (Universidad de Jaen, 2013). Una vez que el atacante está satisfecho con la información recopilada del objetivo y tiene claro el alcance, es cuando da inicio a su ataque. Para ello emplean diferentes técnicas que tienen propósitos distintos, tal como infección de virus, realizar fraudes bancarios, propagarse a las demás direcciones de correo de la víctima. Ya sea empleando ingeniería social o algún otro método de engaño.

Para entender mejor cada uno de las amenazas que se emplean, a continuación se abordaran a detalle.

- **SPAM**

Es el correo electrónico no solicitado que es enviado masivamente a un número muy amplio de usuarios generalmente con el fin de comercializar, ofertar o tratar de despertar el interés con respecto a algún producto o servicio. Este tipo de correos electrónicos también sirve como punto de partida para cometer delitos tal como phishing o el scam. (Panda).

En la propagación del spam aunque están involucradas las empresas proveedoras de productos y servicios, los principales responsables son los creadores de malware, quienes emplean redes zombies para ampliar así la cantidad de correos enviados (ESET, 2011). De acuerdo al estudio realizado por CYREN (2015). “En septiembre del 2015 los niveles de spam fueron los más bajos en 6 años, alcanzando 47.6 billones por día” (p.18).

- **SCAM**

Es un tipo de correo electrónico fraudulento que pretende estafar económicamente al usuario por medio del engaño. Podría ser categorizado como hoax sino fuera porque además del engaño, también buscan el beneficio económico. Por lo tanto, es una mezcla de phishing, pirámides de valor y hoax. (Panda).

Algunos ejemplos clásicos incluyen avisos que indican que has ganado la lotería (cuando ni siquiera has participado), o que alguien necesita transferir millones de dólares a tu país y le gustaría pagarte para que lo ayudes con la transferencia. Entonces, te dirán que tienes que pagar primero una tarifa de procesamiento antes de poder obtener tu dinero. Después de pagar estos honorarios, los criminales desaparecen y nunca más vuelves a saber de ellos. (SANS, 2011).

- **HOAX**

Son correos que contienen información sobre temas diversos, cuyo contenido, además de las conocidas corrientes, consiste en llamamientos dramáticos de corte sentimental o religioso; supuestas campañas humanitarias, de socorro personal, o peor aún, avisos sobre falsos virus cibernéticos que amenazan con infectar su ordenador. (Arias, 2014).

En muchas ocasiones, los hoaxes informáticos son creados por usuarios maliciosos que sólo pretenden hacer una broma pesada. También pueden servir

para recoger un gran número de direcciones de correo electrónico a las que, posteriormente envían mensajes de correo no deseado o spam. (Panda, 2004)

- **PHISHING**

Es una forma de fraude electrónico, caracterizado por adquirir datos personales de diversos tipos; contraseñas, datos financieros como el número de tarjeta de crédito. (Arias, 2014).

Un ataque de phishing comienza con un correo electrónico que pretende proceder de alguna persona u organización que conoces y en quien confías, como tu banco o tienda favorita en línea. Estos correos electrónicos tratan de convencerte para realizar una acción, como dar clic sobre un enlace, abrir un archivo adjunto, o responder a un mensaje. Los cibercriminales elaboran estos correos electrónicos de manera convincente, después los envían a miles, si no es que a millones de personas alrededor del mundo. (SANS, 2011). Solamente en el tercer cuarto del 2015 CYREN rastreo 4.3 millones de url relacionadas al phishing. (CYREN, 2015).

- **PHARMING**

Aunque es muy parecido al phishing debido a que su finalidad es llevar al usuario a una página falsa para robarle información personal, este difiere un poco en el método de engaño, ya que no necesita incitar a la víctima a que haga clic en un enlace incluido en un correo. Este tipo de amenaza consiste en que el usuario teclea la dirección del sitio web en su navegador y debido que el servidor o su equipo ha sido vulnerado por el delincuente, este lo dirige a una página diferente. Algunas veces con apariencia idéntica a la original. (Aguilera, 2010).

El atacante logra hacer esto al alterar el proceso de traducción entre la URL de una página y su dirección IP., para ello requiere instalar en el sistema de la víctima alguna aplicación o programa malicioso (por ejemplo, un archivo ejecutable .exe, .zip, .rar, .doc, etc.) que lo logra introducir a través de diferentes

métodos, como descargas, correo electrónicos o unidades de almacenamiento removibles.

- **Pirámides de valor**

Esta amenaza consiste en captar a usuarios a través de anuncios atractivos y que prometen grandes ganancias. Una vez que se ha engañado al usuario, recibe un correo electrónico o un enlace para acceder a una determinada página web en la que solicitan sus datos personales y cuenta bancaria para poder realizar los ingresos de las futuras comisiones.

Los usuarios solamente deben pagar una determinada cantidad de dinero e incluirse en una cadena de correos. A través de esa cadena, ellos remiten a su vez miles y miles de correos electrónicos para que sus destinatarios repitan el mismo proceso. Cuantos más correos electrónicos envíen más comisión generan, sin embargo ese beneficio no es real. (Medina, 2014).

- **Email spoofing**

Básicamente email spoofing es un subtipo de spoofing, el cual se basa en suplantar la identidad de un equipo o usuario, realizando acciones sobre un sistema en su nombre, llevándose a muchos niveles: usuario, correo, etc. (Gallego, 2014).

Cuando se da la suplantación de la dirección de correo electrónico de otras personas o entidades, se le denomina email spoofing. Dicho de otro modo, la dirección de correo que aparece en el remitente, aunque aparentemente es real, esta es una suplantación del original. Por lo que cuando las víctimas reciben alguna petición de este tipo y ven que proviene de un contacto conocido, pueden morder el anzuelo y facilitar información confidencial.

A como se aprecia existen un sin número de amenazas muy bien diseñadas, cuyo objetivo es realizar algún daño al usuario y obtener alguno provecho de él.

Los delincuentes han utilizado muy bien la ingeniería social para engañar a las personas y así alcanzar el éxito en sus ataques. Para no ser víctima de ello, se debe contar con soluciones de seguridad y estar alerta ante cualquier correo sospechoso

4.3. Análisis del éxito de los ataques

Los factores que determinan el éxito de los ataques cuando se utiliza el correo electrónico son muy diversos. Algunos van desde malas prácticas de seguridad, hasta el mismo desconocimiento del usuario.

Estas malas prácticas abordan muchos aspectos, entre estos se encuentra la desactualización de los sistemas, no contar con antivirus, dejar configuraciones por defectos en los sistemas operativos, no aplicar otras configuración de seguridad, dejar sin protección las redes, utilizar contraseñas débiles, etc. (ESET, 2009).

Además, es importante tomar en cuenta a los usuarios, quienes son catalogados como el eslabón más débil en la cadena de seguridad. (Delgado, 2013). Esto debido a que al momento de navegar por internet acceden a sitios de dudosa reputación, se inscriben en diferentes sitios web, no tienen precaución en proporcionar sus datos, no se toman las medidas necesarias al momento de leer o descargar archivos adjuntos en correo electrónico o sitios web, etc. Básicamente, el usuario debido a que no toma las debidas precauciones tiende a permitir involuntariamente que los ataques sean exitosos.

Sin embargo, hay que tomar muy en cuenta la labor de los delincuentes quienes pasan horas investigando para realizar el ataque. Su punto de partida es el engaño, para ello emplean la ingeniería social que consiste en la manipulación de personas influenciándolas a ejecutar determinada acción, que las lleva a ser víctimas de un delito informático. (Pérez, 2014).

Debido a que la formulación del engaño está debidamente realizada, al momento en que la víctima se enfrenta contra la técnica del ataque, si este no posee conocimientos pertinentes, fácilmente puede ser engañado. En este caso la ingeniería social se podría implementar para correos spam, phishing, scam, hoax, pirámides de valor y email spoffing, ya que primeramente deben brindar al usuario la confianza, para que una vez obtenida proceda con el siguiente paso que es brindar sus datos personales o acceder algún sitio predeterminado.

Es importante notar que este ataque está dirigido a las personas y no a los sistemas en si, por tal motivo el principal éxito es el engaño y la confianza que brinda al usuario. Siendo el más utilizado por la facilidad que requiere.

Aunque el éxito de los ataques está más vinculado al usuario, si los sistemas no están debidamente asegurados y actualizados, podrían presentar vulnerabilidades que los delincuentes podrían explotar. Pudiendo así propagar amenazas y delitos empleando el pharming o phishing.

A como se puede apreciar el éxito del ataque esta mayormente relacionado al usuario, las malas prácticas de seguridad que utiliza y el desconocimiento de este, permiten que el delincuente logre su cometido.

5. Protección contra ataques

En los capítulos anteriores se ha visto las diferentes maneras en que la información y los medios de comunicación (correo electrónico) pueden ser aprovechados para realizar un ataque, demostrando que desde un simple archivo se puede extraer datos muy importante que podrían ser utilizada para llevar a cabo delitos y la implementación de diferentes técnicas para lograr engañar a las personas, todo ello con el objetivo de obtener algún provecho, afectando así al usuario y perjudicando la seguridad de ellos.

Por tanto, para estar preparado ante estas amenazas y disminuir el riesgo de ser víctimas de estos ataques, en este capítulo se plantearan algunas herramientas con las que se cuenta para la protección, se analizaran las medidas que las personas pueden tomar para no ser engañadas, además se investigaran que métodos podrían permitir la identificación de alguna amenaza, todo ello enfocado en dos aspectos, como son los metadatos y el correo electrónico.

5.1. Herramientas de protección

Debido a la gran cantidad de amenazas actuales, las cuales oscila en aproximadamente 400, 000,000 de nuevos malware, amenazas web distribuidas en casi 30, 000,000 de nuevas url sospechosas y 500,000 url nuevas de pishing, solamente para el 1er trimestre del 2015. (McAfee, 2015). Es impresionante tal cantidad, por ello diferentes entidades se han encargado de desarrollar herramientas que permitan proteger a los usuarios de estas, disminuyendo así el éxito de un ataque.

La cantidad de herramientas en el mercado es inmensa, van desde aplicaciones gratuitas hasta comerciales, sin embargo el objetivo de esta investigación no es facilitarle una lista de software a utilizar, sino más bien los beneficios que otorgarían contar con ello y los niveles de seguridad que se lograrían obtener. Los cuales se presentan a continuación.

- **Filtro Web o de contenido**

Un filtro web, comúnmente conocido como "software de control del contenido", es una aplicación diseñada para restringir los sitios web que un usuario puede visitar en su equipo. (Kaspersky).

Se utilizan a menudo como herramienta de prevención de malware o phishing, ya que los filtros bloquean el acceso a los sitios que comúnmente los alojan.

Además de ello, optimiza el ancho de banda, al impedir visitas a páginas inapropiadas (Panda, 2010).

Proporciona altos niveles de seguridad, ya que al navegar en internet solo se puede acceder a url categorizadas como confiables, por tal motivo el riesgo que se corre de ser víctima de algún ataque es menor.

Actualmente en el mercado hay una gran variedad de filtros web tales como Fortinet, Sophos, Astaro, Symantec Web Gateway entre otros.

- **Antivirus**

Es un programa que tiene como función principal prevenir, detectar y eliminar los virus informáticos, tal como spyware, malware, entre otros, minimizando así los riesgos.

En dependencia de la solución que se adquiera, esta puede proporcionar una serie de características de protección, tal como defensa contra estafas online (phishing), contra spam, seguridad en operación bancarias y compras en línea, (Kaspersky, 2016). Gestión de contraseñas, firewall, entre otros.

Los antivirus actualmente proporcionan una amplia gama de herramientas de protección, que ayudan a disminuir los riesgos de ataques tanto para las organizaciones como a las personas. Entre estos se encuentran Eset, Kaspersky, Panda, AVG, etc.

- **Antispam**

Estas herramientas tienen como objetivo lograr el filtrado de correos basura o spam para que no lleguen a la bandeja de entrada de los correos electrónicos. Al utilizar un antispam ya sea que venga incluido en las características del cliente del correo electrónico o por otra fuente, proporciona una serie de ventajas, ya

que reduce la propagación de virus, evita que los servidores dejen de estar en servicio debido a ataques masivos de spam, pudiendo saturar la capacidad del hardware, además de que disminuye la probabilidad de que los usuarios sean víctimas de ataques empleando ingeniería social.

Muchas herramientas antispam se han desarrollado, entre las que destacan los mismos antivirus, los cuales incorporan esta característica de seguridad. También, los mismos clientes del correo electrónico, incluyen módulos para configurar sus propios antispam.

- **Antiphishing**

Es una herramienta que evita que se visite sitios web no seguros o duplicados, esta analiza el nivel de seguridad de los sitios web que se visitan. También bloquea la navegación en sitios web que está confirmado que son fraudulentos o sospechosos. Protegiendo del cibercrimen bloqueando y detectando las aplicaciones y correos electrónicos que solicitan información confidencial haciéndose pasar por entidades legitimas.

Al igual que para el antispam, el auge que ha tenido esta técnica de ataque ha impulsado a las empresas relacionadas a la seguridad, en ofrecer servicios y aplicaciones que protejan a los usuarios contra estas amenazas. No solamente los antivirus incorporan esta protección entre sus características, sino también los mismos navegadores web tienen extensiones antiphishing y filtros de contenido web.

- **Limpieza de Metadatos**

Estas herramientas permiten identificar y eliminar los metadatos de los diferentes archivos digitales, previniendo así la fuga de información sensible y protegiendo a los usuarios contra posibles ataques, ya que se evita revelar datos confidenciales. Algunas de estas aplicaciones ya vienen incorporadas dentro de

las funcionalidades del software con que se creó el archivo, otras se pueden obtener de diferentes sitios web.

Actualmente existen varios software que ofrecen entre sus funcionalidades la capacidad de protección múltiple bajo una sola solución, sin embargo aunque son herramientas potentes, presentan ciertas limitantes en cuanto asegurar todos los puntos débiles en los equipos y redes informáticos. Por tal motivo, se debe contar con más de una aplicación, la cual debe ser utilizada de acuerdo a las necesidades del usuario.

5.2. Medidas a tomar por parte del usuario para no ser víctimas de ataques

Las políticas de seguridad y las soluciones no pueden evitar un ataque, si el personal no cuenta con la educación ni la disposición. (Delgado, 2013). En repetidas veces se ha mencionado que el usuario es el eslabón más débil en la seguridad. Según un estudio se demuestra que 78% considera a aquellos empleados negligentes o descuidados, que no se apegan a las políticas de seguridad, como la mayor amenaza para los sistemas. (Ponemon Institute LLC, 2015).

En su participación en uno de los paneles internacionales, el comisario Ingeniero Oliver González Barrales, director general de ciberseguridad - CERT MX, reconoció que en el tema de la seguridad cibernética, “el eslabón más frágil es el ciudadano, el usuario común, quien puede ser el filtro o facilitador para un ataque de mayores consecuencias, con sólo abrir un correo electrónico con un código malicioso”. (SEGOB, 2015).

Aunque los dispositivos de seguridad ayuden bastante, si detrás de ellos no está un personal capacitado, este mismo personal puede llegar a poner en riesgo su seguridad y la de la empresa. Si el usuario asigna contraseñas débiles,

este será un punto principal por el cual se podría violar la seguridad. Para ello es importante implementar una serie de medidas por parte del usuario., que a continuación se presentan.

5.2.1. Protección al compartir archivos e información

- Intentar no publicar información sensible y confidencial en redes sociales o internet, debido a que personas extrañas pueden aprovechar esta información con fines maliciosos.
- Es recomendable evitar la publicación de fotografías propias y de familiares. Las fotografías pueden ser utilizadas para complementar actos delictivos, incluso fuera del ámbito informático, ya sean en redes sociales o web en general.
- Si se van a compartir archivos a través de correo electrónico, dispositivos extraíbles, nube o algún otro medio de trasmisión, es recomendable utilizar herramientas para que realicen la limpieza de los metadatos.
- Tener la certeza de que se comparte archivos e información con personas u empresas que realmente dicen ser quienes son, ya que podría tratarse de algún engaño.
- Para evitar que los archivos e información sean leídos, si en dado caso se interceptan por un delincuente, es importante cifrarlos antes de enviarlos.
- Cuando se reciben adjuntos ya sea en el correo electrónico o se descargan de algún sitio, prestar especial atención a las extensiones de los mismos, ya que suelen utilizar técnicas de engaño como la doble extensión o espacios entre el nombre del archivo y la extensión del mismo.
- Impedir la ejecución de archivos desde sitios web sin verificar previamente que es lo que dice ser. Es importante no hacer clic sobre el botón ejecutar ya que esto provoca que el archivo se ejecute automáticamente luego de descargado, dejando al margen la posibilidad de verificar su integridad

5.2.2. Protección en el correo electrónico

- No confiar en correos spam con archivos adjuntos y explorar el archivo antes de ejecutarlo. Esto asegura que no se ejecutará un malware.
- Utilizar filtros anti-spam que permitan el filtrado del correo no deseado.
- No responder jamás el correo spam. Es preferible ignorarlos y/o borrarlos, ya que si se responde se confirma que la dirección de correo se encuentra activa.
- En lo posible, evitar el re-envío de mensajes en cadena (por lo general son hoax), ya que suelen ser utilizados para recolectar direcciones de correo activas.
- Si de todos modos se desea enviar mensajes en cadena, es recomendable hacerlo siempre con copia oculta (CCO) para que quien lo recibe lea solo la dirección del emisor.
- Proteger la dirección de correo utilizando una cuenta alternativa durante algún proceso de registro en sitios web y similares. Esto previene que la dirección de correo personal sea foco del spam.
- Como medida de seguridad extra, bloquear las imágenes de los correos y descargarlas cuando se asegure de que el correo no es dañino.
- Tener en cuenta que las entidades bancarias y financieras no solicitan datos confidenciales a través de este medio, de esta manera se minimiza la posibilidad de ser víctima del phishing.
- Desconfiar de los correos que dicen ser emitidos por entidades que brindan servicios y solicitan cambios de datos sensibles ya que suelen ser métodos de Ingeniería Social.
- No hacer clic sobre enlaces que aparecen en el cuerpo de los correos electrónicos, ya que pueden re direccionar hacia sitios web clonados o hacia la descarga de malware.

- Asegurarse de que la dirección del sitio web al cual se accede comience con el protocolo https. La ”s” final, significa que la página web es segura y que toda la información depositada en la misma viajará de manera cifrada.
- Verificar la existencia de un certificado digital en el sitio web. El certificado digital se despliega en pantalla al hacer clic sobre la imagen del candado
- Revisar que el certificado digital no haya caducado, ya que el mismo podría haber sido manipulado intencionalmente con fines maliciosos.
- Comunicarse telefónicamente con la compañía para descartar la posibilidad de ser víctimas de un engaño, si se tiene dudas sobre la legitimidad de un correo
- Jamás se debe enviar contraseñas, números de tarjetas de crédito u otro tipo de información sensible a través del correo electrónico, ya que la comunicación podría ser interceptada y robada.

5.2.3. Protección al navegar por la red

- Ignorar los mensajes que ofrecen material pornográfico, pues usualmente a través de ellos suele canalizarse la propagación de malware, además de otras acciones ofensivas desde el punto de vista ético y moral.
- Evitar publicar las direcciones de correo en sitios web de dudosa reputación como sitios pornográficos, foros, chats, entre otros. Esto minimiza la posibilidad de que la dirección se guarde en la base de datos de los spammers
- También es preferible que se evite ingresar el nombre de usuario y su respectiva contraseña en sitios de los cuales no se tenga referencia. De esta manera se preserva la privacidad de la cuenta de correo y, por ende, la información que se intercambia a través de la misma
- Evitar el ingreso a sitios web con contenidos que, dependiendo el país, son ilegales, como aquellos que ofrecen cracks y programas warez; ya que constituyen canales propensos a la propagación de malware.

- Configurar el navegador web para minimizar el riesgo de ataques a través del mismo.
- Si se navega desde sitios públicos, es recomendable eliminar los archivos temporales, caché, cookies, direcciones URL, contraseñas y formularios donde se haya ingresado datos.
- El bloqueo de determinados sitios considerados maliciosos, ya sea porque descargan malware o porque contienen material de dudosa reputación, es también otra de las mejores prácticas que ayudan a la prevención y refuerzan la seguridad del equipo.
- Evite la realización de transacciones bancarias en línea o la utilización de redes sociales o servicios de correo electrónico, si utiliza equipos públicos o conexiones no seguras, de este modo podrá prevenir el robo de información sensible y/o credenciales de acceso.

Es sumamente importante incorporar como hábito cotidiano las medidas de seguridad expuestas. Al bloquear las amenazas de forma temprana se reduce considerablemente la posibilidad de ser potenciales víctimas de las actividades delictivas que se llevan a cabo atentando contra la seguridad de los entornos de información. Complementar estas buenas prácticas con las herramientas de seguridad existentes, disminuirá notablemente la probabilidad de que algún ataque tenga éxito.

5.3. Identificando las amenazas

Es evidente que con la masificación en el uso del correo electrónico, se convirtió en un elemento socorrido por los cibercriminales, que con el afán de sacar ventaja sobre los usuarios, comenzaron a utilizarlo con fines maliciosos. (ESET, 2015). A como anteriormente se ha abordado se empezaron a emplear técnicas como spam, phishing, hoax, etc. para llevar sus ataques. Además aprovecharon el desconocimiento que tiene el usuario de prácticas de seguridad, al dejar los metadatos en los archivos.

Esto ha proporcionado un medio a través del cual ejecutar sus crímenes y un objeto que contiene información confidencial, lo que les facilita el éxito de un ataque o la recopilación de información. Con el objetivo de que el usuario logre identificar una amenaza, se facilitaran algunas medidas que se deben tomar para saber si realmente se está en una zona segura.

5.3.1. Identificando el SPAM

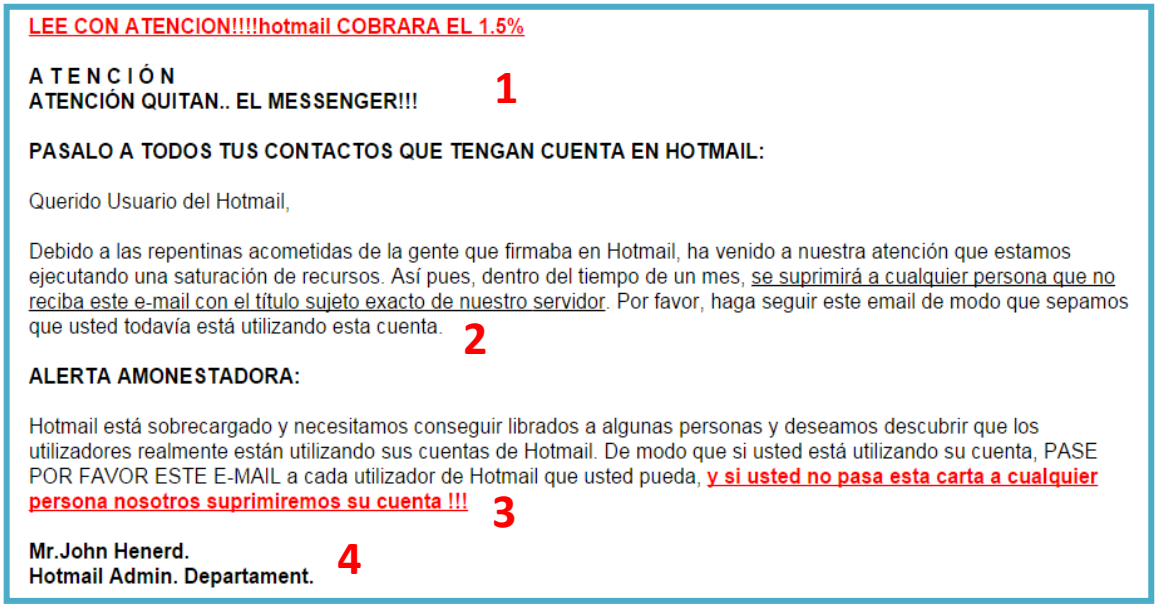
Una de las principales características del spam es el contenido de ellos, básicamente son correos que provienen de remitentes desconocidos, ofreciendo algún tipo de promoción, propaganda o servicios. Además, como son enviados masivamente, no presentan una estructura personalizada. A continuación se analizar un correo proveniente de un remitente desconocido.

Figura 9. Correo SPAM

A como se aprecia en la figura 9, el correo presenta ciertas características que lo identifican como un correo basura o spam, primeramente está el contenido en el cual se ofrece un servicio educativo [1], además al referirse al propietario del correo lo hacen con su id, nickname o usuario [2] y por último presenta un link dentro del cuerpo del correo que lo redirige a un sitio web [3].

5.3.2. Identificando el HOAX

Este tipo de correo es similar al spam, ya que es enviado masivamente y el remitente es desconocido, sin embargo su contenido lo delata, ya que está estructurado en tres partes: captar el interés, amenazar y solicitar. Procederemos a analizar un ejemplo bastante difundido en años anteriores y que posiblemente aún sigue circulando el mundo.



LEE CON ATENCION!!!!hotmail COBRARA EL 1.5%

A T E N C I Ó N
ATENCIÓN QUITAN.. EL MESSENGER!!! 1

PASALO A TODOS TUS CONTACTOS QUE TENGAN CUENTA EN HOTMAIL:

Querido Usuario del Hotmail,

Debido a las repentinas acometidas de la gente que firmaba en Hotmail, ha venido a nuestra atención que estamos ejecutando una saturación de recursos. Así pues, dentro del tiempo de un mes, se suprimirá a cualquier persona que no reciba este e-mail con el título sujeto exacto de nuestro servidor. Por favor, haga seguir este email de modo que sepamos que usted todavía está utilizando esta cuenta. 2

ALERTA AMONESTADORA:

Hotmail está sobrecargado y necesitamos conseguir librados a algunas personas y deseamos descubrir que los utilizadores realmente están utilizando sus cuentas de Hotmail. De modo que si usted está utilizando su cuenta, PASE POR FAVOR ESTE E-MAIL a cada utilizador de Hotmail que usted pueda, **y si usted no pasa esta carta a cualquier persona nosotros suprimiremos su cuenta !!!** 3

Mr.John Henerd.
Hotmail Admin. Departament. 4

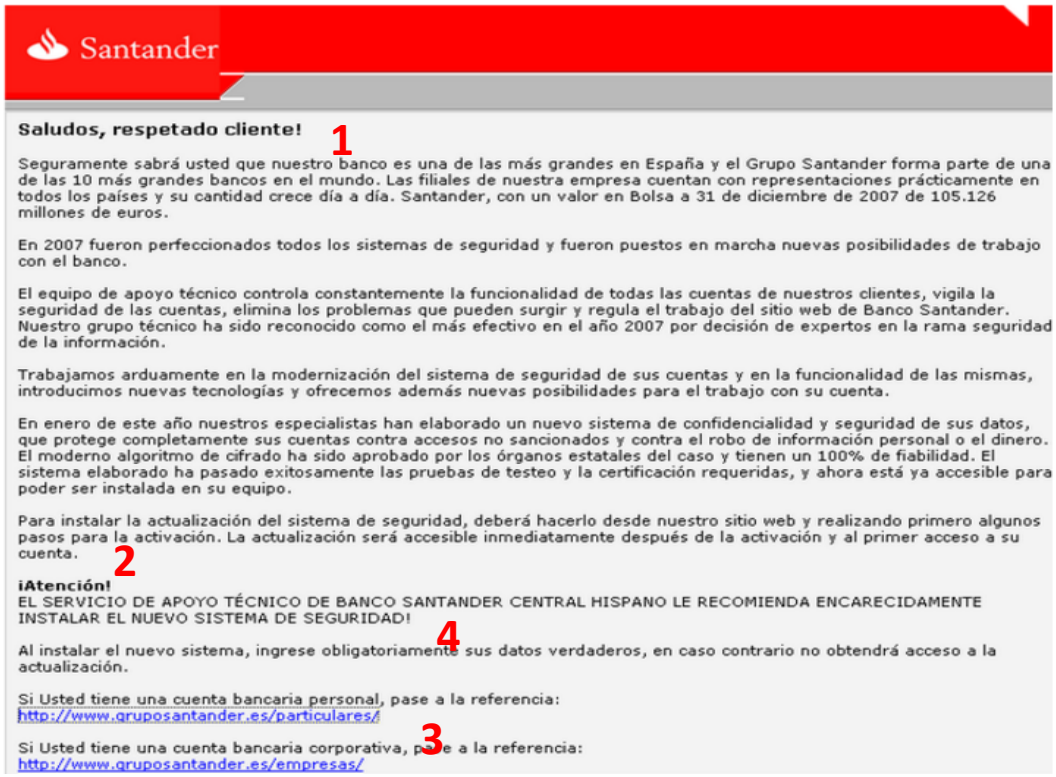
Figura 10. Correo HOAX

Antes que nada, si una noticia de este tipo fuese verdad, debería ser anunciada por otros medios y de manera oficial y más formal, y no emplear un correo mal redactado para darla a conocer. Prosiguiendo con el análisis del contenido del correo se pueden observar las tres partes que anteriormente se mencionan, primeramente se capta el interés del usuario tanto el asunto del correo

" **Atención quitan.. el Messenger!!!**", como en el principio del texto [1], Luego advierten de las consecuencias de no reenviar este correo a modo de amenaza [2] y por ultimo solicitan que se envíe el correo a lo que utilizan Hotmail o a sus contactos [3]. Para hacer el correo aún más creíble mencionan al encargado de la entidad [4].

5.3.3. Identificando el PHISHING

Este tipo de correo tiene como principal objetivo el fraude y robo de identidad. El cual aparentemente parece proceder de una empresa o persona legítima, pero no es así. La mayoría de las veces no están dirigidas de manera personal, ya que son enviados masivamente, además están diseñados muy parecidos a los correo de la compañía por la que se están haciendo pasar e incluyen enlaces que dirigen a sitios web parecidos al original. Esta amenaza consta de dos partes, las que se procederá analizar en el siguiente ejemplo.


Santander

Saludos, respetado cliente! 1

Seguramente sabrá usted que nuestro banco es una de las más grandes en España y el Grupo Santander forma parte de una de las 10 más grandes bancos en el mundo. Las filiales de nuestra empresa cuentan con representaciones prácticamente en todos los países y su cantidad crece día a día. Santander, con un valor en Bolsa a 31 de diciembre de 2007 de 105.126 millones de euros.

En 2007 fueron perfeccionados todos los sistemas de seguridad y fueron puestos en marcha nuevas posibilidades de trabajo con el banco.

El equipo de apoyo técnico controla constantemente la funcionalidad de todas las cuentas de nuestros clientes, vigila la seguridad de las cuentas, elimina los problemas que pueden surgir y regula el trabajo del sitio web de Banco Santander. Nuestro grupo técnico ha sido reconocido como el más efectivo en el año 2007 por decisión de expertos en la rama seguridad de la información.

Trabajamos arduamente en la modernización del sistema de seguridad de sus cuentas y en la funcionalidad de las mismas, introducimos nuevas tecnologías y ofrecemos además nuevas posibilidades para el trabajo con su cuenta.

En enero de este año nuestros especialistas han elaborado un nuevo sistema de confidencialidad y seguridad de sus datos, que protege completamente sus cuentas contra accesos no sancionados y contra el robo de información personal o el dinero. El moderno algoritmo de cifrado ha sido aprobado por los órganos estatales del caso y tienen un 100% de fiabilidad. El sistema elaborado ha pasado exitosamente las pruebas de testeo y la certificación requeridas, y ahora está ya accesible para poder ser instalada en su equipo.

Para instalar la actualización del sistema de seguridad, deberá hacerlo desde nuestro sitio web y realizando primero algunos pasos para la activación. La actualización será accesible inmediatamente después de la activación y al primer acceso a su cuenta. 2

¡Atención!
EL SERVICIO DE APOYO TÉCNICO DE BANCO SANTANDER CENTRAL HISPANO LE RECOMIENDA ENCARECIDAMENTE INSTALAR EL NUEVO SISTEMA DE SEGURIDAD!

Al instalar el nuevo sistema, ingrese obligatoriamente sus datos verdaderos, en caso contrario no obtendrá acceso a la actualización. 4

Si Usted tiene una cuenta bancaria personal, pase a la referencia:
http://www.gruposantander.es/particulares/

Si Usted tiene una cuenta bancaria corporativa, pase a la referencia: 3
http://www.gruposantander.es/empresas/

Figura 11. Correo PHISHING, parte 1 del ataque

Por lo general cuando las entidades bancarias envían un correo a sus clientes lo hacen de manera personalizada, no empleando palabras muy generales [1]. Este tipo de amenazas tiene la peculiaridad que solicita al usuario acceder a su cuenta para activar o realizar algún proceso a solicitud de la compañía [2], a través de los enlaces presentes en el correo que aparentemente dirigen a la dirección correcta, sin embargo son enlaces camuflados que direccionan al sitio falso diseñado por el atacante [3], además están redactados de manera tal que dan un sentido de urgencia [4]. Al momento que es recibido el correo es importante notar el dominio del que provienen, ya que en ocasiones se trata de aparentar que la dirección es legítima, sin embargo se eliminan ciertos caracteres o sustituyen por otros, con el fin de no ser percibidos como falsos, tal como xxxxxx@bancosantender.es, xxxxxx@bancosantonder.es, cuando en realidad es xxxxxx@bancosantander.es.

Si el usuario es engañado y procede a acceder al sitio web a través del enlace proporcionado en el correo, el riesgo que corre es sumamente alto. Por ello al momento de acceder a cualquier sitio, sin importar que se teclee el nombre directamente en el navegador, se deben tomar las medidas correspondientes. Para lograr identificar si un sitio web es falso, vamos analizar la siguiente parte del ataque.

Figura 12. Sitio falso - PHISHING, parte 2 del ataque

Cuando se encuentra dentro del sitio web de la entidad financiera para lograr identificar si la página es falsa, se debe realizar varias verificaciones. Por lo general el nombre del dominio es similar al original [1], en la cadena de la url debe aparecer el protocolo https, la "s" indica que la información viaja cifrada y que el sitio es seguro [2], además de ello debe verificar que el certificado sea válido y pertenezca a la entidad correspondiente, este se obtiene dando clic en el candado u hoja del sitio, al lado del https [3]. Sin embargo este procedimiento ya no es del todo seguro, debido a que se han dado caso donde se utiliza el protocolo https, para sitios web falsos. (Bortnik, 2011). Otro aspecto a tener en cuenta es la gramática [4] y la calidad de las imágenes [5] del sitio, por lo general son detalles que debido a que los atacantes no se toman el tiempo adecuado para diseñarlo, no le ponen mucho interés y como norma general nunca acceder a un sitio a través de una url proporcionada en el correo.

5.3.4. Identificando es PHARMING

El sistema operativo utiliza el archivo hosts para resolver los nombres de dominios de internet. Por lo que al momento que se quiere acceder a un sitio web, este archivo es consultado y si el dominio se encuentra registrado, el usuario es dirigido al IP relacionado. En este punto es donde esta amenaza se aprovecha, ya que su principal objetivo es modificar el hosts y asignar a dominios reales a IP falsa.

Tiene dos fases como el phishing, en la cual una de ellas es hacer una copia de algún sitio web original por medio del cual roba la información. Y la otra se analizara a continuación a través del siguiente ejemplo.

Figura 13. Correo electrónico – PHARMING

Esta amenaza para lograr sus objetivos envía correos con archivos adjuntos [1], o enlaces a sitios web donde descargar programas, imágenes, postales, entre otras. [2], además el contenido del correo es redactado para que sea llamativo, utilizando noticias, envió de postales, premios, etc. [3]. Aunque no necesariamente emplea el correo electrónico para propagarse, sino que simplemente con que el usuario descargue algún programa de internet, si este contiene el virus que modifica el host, ya puede ser víctima del phaming.

Además para identificar si ya es víctima de este ataque, lo mejor es revisar el archivo de hosts del equipo, el cual sino ha sido configurado personalmente, debe lucir como en la siguiente figura 14.

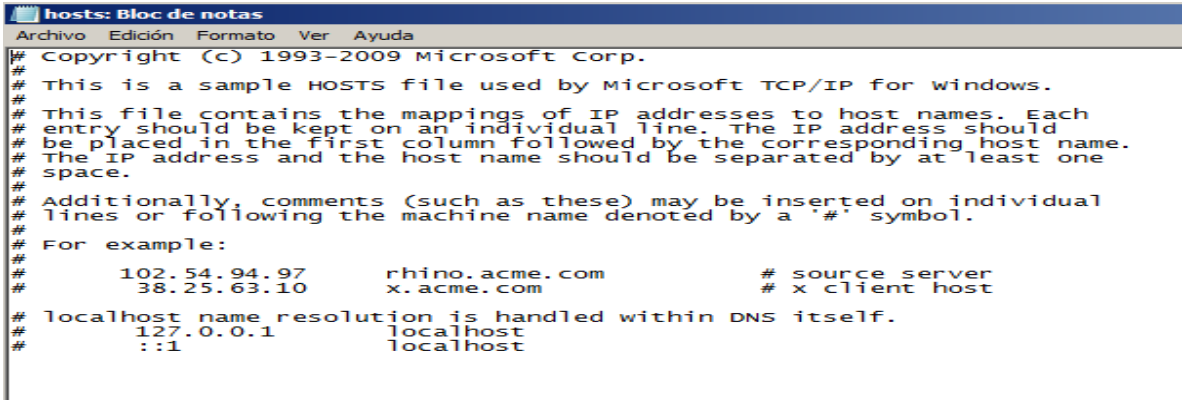


Figura 14. Archivo hosts

Si el archivo contiene alguna otra IP asociada al dominio, posiblemente haya sido modificada por un malware y el sitio al que apunta es falso [4], a como se aprecia en la figura 15.

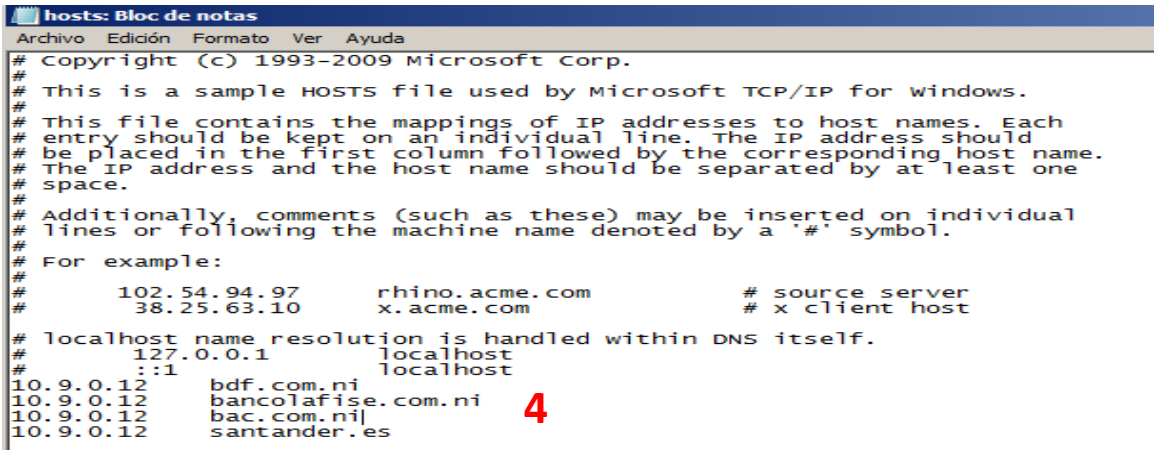


Figura 15. Archivo hosts modificado

5.3.5. Identificando un email spoffing

Este tipo de amenaza se caracteriza porque suplanta la dirección electrónica de una persona o institución legítima, haciendo creer a los usuarios que es auténtica. El proceso de identificación es un poco complicada y lo mejor es contar con herramientas que detecten este tipo de anomalías. Sin embargo a continuación se mostrara una manera para poder identificarlo.

```
Delivered-To: --
Received: --
Received: --
Return-Path: --
Received: from emkei.cz (emkei.cz. [46.167.245.118])  1
        --
Received-SPF: --
Authentication-Results: --
Received: by emkei.cz (Postfix, from userid 33)
        --
To: --
Subject: --
From: correofalso@hotmail.com  2
X-Priority: --
Importance: --
Errors-To: --
Reply-To: --
Content-Type: --
Message-Id: --
Date: --

Mensaje
```

Figura 16. Cabecera de mensajes

Cuando se recibe un correo y se tiene sospecha de la legitimidad de este, una manera para comprobar que realmente proviene de la dirección que dice ser, es verificar la cabecera del correo, los puntos importante a notar es en los campos Received by [1],, estos deben coincidir con los que aparecen en From [2], si difieren en su dominio, se está ante una suplantación de correo electrónico.

El número de técnicas y los esfuerzos de los atacantes para logar sus objetivos, ha hecho que estos lleven la ingeniería social a puntos donde un usuario sin conocimientos adecuados, fácilmente puede ser una víctima. Además, al usar los tecnológicos para propagar sus amenazas e implementar mecanismos de engaño, ya sea para robar información o infectar con malware, los vuelve aún más peligrosos. Es importante tener mucha precaución al abrir un correo o descargar algún archivo, ya que se estarían abriendo las puertas para que un delincuente haga de las suyas.

6. Impacto de los ataques

Los principales objetivos de los delincuentes es formular ataques y recolectar información con el fin de causar algún daño a los demás, ya sea económico o social.

Los delincuentes informáticos se aprovechan de las vulnerabilidades de los sistemas o desconocimiento y malas prácticas de seguridad de las personas para lograr sus objetivos, por ello el nivel de éxito que tienen es alto. A continuación se realizara un análisis del impacto que ocasionan estos ataques en el mundo y la importancia de contrarrestarlos.

6.1. Impacto económico

De acuerdo al estudio de Kaspersky Lab titulado “Ciberamenazas Financieras en 2014” reveló que el 28,73% de los ataques de phishing en 2014 tenía el propósito de robar datos financieros de los usuarios. Para llevar a cabo sus fechorías, los cibercriminales han cambiado el enfoque de ataque de las empresas financieras a los sistemas de pago y los sitios de compras online. (Kaspersky, 2015).

Sin duda alguna el porcentaje de ataques solamente de phishing es amplio, pero más alarmante son las pérdidas millonarias que este conlleva, según reporte de RSA Security, la división de seguridad de EMC Corporation, las pérdidas globales para Estados unidos es de 1,3 billones, Canadá 160 millones, Reino unido 130 millones, China 283 millones y España 64 millones en dólares (RSA, 2015). Es importante mencionar que esta amenaza no actúa sola, para lograr obtener potenciales víctimas utiliza otro tipo de elementos como spam y hoax para engañar y recolectar correos electrónicos. Además, el pharming aunque no es un phishing en su totalidad, actúa muy parecido y estas pérdidas millonarias están en cierta manera relacionadas con esta amenaza.

Estos datos presentados están relacionados solamente a transacciones electrónicas o compras en línea. Al referirnos a ataques dirigidos, no existe una formula exacta para calcular los costos, esto debido a que va a depender del tamaño de la organización y el daño que haya generado el ataque, el cual puede deberse a que se revelo información sin ninguna intención (metadatos) o porque los sistemas de seguridad son insuficientes para detener la amenaza. Según un estudio realizado por McAffe, el costo global estimado por la ciberdelincuencia es de 400 billones de dólares a nivel empresarial (McAfee, 2014).

Las pérdidas millonarias que genera la delincuencia electrónica, perjudica el rendimiento de las empresas y las economías nacionales, ya que afecta directamente el comercio, la competencia y el crecimiento económico mundial.
Este impacto económico que causan lo ataques o amenazas informáticas no solo está ligado a pérdidas financieras, sino también a las grandes inversiones que hacen las compañías en tecnología para proteger sus datos, infraestructura y comunicaciones. Según un estudio realizado por EY (Ernst & Young) , concluye que el 93% de las empresas a nivel mundial han mantenido o incrementado su inversión en seguridad cibernética para combatir la creciente amenaza de ataques. (Ernest & Young, 2013). Pero aunque las compañías continúan invirtiendo para protegerse de ataques cibernéticos, el número de fallos de seguridad aumenta, debido a que cada vez más empresas se convierten en blanco de ataque.

Así que viéndolo desde estos dos puntos de vista, tanto de ataque como de protección. Los altos niveles de inversión y las grandes sumas financieras que se pierden, afecta aún más el desarrollo de cualquier industria o nación.

6.2. Impacto social

El impacto social que ocasionan los ataques informáticos es sumamente negativo para el desarrollo de un país, ya que afecta tanto a las empresas

(pérdida efectiva de clientes, pérdida de confianza por parte clientes, pérdida de imagen corporativa o de marca) y, finalmente a la sociedad en su conjunto, ya que se frena las posibilidades de avanzar en la economía digital, en particular, y de la sociedad de la Información, en general.

Más allá de las cuantiosas pérdidas monetarias que reflejan las investigaciones anteriores, el mayor inconveniente se ve en el desarrollo de una economía basada, cada vez más en las tecnologías. Al existir esta gran cantidad de amenazas y los costos en que se incurre para contrarrestarla, resulta triste pero cierto que cerca de nueve de cada 10 adultos (86%) piensan sobre los ciberdelitos y más de un cuarto (28%) espera ser víctimas de una estafa o de un fraude online. Sólo una pequeña minoría (3%) piensa que no va a ser víctima de un ciberdelito (Symantec, 2011).

Con este pensamiento tan negativo en la sociedad, es evidente que el desarrollo digital no podrá alcanzar niveles óptimos de aceptación. La inseguridad que sienten las personas al hacer uso de medio de comunicación impide que sea recibida satisfactoriamente.

Al existir tantas amenazas involucradas en el uso de las tecnologías y comunicaciones, la confianza en los usuarios disminuye. Además, cuando una empresa es atacada, pierde imagen en el mercado, por lo tanto menos clientes confían en ella. Esto va más allá de aspectos económicos, sino que se centra en aspectos intangibles.

Aunque cada país aborda de manera distinta la seguridad, dependiendo de su panorama económico, político y cultural. Algunos países la consideran principalmente como un asunto de seguridad nacional y defensa. Otros opinan que tiene un mayor impacto en el desarrollo económico o en la competitividad internacional. Otros más la ven como un factor clave para la educación, la interacción social y la gobernanza centrada en los ciudadanos, aunque,

sabiamente, muchos países están tratando de incorporar todas estas consideraciones en sus regímenes de seguridad cibernética. (Trend Micro Incorporated, 2013). Este planteamiento es importante, ya que expresa los puntos de vista de la sociedad y da las pautas de enfoque que deben tener las naciones.

Ciertamente la sociedad se encuentra en una encrucijada, por un lado al hacer uso de las tecnologías, el desarrollo personal y profesional aumentaría, permitiría la comunicación e interacción con el mundo, fomentaría la calidad del aprendizaje y del desarrollo de destrezas de la sociedad, aumentaría la productividad económica. Sin embargo al tener estas grandes ventajas, por otro lado existen grandes riesgos, como la suplantación de identidad, extorción, robo, contrabando, proliferación de pornografía, etc. Esto ha creado en algunos individuos poca confianza en las tecnologías, por lo que evitan hacer uso de ella.

El delito informático produce un impacto económico negativo: no solo el daño directo para el que sufre o asume el ataque, sino también las pérdidas derivadas de el; ambas provocan un impacto social, que se traduce en un freno al desarrollo de la sociedad de la Información.

6.3. Importancia de contrarrestar los ataques.

Debido a las grandes pérdidas económicas y al impacto social que ocasiona un ataque informático, ya sea en las personas, compañías o nación. Es de suma importancia contrarrestarlos con el objetivo de disminuir el riesgo en lo más mínimo.

Proteger la información, la privacidad de las personas y la imagen empresarial, son uno de los principales factores a tomar en cuenta.

Aunque avanzar tecnológicamente conlleva a innumerables beneficios y mejoras, también se incurre en nuevos riesgos a los que es necesario hacer frente de una forma contundente y eficaz. Para hacer uso de las ventajas que brindan estas herramientas, es de suma importancia implementar mecanismos de seguridad, tanto en concientización, como hardware y software.

Hay que tomar muy en cuenta que los ataques son procesos muy dinámicos y variables, por lo tanto el proceso de seguridad debe ser mejor que ellos, siempre estar encaminado a la actualización permanente de mecanismos, métodos, técnicas y procedimientos que ayudan a contrarrestar los ataques o amenazas informáticas

Además, es muy importante para cada usuario mantener la disponibilidad, confidencialidad, integridad y autenticidad de los datos y transacciones. Por lo general los ataques tratan de afectar estas características, con el objetivo de obtener algún beneficio.

Al implementar mecanismos de seguridad y concientizar a los usuarios en el uso de las tecnologías, permitirá que existe una reducción en el éxito de los ataques, de esta manera se podrá trabajar y comercializar de manera más segura, disminuyendo así el temor que se tiene al hacer uso de la tecnología.

Los ataques abarcan muchos aspectos tanto económicos como sociales y afectan no solo a grandes empresas, sino también a usuarios que hacen uso de las tecnologías. Tener precaución al hacer uso de esta herramienta y tomar las medidas correctas, permitirá a los usuarios aprovechar de manera óptima los grandes beneficios que brinda.

7. Implementación de herramienta de seguridad

Hasta este punto se ha demostrado la cantidad de amenazas existentes que afecta directamente a los usuarios y organizaciones en general, en el que se hace uso de correos electrónicos y metadatos. Cuando un ataque logra tener éxito el impacto que ocasiona es sumamente alto, afectando diferentes aspectos, que van desde impacto social, económico y legal.

Para proporcionar a los usuarios además de los elementos prácticos y medidas de seguridad útiles para defenderse y que se presentaron en acápites anteriores. El actual capitulo se centrara en un análisis e implementación de un aplicativo que brindara al usuario un medio a través del cual podrá enviar y recibir correos electrónicos, los cuales serán analizados para determinar si su procedencia es maliciosa, se facilitara la administración de cuentas electrónicas para establecer dominios confiables y se realizara la eliminación de metadatos de archivos antes de que sean adjuntados, todas estas funciones serán integradas en un solo sistema, el cual realizara los procesos de manera transparente al usuario, siendo eficiente ya que no se da lugar a la intervención humano. Sin embargo es de suma importancia, fusionar tanto las herramientas de seguridad como el conocimiento del usuario.

Este capítulo contara de los siguientes puntos a desarrollar, primeramente se analizar el problema, luego los requerimientos que la aplicación debe cumplir, para posteriormente pasar al diseño e implementación y por ultimo verificar la funcionalidad.

7.1. Análisis del problema

A lo largo de la investigación se han demostrado varios problemas relacionados a la seguridad, tanto en los correos electrónicos como información oculta en archivos y desconocimiento en materia que tiene el usuario.

Esta inseguridad se debe a que no se aplican elementos o medidas de seguridad adecuados y que los delincuentes informáticos se han valido de diferentes herramientas y métodos para llevar a cabo sus ataques, los cuales tienen altos índices de éxito.

La manera en que se elaboran los ataques puede variar en muchas formas, pero se basa fundamentalmente en lo siguiente:

- Recopilar direcciones de correo electrónico, las cuales serán las potenciales víctimas.
- Investigar a la víctima para diseñar mejor el ataque o simplemente envió masivos de correos en busca de algún usuario ingenuo.
- Llevar a cabo el ataque empleando diferentes métodos de engaño, algunos de los cuales ya fueron analizados con anterioridad.
- Si la victima cae en la trampa, proporciona sus datos o archivos que contienen información oculta (metadatos).

Esto generaría una serie de problemas tanto en las personas como organizaciones, ya que habría pérdidas económicas, fraudes, suplantación de identidad, información privada, detección de vulnerabilidades, entre otros casos.

La principal debilidad es que al estar conectados en una red mundial como el internet, de una u otra manera nuestra información se encuentra en la web, ya sea porque nos registramos en foros, inscribimos en algún curso, compartimos o almacenamos archivos en la nube, etc. Aunque es una gran ventaja las facilidades que proporciona esta tecnología, es de vital importancia tomar las medidas necesarias para disminuir el riesgo de amenazas.

La amenaza se llega a materializar cuando el usuario recibe un correo electrónico. Debido a que no cuenta con las habilidades necesarias para detectar si es un ataque, fácilmente es engañado, pudiendo leer el mensaje,

respondiendo o dejándose guiar por el contenido de este. Siendo el esquema del ataque de la siguiente manera.

- La dirección del correo electrónico proviene de algún servidor que no posee los elementos de autenticidad que la acrediten como legítima, aunque es algo común que no todos los dominios tengan certificados de autenticidad. Alguno de los dominios que generan ataques, son detectados como maliciosos por diferentes entidades de seguridad, por lo tanto, el usuario no debería tener la opción de recibir estos correos.
- Al recibir el correo, el usuario por lo general no toma las medidas pertinentes para identificar la fuente o el contenido de este, así que tiende a ser una víctima potencial. En este punto responde al correo, ya sea enviando archivos adjuntos, respondiente al remitente o simplemente acceder a través de enlaces o llamar a números telefónicos presentes en el cuerpo del mensaje.
- En este punto el ataque tuvo éxito, ya que de una u otra manera el correo logro llegar a manos de la víctima. Logrando evadir los diferentes mecanismos de seguridad existentes.

Además de ello, otro punto fundamental es que los archivos que se envían de manera adjunta, ya sean imágenes, documentos ofimáticos, entre otros, contienen información privada que es oculta para el usuario. Por lo que al momento que envía información, comparte en la nube o sube archivos a alguna red social, se está poniendo en manos del que lo reciba o descargue, mayor información de la cual esta consiente el propietario del archivo. Esto surge de la siguiente manera.

- Al momento que se genera algún tipo de archivo, los sistemas le agregan datos, mejor conocidos como metadatos, los cuales sirven para agilizar ciertos procesos que los sistemas utilizan. Sin embargo, estos datos pueden ser utilizados para otros fines, ya que contienen información privada.

- Una vez que estos datos estén en manos de algún delincuente, este tiende a utilizarlo en busca de algún indicio que pueda servir para llevar a cabo un ataque o explotar alguna vulnerabilidad.
- También, nos encontramos en el caso cuando los usuarios de redes sociales o servidores en la nube suben archivos, los cuales pueden ser descargados por delincuentes, en este caso se estaría brindando un medio a través del cual el atacante puede extraer información de un determinado usuario para luego formular su ataque.

Por último, gran parte de las organizaciones no controlan las comunicaciones que establecen los usuarios a través de correos electrónicos, esto permite que exista flujo de información sin control.

- Primeramente cuando un empleado de una organización no tiene permitido extraer información a través de los diferentes medios de almacenamientos existentes, hace uso de la nube, servidores FTP o correo electrónico.
- El bloqueo de los puertos de los equipos y sitios web o programas para transferencia de archivos, es una buena solución, sin embargo bloquear el correo electrónico, no es algo que comúnmente se realice, ya que es un medio de comunicación útil. Por lo que en este caso, lo más recomendable es realizar filtros para evitar el flujo de información.

Hasta aquí se han englobado los principales problemas que esta aplicación pretende resolver. Para lo cual se hará uso de diferentes herramientas que optimicen y proporcionen altos niveles de seguridad.

7.2. Requerimientos

Para que la aplicación cumpla con las funciones para las cuales se ideo, debe cumplir ciertos requerimientos importantes que se presentan y explican a continuación.

- Bloquear o filtrar correos electrónicos procedentes de dominios maliciosos o sospechosos.

Se deben escanear las direcciones de los dominios pertenecientes al correo electrónico antes que lleguen a la bandeja de entrada, con el objetivo de bloquearlo o filtrarlo, impidiendo que el usuario tenga la posibilidad de acceder a ellos.

- Bloquear o filtrar correos electrónicos procedentes de dominios catalogados como maliciosos o no deseados por el administrador del sistema.

Detectar cuando un correo electrónico fue bloqueado por el administrador del sistema, para posteriormente bloquearlo o filtrarlo impidiendo que el usuario tenga la posibilidad de acceder a ellos.

- Bloquear él envió de correos electrónicos a direcciones con dominios maliciosos o catalogados por el administrador del sistema como no deseado.

Al momento que el usuario realice un correo electrónico, antes de que este sea enviado, la dirección del remitente será escaneada, verificando el dominio tanto con los bloqueados o permitidos por el administrador y por el proceso de detección de dominio malicioso.

- Administrar la catalogación de dominios aceptables y no deseados.

El administrador de sistema debe tener la opción de la gestión de los dominios que serán permitidos o bloqueados por la aplicación.

- Eliminar los metadatos de archivos antes de que sean adjuntados al correo electrónico.

Cuando el usuario seleccione un archivo para adjuntar, antes de que se realice esta tarea, la aplicación eliminara todos los metadatos relacionados al archivo.

7.3. Diseño del sistema

El desarrollo de la aplicación estará fundamentado en tres puntos: Escaneo de dominios maliciosos, filtro de dominios y limpieza de metadatos de los archivos.

Para lograr obtener altos rendimientos en la detección de dominios maliciosos, se hará uso del API proporcionada por Virus Total, el cual es un servicio en línea que analiza archivos y urls, habilitado para la identificación de virus, trojanos y cualquier tipo de contenido malicioso, haciendo uso de diferentes antivirus y sitios web de escaneo (VirusTotal, 2016). Por esta razón, se optó hacer uso de ella, ya que cuando se reciba un dominio este será escaneando con varios elementos de seguridad.

7.3.1. Diagrama UML – Casos de Uso

A través del análisis de las actividades referentes al sistema, se han especificado los procesos realizados por el aplicativo por medio del modelaje en UML. Los que a su vez son detallados a continuación.

7.3.1.1. Interacción de autores con el sistema

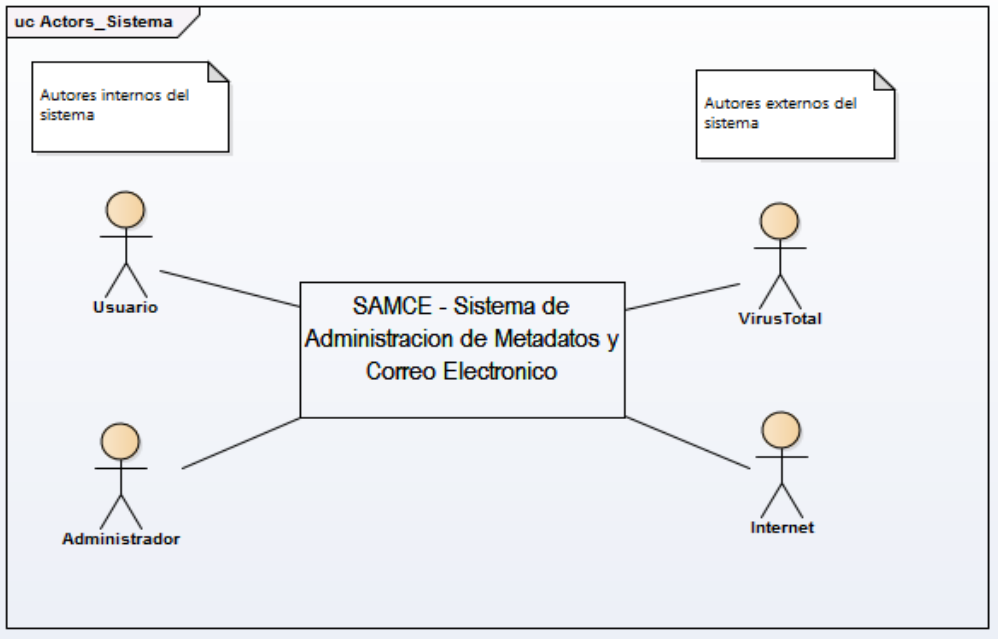


Figura 17. Interacción autores – sistema

7.3.1.2. Definición de actores involucrados

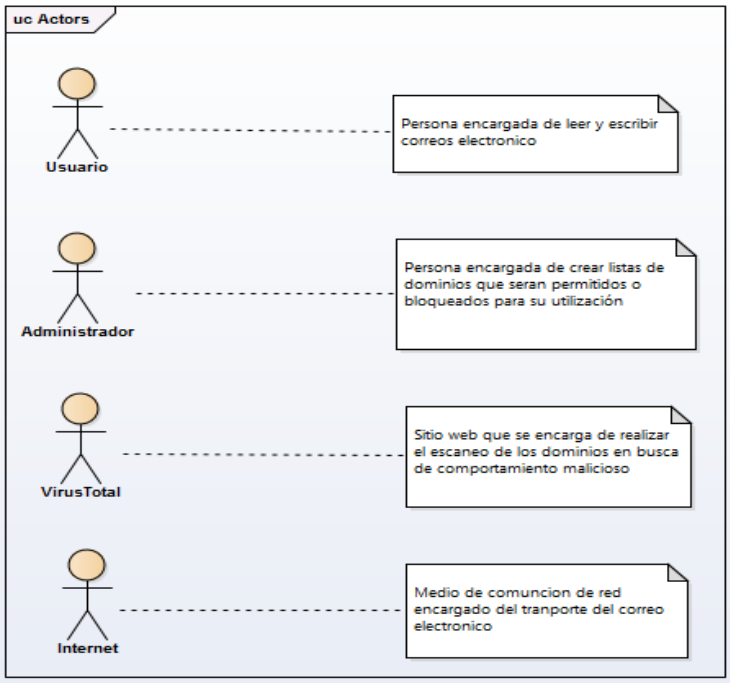


Figura 18. Definición de autores

7.3.1.3. Definición de casos de usos

Casos de usos relacionados directamente con el usuario son leer correos, recibir correos y adjuntar archivos, estas operaciones consisten tanto en la lectura como escritura de correos electrónicos y el anexo de archivos en el correo.

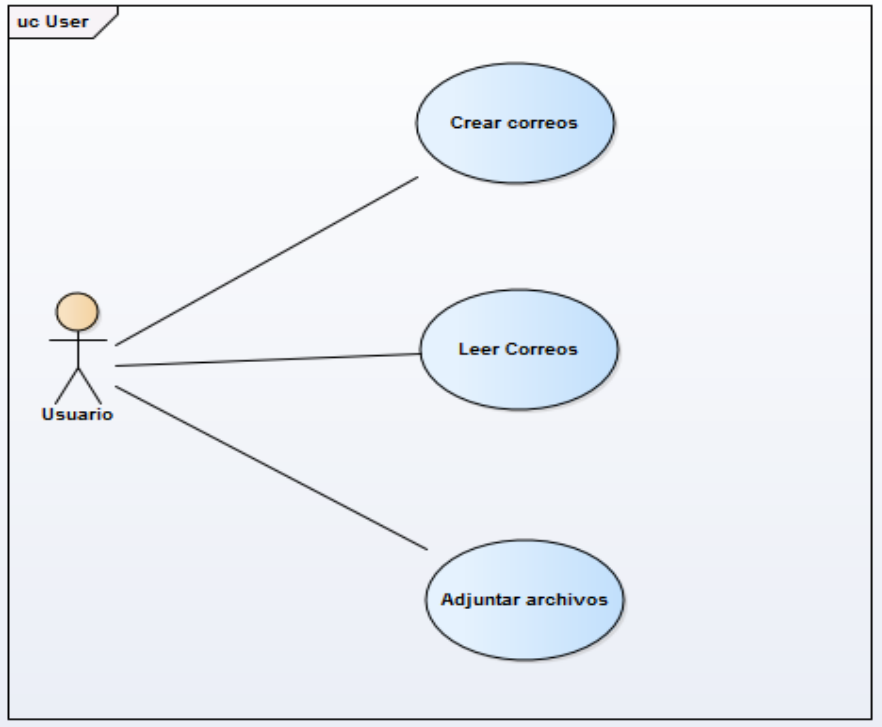


Figura 19. Caso de uso correo

Caso de uso directamente relacionado con el administrador, consiste en la gestión de los dominios. Este proceso es ejecutado cuando el administrador del sistema considere que un dominio es malicioso y debe ser bloqueado o de confianza y debe ser permitido.

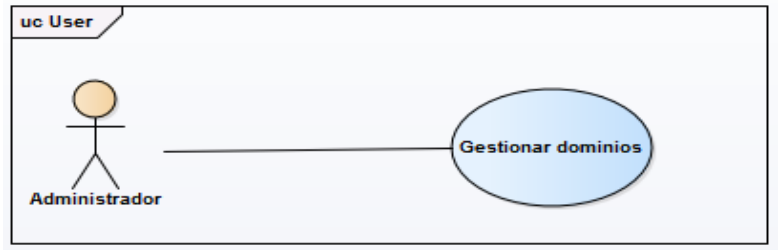


Figura 20. Caso de uso gestión de dominio

Caso de uso directamente relacionado con Virus Total, consiste el escaneo de los dominios que son utilizados en los correos electrónicos.

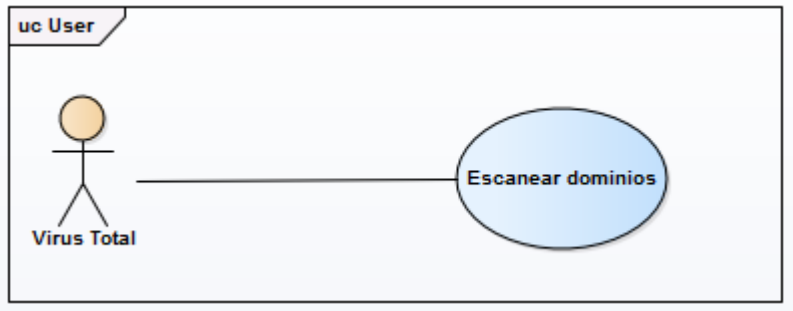


Figura 21 Caso de uso escaneo de dominio

Caso de uso directamente relacionado con Internet, este consiste en transportar, enviar o recibir los correos electrónicos realizados por el usuario.

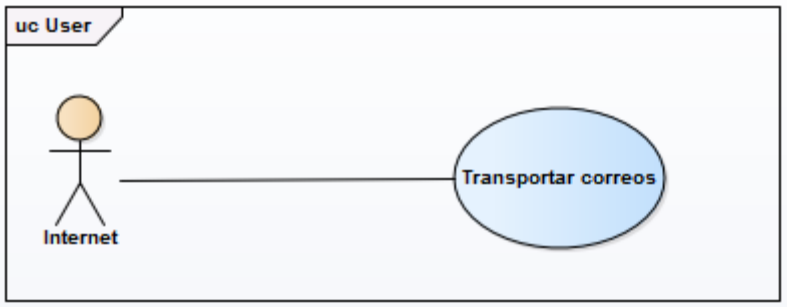


Figura 22. Caso de uso transporte

Ya detallado los casos de usos principales, pasaremos a los más específicos. Como es metadatos, que consiste en la eliminación de los metadatos de los archivos antes de que sean adjuntados al correo electrónico.

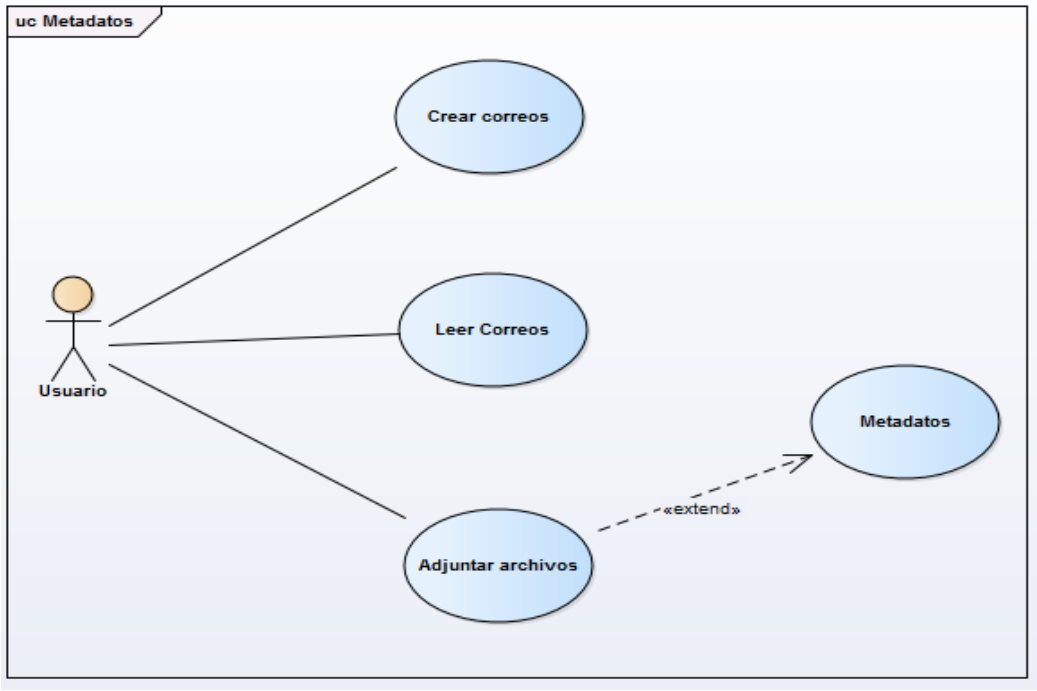


Figura 23. Caso de uso metadatos

Antes de que un correo electrónico sea enviado o recibido, existe el caso de uso validar, que se debe cumplir siempre y que se auxilia de la gestión de dominios realizada por el administrador y el escaneo de dominios proporcionado por virus total, este último no siempre se ejecuta, ya que si se tienen los registros del dominio en la gestión de dominios, ya no es necesario realizar el escaneo.

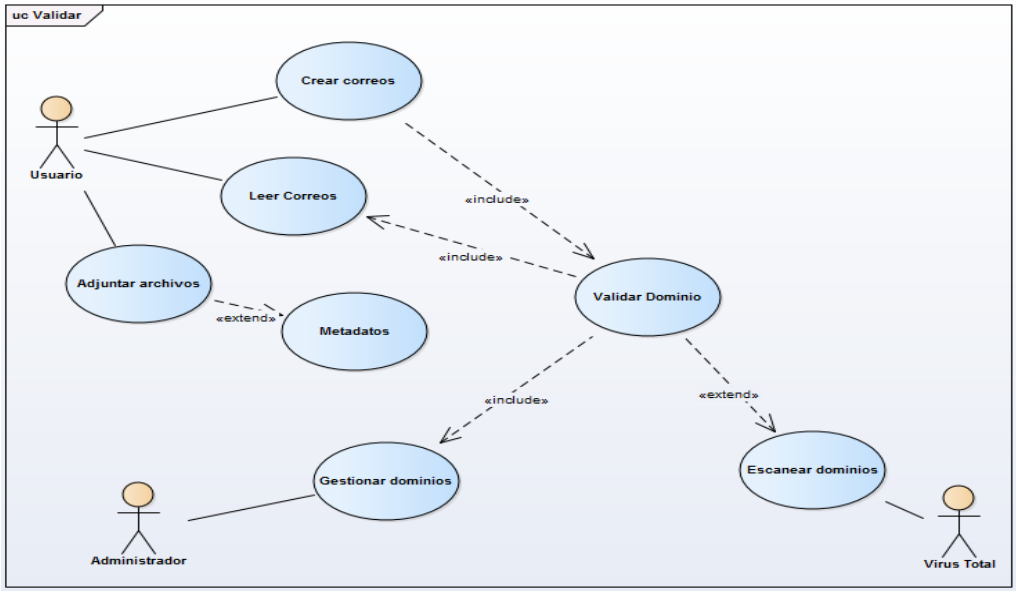


Figura 24. Caso de uso validación de dominio

A continuación se presenta el diagrama final del sistema, en el cual hay tres casos de usos más que a continuación se detallan. El primero es enviar correo, este consiste en que si la operación de validar dominio lo considera de confianza entonces, se procede a adjuntar el archivo ya limpio de metadatos y enviar el correo por medio de transportar correo, el otro caso de uso es recibir correo, este contiene un dominio, el cual debe ser evaluado por validar dominio, para determinar su confiabilidad, si todo está bien el correo pasa a leer correo, donde el usuario puede acceder a él. Sin embargo ninguno de estos casos de uso se lograrían ejecutar si validar dominio determina que la url es maliciosa, este bloqueara el correo y agregara el dominio a gestionar dominios, evitando así potenciales ataques o fuga de información.

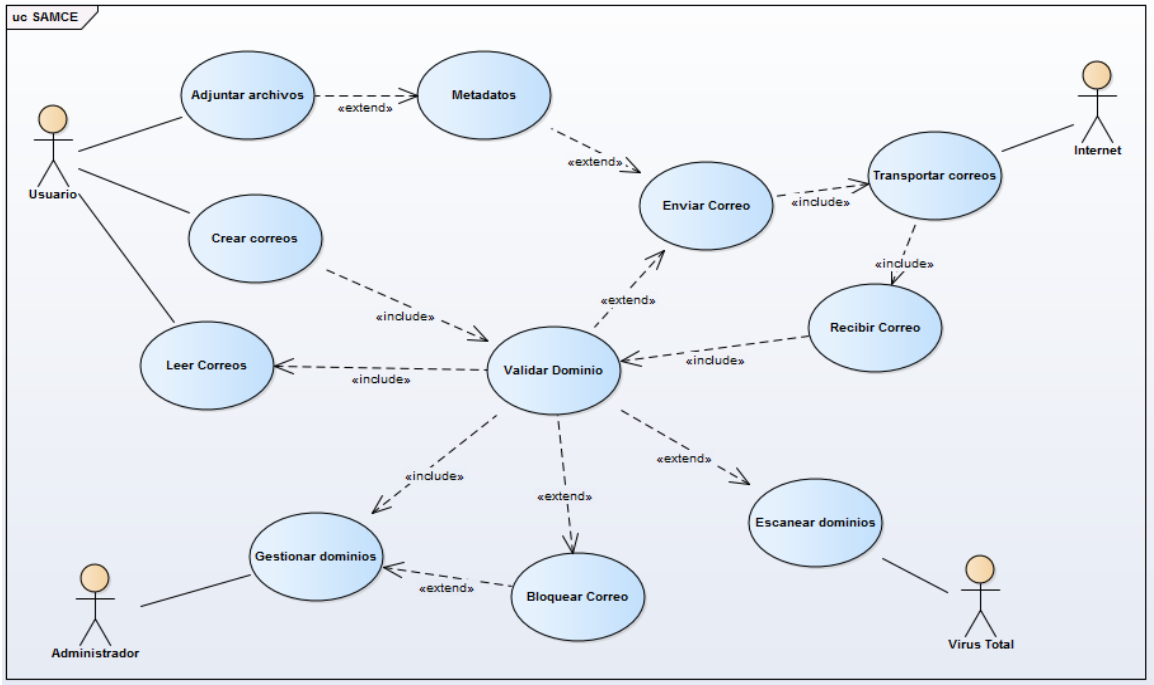


Figura 25. Caso de uso enviar, recibir y transportar correo

7.3.2. Implementación

La implementación de la aplicación fue realizada empleado el paradigma de programación orientado a objetos, haciendo uso del lenguaje java y base de

datos PostgreSQL. A continuación se presentan las diferentes funcionalidades del sistema.

7.3.2.1. Ventana de acceso a cuenta

Antes de empezar a utilizar la aplicación es necesario que se ingrese una cuenta de correo valida, la cual será sincronizada para recibir y enviar correos. Por el momento el sistema solamente soporta el servicio de correo de yahoo.

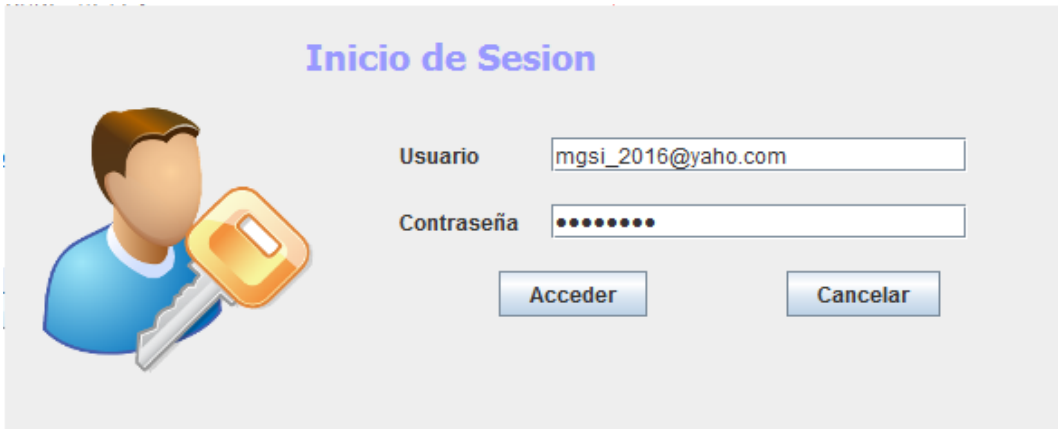


Figura 26. Ventana de inicio de sesión

7.3.2.2. Ventana principal

Una vez autenticado, la aplicación carga una ventana que contiene diferentes controles, los cuales indican los correos electrónicos de la bandeja de entrada [1], correos electrónico bloqueados [2], área de lectura del correo electrónico [3] y enlaces para crear un nuevo correo o configurar los dominios permitidos y bloqueados [4]

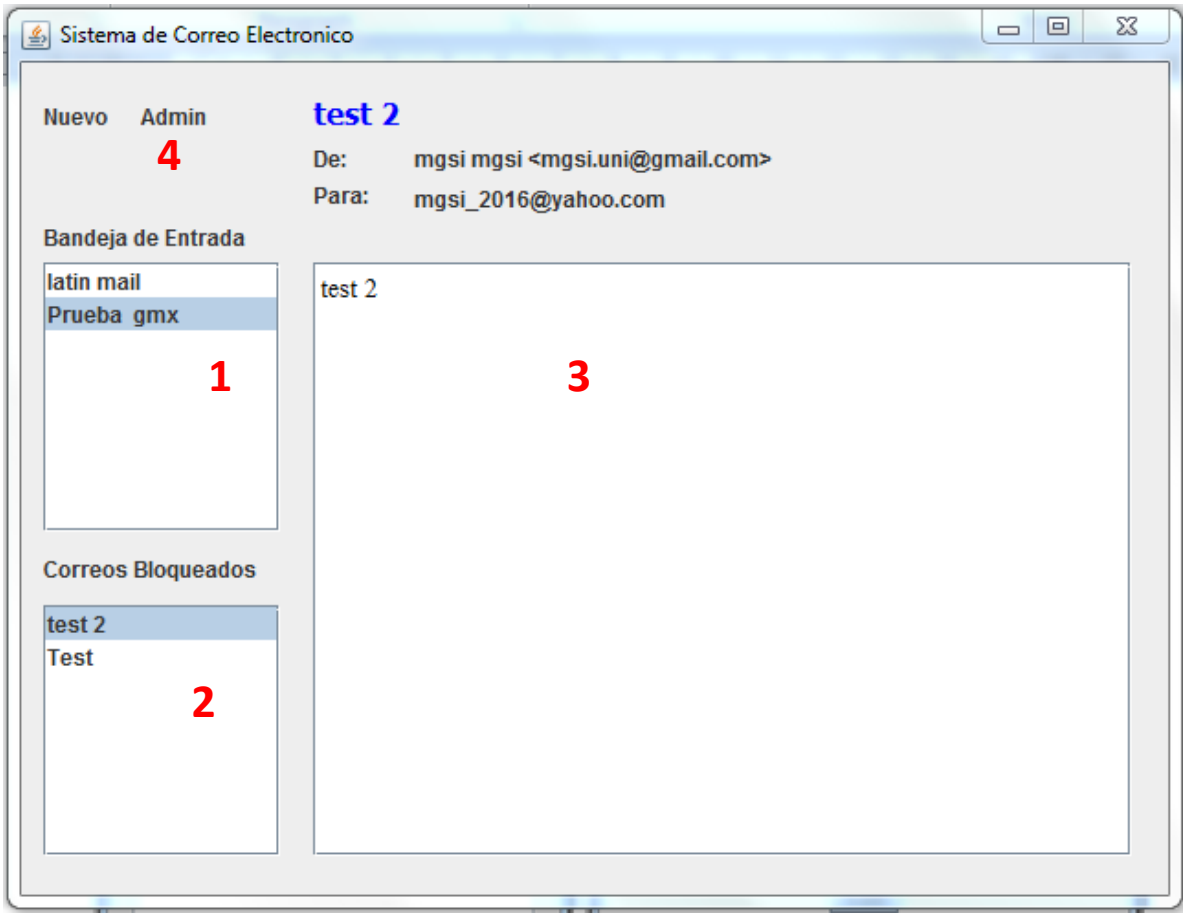


Figura 27. Ventana principal del sistema

Para lograr determinar cuándo que un correo se encuentre en la bandeja de entrada o bloqueados, se utilizaron dos elementos: Cuando el sistema empieza a descargar los correos del servidor, este realizar una comparación con la lista de dominios permitido o bloqueados, si el dominio o correo no se encuentra registrado, se procede a realizar un escaneo en Virus total para determinar la confiabilidad del dominio, en ambos caso y en dependencia de los resultados, el correo es categorizado como bloqueado o de confianza.

Aunque no es recomendable dar acceso a los usuarios cuando el dominio del correo es malicioso, solo para fines investigativos y demostrativos está siendo habilitado.

7.3.2.3. Ventana de creación de correos

Al hacer clic sobre el enlace nuevo de la ventana principal, esta acción habilita una ventana en la cual se puede crear el correo electrónico y que está conformada de la siguiente manera: en el campo “Para” se introduce la dirección del correo electrónico [1] y el asunto del correo [2]. Si se desea adjuntar algún archivo ya sea .jpg o .docx (actualmente la aplicación solo soporta estos dos formatos), se presiona el texto “adjuntar” [3], este llama a un proceso que se encarga de eliminar los metadatos del archivo seleccionado. En el momento que se presiona enviar [4], la aplicación realiza una consulta a la lista de dominios y correos permitidos y bloqueados, si la consulta no arroja nada, el sistema automáticamente realiza un escaneo empleando VirusTotal, si el correo no es considerado como maliciosos, entonces se envía, en caso contrario, se agrega a la lista de bloqueados e impide que el correo sea enviado.

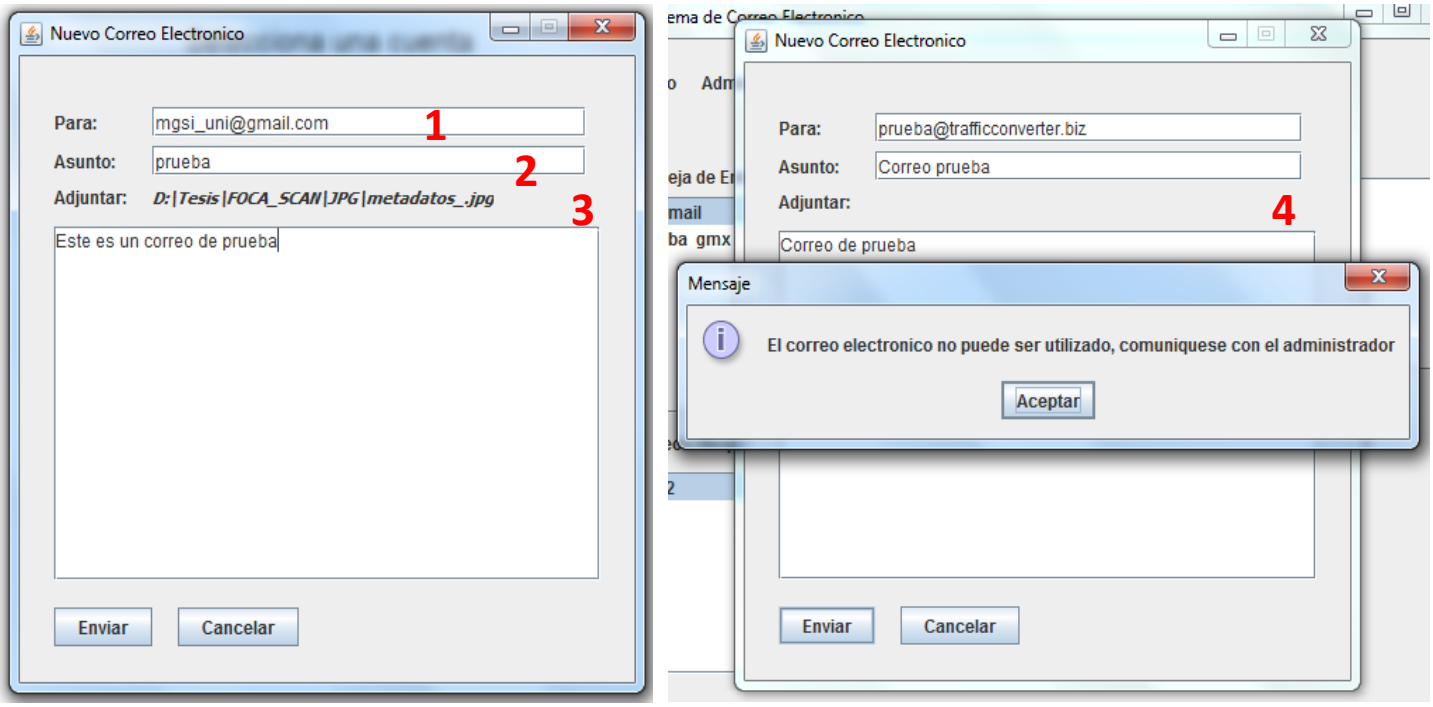


Figura 28. Venta de creación y validación de correo electrónicos

7.3.2.4. Ventana de administración de correos y dominios

La función principal de esta ventana es la administración de dominios y correos electrónicos que serán permitidos o bloqueados, donde el administrador puede agregar, editar, habilitar o deshabilitar el dominio o correo que serán parte de la lista de control de acceso. Tanto la ventana de correos como dominios son bastante similares en su estructura, por lo que se harán referencia como una sola. En el cuadro de texto [1] se ingresa el dominio o correo y empleando la lista desplegable [2] se establecerá si el campo agregado será permitido o bloqueado. Otra manera de agregar a la lista es cuando se intenta enviar un correo y virus total lo detecta como malicioso, este automáticamente lo agrega a y le asigna el estado de "Denegar" [3].

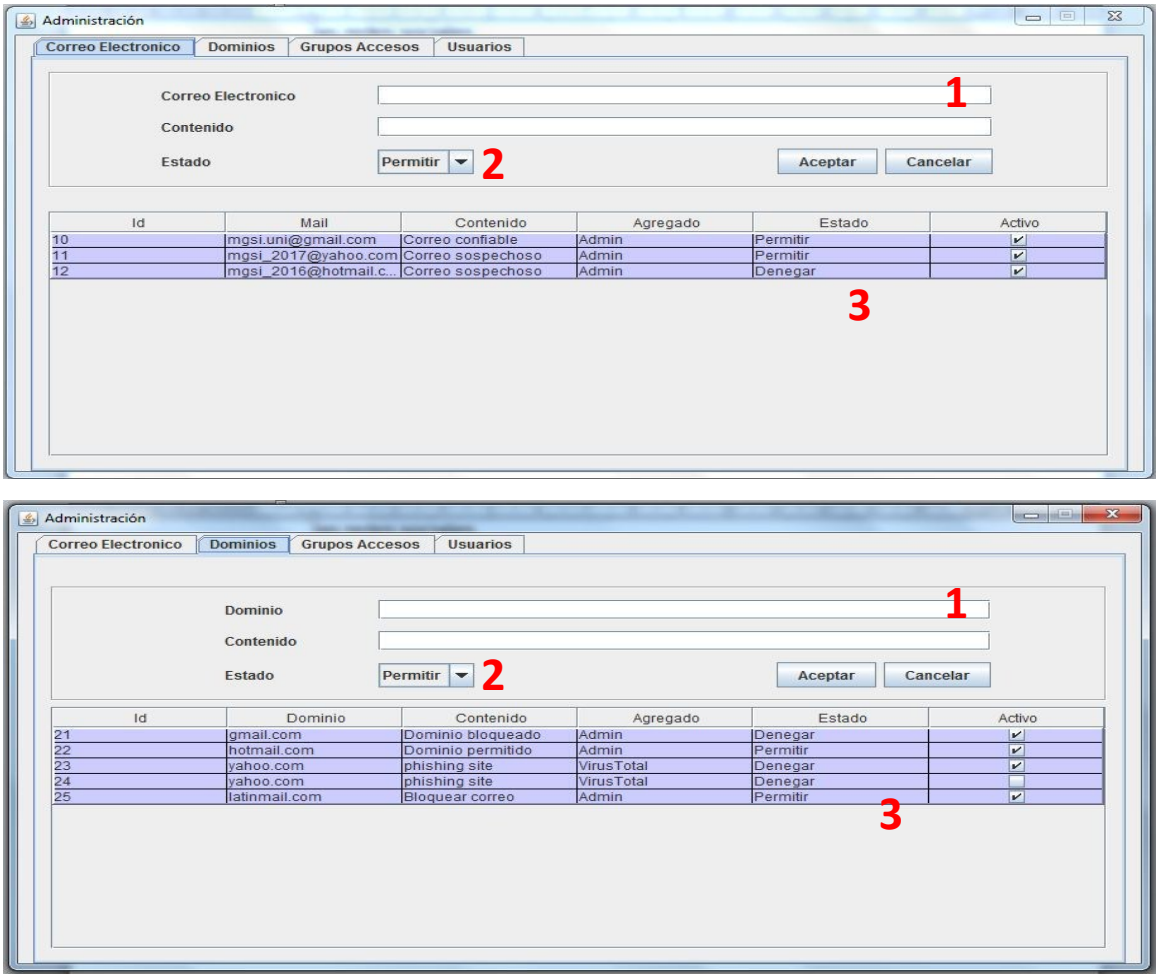


Figura 29. Administración de correos electrónicos y dominios

7.3.2.5. Ventana de lista de grupos de accesos

Una vez que se hayan creado los diferentes dominios y correos electrónicos y asignado su respectivo estado, ya sea denegado o permitido, se debe proceder a la siguiente ventana en la que se presentan cuatros listas de control de accesos, dos que son para dominios y correos electrónicos bloqueados [1] y otras dos también para dominios y correos electrónicos, pero en este caso permitidos [2]. La información disponible en cada campo, dependerá de los registros agregados previamente. Una vez que estén definidas las listas se les debe asignar un nombre, el cual contendrá la configuración realizada [3].

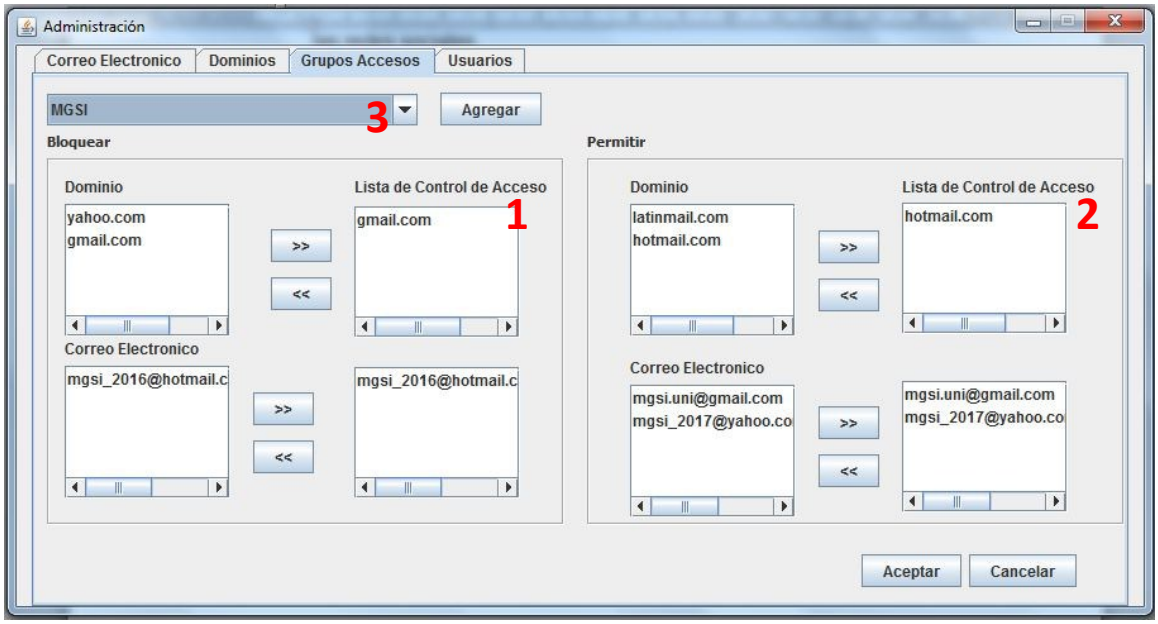
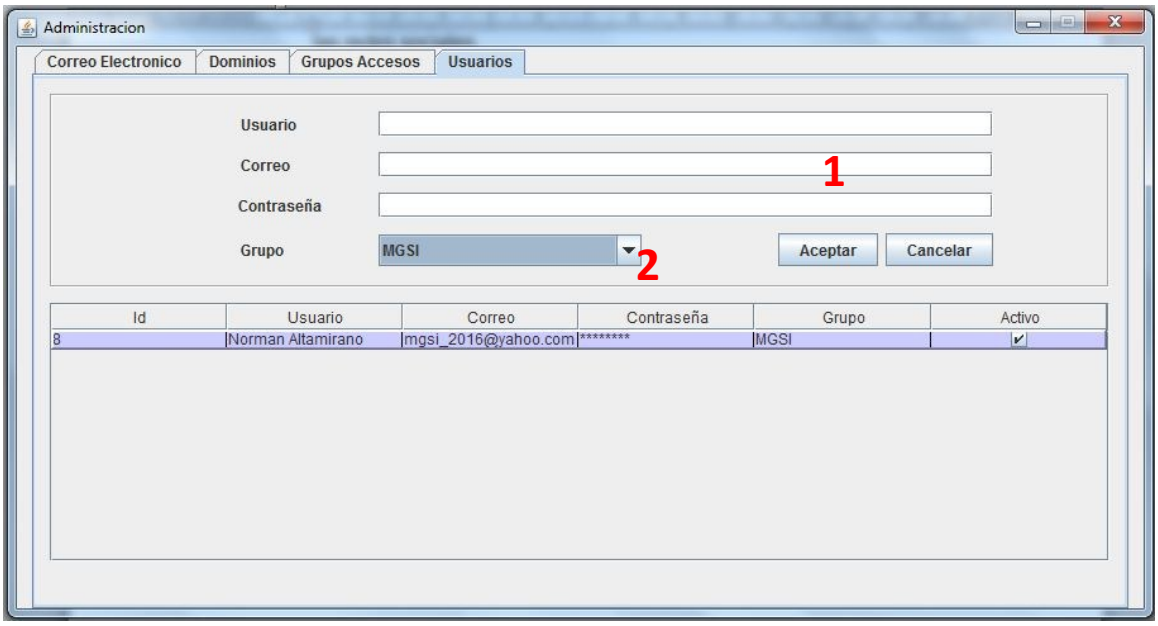


Figura 30. Listas de grupo de accesos

7.3.2.6. Ventana de usuarios

En esta ventana se crean las cuentas de usuario y se relacionan la lista de control de acceso. Una vez que se hayan agregado los datos correspondientes a la cuenta de correo del usuario [1], se debe proceder a asignarle un grupo de acceso que ha sido configurado en la ventana previa [2].



Básicamente la aplicación se basa en bloquear y permitir dominios o correos electrónicos de acuerdo a la configuración por grupos explicada, si en algún correo o dominio no se encuentra en la lista de control de accesos, el sistema hará uso del servicio externo de virus total para determinar la confiabilidad del correo o dominio, de estar todo bien se procederá ya sea a recibir o enviar correos electrónicos. Además de que todo archivo en formato .jpg o .docx que sea adjuntado, antes de ser enviado se eliminara los metadatos que contiene.

8. Conclusiones y recomendaciones

A lo largo de la presente investigación se abordaron diferentes temas relacionados a la seguridad y amenazas que afectan a las organizaciones y personas, con lo cual se ha llegado a las siguientes conclusiones:

- Para los sistemas y personas, tanto los metadatos como el correo electrónicos son muy usados en la actualidad, esto es debido a diferentes características esenciales y útiles que ayudan en gran manera a los involucrados. Pero su utilización ha ido más allá de los propósitos para los

que fueron desarrollados, llevándolo a un nivel en el que pueden ser usados para generar algún ataque tanto en el medio digital como físico.

- Los delincuentes informáticos hacen uso de herramientas especializadas y técnicas muy bien diseñadas para elaborar y llevar a cabo sus ataques, por lo que si las personas u organizaciones no toman en serio el tema de seguridad, podrían ser potenciales víctimas.
- Al ser el factor humano uno de los principales elementos que permite el éxito de un ataque, es de suma relevancia brindarle la debida capacitación y conocimiento, con el objetivo de tomar precauciones para protegerse tanto así mismo como al medio en el que se desarrolla.
- La implementación de sistemas de seguridad en las organizaciones y para uso personal son muy importantes para proteger a las personas y su información contra ataques informáticos. Contar con herramientas especializadas en este tema, brinda un medio que permite disminuir los riesgos y amenazas.
- No todos los sistemas de seguridad ofrecen un éxito en efectividad del 100%, siempre está la probabilidad de que puedan ser vulnerados, por lo que para lograr óptimos rendimientos, se debe trabajar en conjunto con el usuario común y diversos estándares de seguridad.
- El impacto social y económico que genera un ataque va a depender del tamaño de la organización, a quien va dirigido y objetivos del ataque, por tal motivo es importante poner en balanza si se asume el riesgo al no contar con elementos de protección óptimos o se invierte en materia de seguridad.
- Los diferentes elementos para protegerse contra un ataque proporcionados en esta investigación, permite a las personas u organizaciones disminuir el riesgo de éxito de alguna amenaza, pudiendo ser usados a diario o implementarlos como políticas de buenas prácticas en materia de seguridad. Además, se han demostrado de manera general como un atacante recopila información y genera ataques. Esto da como resultado un documento que permitirá al usuario ampliar sus conocimientos respecto al tema.

- La herramienta desarrollada proporciona al usuario una mayor confianza y seguridad al momento de enviar o recibir correos, ya que un análisis previo del correo determina que tan confiable es. También permite la eliminación de metadatos de los archivos adjuntos, dando así un elemento extra que evita que haya mayor flujo de información.
- Además de ser una aplicación orientada a la seguridad, trabaja de manera transparente al usuario, por lo que las personas que hagan uso de ella no deben realizar ningún proceso adicional, limitando así la intervención del factor humano.
- El contar con esta aplicación que evita enviar o recibir correos de dominios maliciosos o catalogados como bloqueados, permitirá que las personas envíen correos a destinos de confianza e impedirá recibir correos sospechosos, disminuyendo así ser víctimas de algún ataque.
- Al eliminar los metadatos de los archivos, se tendrá la plena seguridad de que la información que se está enviando es solamente la contenida dentro del archivo y no se proporcionarían datos adicionales que permitirían descubrir vulnerabilidades o tener un mayor conocimiento de los diferentes elementos encontrados en los metadatos.

Es importante tener presente que la tecnología está avanzando muy rápidamente, de igual manera los delincuentes informáticos lo hacen, por lo que se debe estar pendiente de las nuevas amenazas que surjan y de los diferentes elementos de seguridad que se desarrollan.

Por lo tanto para estar preparados y protegidos contra las diferentes amenazas que día a día surgen, se recomienda lo siguiente:

- Implementar las diferentes medidas de seguridad para contrarrestar un ataque que fueron proporcionadas en este documento, además de analizar cuales se adaptan mejor al ambiente de trabajo.

- Analizar otras medidas de seguridad que mejor se ajusten al perfil y elementos (hardware, software, giro de negocio, etc) que se desea proteger.
- Utilizar herramientas de seguridad, tal como filtros de contenido, antivirus, firewall, IDS, IPS, antispyware, etc.
- Utilizar herramientas para eliminar los metadatos de los archivos antes de que sean subidos a la web, enviados por correo electrónico, almacenados en la nube o agregados en alguna red social.
- Capacitar a las personas en el uso correcto de los medios informáticos y crear la cultura de siempre estar alerta ante cualquier amenaza.
- Utilizar la herramienta desarrollada para enviar y recibir correos electrónicos.

Como parte de la mejora continua y planes a futuro, se pretende realizar lo siguiente:

- Seguir desarrollando la aplicación para que soporte diferentes servidores de correo, tanto comerciales como corporativos. Además de la eliminación de metadatos de los diversos archivos existentes, tal como mp3, pdf, xlsx, etc.
- Adaptar la aplicación a los diferentes clientes de correo existentes, brindando las funcionalidades de seguridad, sin la necesidad de cambiar de software.
- Incorporar nuevas funcionalidades de seguridad, como el análisis del contenido, escaneo de imágenes en el cuerpo del mensaje, etc.
- Llevar el análisis de dominios y eliminación de metadatos no solo al correo electrónico, sino también a la web. Eliminando la información oculta antes de publicarla, analizar la dirección web antes de que cargue el sitio, etc.

9. Citas y referencias Bibliográficas

Baca, M. (1999). Introducción a los metadatos. Los Angeles, Calif.: J. Paul Getty Trust.

Caplan, P. (1995) *"You Call It Corn, We Call It Syntax-Independent Metadata for Document-Like Objects." The Public-Access Computer Systems Review 6, no. 4 (1995)*. Recuperado de http://xml.coverpages.org/caplan.html

Pérez, I. (2014). *Metadatos: tus fotos podrían mostrar más de lo que ves.* Recuperado de http://www.welivesecurity.com/la-es/2014/05/13/metadatos-fotos-podrian-mostrar-mas/

Lamarca, M. (2013). *Metadatos*. Recuperado de http://www.hipertexto.info/documentos/metadatos.htm

Molist, M. (2003). *Microsoft Word pone en ridículo al gobierno británico.* Recuperado de http://www.vsantivirus.com/mm-word-blair.htm

Meyssan, T. (2003). *Tony Blair confiesa lo falso del informe británico contra Irak.* Recuperado de http://www.voltairenet.org/article120014.html

Symantec Security Response. (2012*). Flamer: Highly Sophisticated and Discreet Threat Targets the Middle East*. Recuperado de http://www.symantec.com/connect/blogs/flamer-highly-sophisticated-and-discreet-threat-targets-middle-east

Pacheco, F., Jara, H. (2009) *Ethical Hacking 2.0: Implementación de un sistema para la gestión de la seguridad*. Buenos Aires, Argentina: Fox Andina

Elevenpaths*. Soluciones preventivas contra la fuga de información sensible.* Recuperado de https://www.elevenpaths.com/es/tecnologia/metashield/index.html

Microsoft Support. *Inspect documents for hidden data and personal information*. Recuperado de https://support.office.com/en-in/article/Inspect-documents-for-hidden-data-and-personal-information-85951777-89dd-45dd-960a-fc979414e8fc

THE RADICATI GROUP, INC. (2013). *Email statistics reports, 2013-2017*. Recuperado de http://www.radicati.com/wp/wp-content/uploads/2013/04/Email-Statistics-Report-2013-2017-Executive-Summary.pdf

Universidad de Jaén. (2013). *Guía de seguridad de UJA 4, seguridad en el correo electrónico*. Recuperado de https://www10.ujaen.es/sites/default/files/users/sinformatica/guiaspracticas/Guias%20de%20seguridad%20UJA%20-%204.%20Seguridad%20en%20el%20correo%20electronico.pdf

Delgado, A. (2013). *El eslabón más débil de la cadena en seguridad es el usuario.* Recuperado de https://revistaitnow.com/el-eslabon-mas-debil-de-la-cadena-en-seguridad-es-el-usuario/

Arroyo, M. (2014). *El eslabón más débil de la cadena de seguridad*. Recuperado de http://cordopolis.es/estas-seguro-de-que-estas-seguro/2014/02/28/el-eslabon-mas-debil-de-la-cadena-de-seguridad/

Vásquez, C. METADATOS: *Introducción e historia*. Recuperado de http://users.dcc.uchile.cl/~cvasquez/introehistoria.pdf

Lamarca, M. (2013). *El nuevo papel de las bibliotecas*. Recuperado de http://www.hipertexto.info/documentos/papel.htm

Miller, P. (1996). Metadata for the Masses. Recuperado de http://www.ariadne.ac.uk/issue5/metadata-masses/

Pérez, N. (2006). De la descripción bibliográfica a la asignación de metadatos: un llamado al orden. Recuperado de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1024-94352006000600012

Taylor A. (1999). *Organization of information.* Englewood: Libraries Unlimited.

Stevez, S. (2013). *METADATOS. QUE SON Y PARA QUE SIRVEN. PELIGROS*. Recuperado de https://santiagoestevez.wordpress.com/2013/09/13/metadatos-que-son-y-para-que-sirven-peligros/

DublinCore. (2013). *Dublin Core Metadata Element Set, Version 1.1.* Recuperado de http://dublincore.org/documents/dces/

Eito, R. (2011). *METS: introducción y tutorial*. Recuperado de http://www.loc.gov/standards/mets/METSOverview_spa.html

MODS. (2014). *MODS: Uses and Features.* Recuperado de http://www.loc.gov/standards/mods/mods-overview.html

EAD. (2012). *Design Principles.* Recuperado de http://www.loc.gov/ead/eaddesgn.html

TEI. (2015). *P5: Guidelines for Electronic Text Encoding and Interchange.* Recuperado de http://www.tei-c.org/release/doc/tei-p5-doc/en/html/ST.html#STIN

Barry & Associates, inc*. Universal Data Element Framework (UDEF).* Recuperado de http://www.servicearchitecture.com/articles/xml/universal_data_element_framework_udef.html

MPEG. *Standards.* Recuperado de http://mpeg.chiariglione.org/standards/

W3C. (2013). *W3C SEMANTIC WEB ACTIVITY*. Recuperado de http://www.w3.org/2001/sw/

Eleven Paths. (2015*). Foca.* Recuperado de https://www.elevenpaths.com/es/labstools/foca-2/index.html

Sanko. (2013). *Grampus Project - Presentación detallada.* Recuperado de http://www.sniferl4bs.com/2013/01/grampus-project-presentacion-detallada.html

Google. *Metagoofil.* Recuperado de https://code.google.com/p/metagoofil/

Matthias. (2015*). Exif Jpeg header manipulation tool.* Recuperado de http://www.sentex.net/~mwandel/jhead/

Mamani, D. (2013). *Fases de un Ataque Hacker.* Recuperado de http://www.revistasbolivianas.org.bo/pdf/rits/n8/n8a29.pdf

Bautista, H. (2013). *Problemas de seguridad al no eliminar los metadatos*. Recuperado de http://rootear.com/seguridad/problemas-seguridad-metadatos

Everstine B. (2015). *Carlisle: Air Force intel uses ISIS 'moron's' social media posts to target airstrikes.* Recuperado de http://www.airforcetimes.com/story/military/tech/2015/06/04/air-force-isis-social-media-target/28473723/

Maligno. (2012). *John McAfee: La huida y los metadatos de un iPhone 4S.* Recuperado de http://www.elladodelmal.com/2012/12/john-mcaffe-la-huida-y-los-metadatos-de.html

Zafra, I. (2012). *La policía acredita 200.000 euros ilegales en la campaña de Camps en 2007.* Recuperado de http://ccaa.elpais.com/ccaa/2012/06/11/valencia/1339444907_683693.html

Salaberry, A. (2012*). TGIF: Hacker acusado gracias a fotos de los pechos de su novia*. Recuperado de http://hipertextual.com/2012/04/tgif-hacker-acusado-gracias-a-fotos-pechos-su-novia

ITProPortal (2010). *Designer arrested over Anonymous press reléase*.

Recuperado de http://www.itproportal.com/2010/12/15/designer-arrested-over-anonymous-press-release/

THE RADICATI GROUP, INC. (2013). *Email statistics reports, 2013-2017.* Recuperado de http://www.radicati.com/wp/wp-content/uploads/2013/04/Email-Statistics-Report-2013-2017-Executive-Summary.pdf

McAfee. (2015*). Informe de McAfee Labs sobre amenazas.* Recuperado de http://www.mcafee.com/es/resources/reports/rp-quarterly-threat-q1-2015.pdf

Berrio, j. *Hacking en 5 pasos usando Software libre*. Recuperado de http://www.dsteamseguridad.com/archivos/barcamp/BARCAMP2.pdf

Universidad de Jaén. (2013). *Guía de seguridad de UJA 4, seguridad en el correo electrónico.* Recuperado de https://www10.ujaen.es/sites/default/files/users/sinformatica/guiaspracticas/Guias%20de%20seguridad%20UJA%20-%204.%20Seguridad%20en%20el%20correo%20electronico.pdf

Panda. *Spam*. Recuperado de http://www.pandasecurity.com/spain/homeusers/security-info/cybercrime/spam/

ESET. (2011). *Tendencias 2011: las botnet y el malware dinámico*. Recuperado de http://www.eset-la.com/pdf/prensa/informe/tendencias_2011_las_botnet_y_el_malware_dinamico.pdf

CYREN. (2015).*CYBERTHREAT Report.* Recuperado de https://www.cyren.com/tl_files/downloads/CYREN_Q3_2015_CyberThreat_Report.pdf

Panda. *Otras amenazas de Cibercrimen: redes de Bots y scams.* Recuperado de http://www.pandasecurity.com/spain/homeusers/security-info/cybercrime/others/

SANS. (2011*).Phishing y Scams en el Correo Electrónico*. Recuperado de https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201112_sp.pdf

Arias, A. (2014). *Las Estafas Digitales.*

Panda. (2004).*Hoaxes* informáticos: un peligro fácilmente evitable. Recuperado de http://www.pandasecurity.com/about/press/viewnews.htm?noticia=5165&entorno=&ver=&pagina=&producto

Aguilera, L. (2010). *Seguridad informática*. Pozuelo de Alarcón, Madrid: Editex

Medina, M. (2014). *Tipos de delitos informáticos.* Recuperado de http://www.elchedetectives.com/tipos-de-delitos-informaticos/

Gallego, J. (2014). *Operaciones Auxiliares Para La Configuración y La Explotación.* Pozuelo de Alarcón, Madrid: Editex

ESET. (2009). *Buenas prácticas de seguridad informática.* Recuperado de http://www.welivesecurity.com/wp-content/uploads/2014/01/buenas_practicas_seguridad_informatica.pdf

Pérez, I. (2014). *Las técnicas de Ingeniería Social evolucionaron, ¡presta atención!.* Recuperado de http://www.welivesecurity.com/la-es/2014/05/21/tecnicas-ingenieria-social-evolucionaron-presta-atencion/

Kaspersky. *¿Qué es un filtro web?.* Recuperado de http://latam.kaspersky.com/mx/internet-security-center/definitions/web-filter

Panda. (2010). *Evite la navegación por páginas con contenidos indeseados y potencialmente peligrosos.* Recuperado de http://www.pandasecurity.com/nicaragua/enterprise/solutions/security-appliances/web-filter.htm

Kaspersky. (2016). *Kaspersky.* Recuperado de http://usa.kaspersky.com/store/kaspersky-store

Ponemon Institute LLC. (2015). *2015 State of the Endpoint Report: User-Centric Risk*. Recuperado de https://www.lumension.com/Lumension/media/graphics/Resources/2015-state-of-the-endpoint/2015-State-of-the-Endpoint-Whitepaper-Lumension.pdf

SEGOB. (2015). *Participa comisión nacional de seguridad en coloquio sobre seguridad cibernética en Washington.* Recuperado de http://ssp.gob.mx/portalWebApp/appmanager/portal/desk;jsessionid=MJt2WnDbfGnkJGX7yLyvynpWLWQ9wpM8vdLKvY1CQMcn28Jy1bxn!-1603502763?_nfpb=true&_windowLabel=portlet_1_1&portlet_1_1_actionOverride=%2Fboletines%2FDetalleBoletin&portlet_1_1id=1396387

ESET. (2015). *Las amenazas frecuentes en correo electrónico y cómo han cambiado.* Recuperado de http://www.welivesecurity.com/la-es/2015/10/09/amenazas-frecuentes-correo-electronico/

Bortnik, S. (2011). *Phishing por HTTPS: del pronóstico a la realidad.* Recuperado de http://www.welivesecurity.com/la-es/2011/09/21/phishing-https-pronostico-realidad/

Kaspersky. (2015). *Kaspersky Lab: el 28,8% de los ataques phishing de 2014 buscó robar datos financieros.* Recuperado de https://securelist.com/files/2015/02/KSN_Financial_Threats_Report_2014_eng.pdf

RSA. (2015).*Total global losses from phishing attack*. Recuperado de http://www.emc.com/microsites/rsa/phishing/index.htm

McAfee. (2014). *Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II.* Recuperado de http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

Symantec. (2011). *Informe de sobre los Ciberdelitos: el Impacto Humano.* Recuperado de http://www.symantec.com/content/en/us/home_homeoffice/media/pdf/cybercrime_report/Norton_Spanish-Human%20Impact-A4_Aug11.pdf

Ernest & Young. (2013). *Under cyber attack EY's Global Information Security Survey 2013*. Recuperado de http://www.ey.com/Publication/vwLUAssets/EY_-_2013_Global_Information_Security_Survey/$FILE/EY-GISS-Under-cyber-attack.pdf

Trend Micro incorporated. (2013). *Tendencias en la seguridad cibernética en América Latina y el Caribe y respuestas de los gobiernos*. Recuperado de http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-tendencias-en-la-seguridad-cibernetica-en-america-latina-y-el-caribe-y-respuestas-de-los-gobiernos.pdf

VirusTotal (2016). *About Virus Total.* Recuperado de https://www.virustotal.com/es/about/

10. Glosario de Términos

- Nube: Conocida también como servicios en la nube o informática en la nube, es un paradigma que permite ofrecer servicios de computación a través de una red, que usualmente es Internet.
- Web Semántica: Es una ampliación de la Web, por medio de la que se intenta realizar un filtrado de manera automática pero precisa de la información
- Selfie: es un autorretrato realizado con una cámara fotográfica, típicamente una cámara digital o teléfono móvil, bastante relacionada a las redes sociales.
- Malware: Código maligno, software malicioso o software malintencionado, que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario.
- Blog: Sitio web que incluye, a modo de diario personal de su autor o autores, contenidos de su interés, actualizados con frecuencia y a menudo comentados por los lectores.
- GPS: Sistema de posicionamiento global que permite determinar en todo el mundo la posición de un objeto con una precisión de hasta centímetros
- Topología de red: Es el mapa físico o lógico de una red para intercambiar datos. En otras palabras, es la forma en que está diseñada la red, sea en el plano físico o lógico.