Universidad del Azuay

Facultad de Ciencias de la Administración

Escuela de Ingeniería de Sistemas y Telemática

DIAGNÓSTICO DE VULNERABILIDADES DE INFORMACIÓN EN DOCUMENTOS PÚBLICOS DE ENTIDADES DEL SECTOR PÚBLICO DE LA CIUDAD DE CUENCA

Trabajo de graduación previo a la obtención del Título de Ingeniero en Sistemas y Telemática

Autor:

Christian Flores Terreros.

Director:

Ing. Pablo Pintado Zumba.

Cuenca – Ecuador

2018

DEDICATORIA

Este trabajo de tesis va dedicado a mis padres que son las personas que me apoyaron durante todo mi camino universitario y sin su apoyo no hubiera alcanzado este objetivo en mi vida.

AGRADECIMIENTO

Quiero brindar un especial agradecimiento a mi director de tesis el Ing. Pablo Pintado Zumba por ser la persona que confió en mi para realizar esta tesis de grado

A toda mi familia por su apoyo.

Al PhD Francisco Salgado, quien me brindo apoyo en la investigación del tema.

RESUMEN:

"Azuay, al ser la cuarta provincia con mayor uso de Tics en el país, acrecienta el número de posibles vectores para ataques cibernéticos a las entidades estatales. El objetivo de esta investigación es evaluar el nivel de obtención de información privilegiada de documentos públicos de entidades estatales de Cuenca. Se realizó un análisis de 6 empresas del sector público de Cuenca. Los métodos de acceso a los metadatos son considerados legales por la legislación ecuatoriana. Los resultados fueron la obtención de 1.041 documentos con metadatos, relacionados con 159 equipos y 184 usuarios. Se comprobó que el 100% de los documentos analizados contenían información privilegiada y son vulnerables a ataques cibernéticos. Estos resultados alientan a la aplicación de buenas prácticas de seguridad de la información."

Palabras clave: fuga de datos, documentos informáticos, documentos públicos, información privilegiada

ABSTRACT

As Azuay was the fourth province with the highest use of ICTs in the country, it increased the number of possible vectors for cyber attacks to state entities. The objective of this investigation was to evaluate the level of obtaining privileged information from public documents of state entities of Cuenca. An analysis was made of 6 companies of the public sector. The methods of access to metadata are considered legal by Ecuadorian law. The results were the obtainment of 1,041 documents with metadata, related to 159 teams and 184 users. It was found that 100% of the analyzed documents contained privileged information and were vulnerable to cyber attacks. These results encourage the application of good information security practices.

Keywords: Data leak, electronic documents, public documents, privileged information.

UNIVERSIDAD DEL AZUAY
Dpto. Idiomas

Translated by

Ing. Paul Arpi

ÍNDICE

Índice de contenido

Índice de tablas y figuras

Tablas

Figuras

CAPÍTULO 1
1. LAS TICS EN EL PAÍS

Introducción

Para comprender de mejor manera este trabajo de investigación se considera una introducción sobre las Tics dentro del país y de la provincia del Azuay, con el fin de obtener una visión más clara del entorno actual de las tecnologías de información y comunicación, sobre el cual se desarrollará esta investigación. Con este capítulo se espera tener una visión más clara para comprender el alcance del vector de ataque de esta problemática planteada.

1.1 Las Tics en Ecuador

Según datos del Instituto Nacional de Estadísticas y Censos en su publicación "Tecnologías de la información y Comunicaciones (TICS) 2016", brinda datos importantes sobre las Tics en el país. El uso de las Tics en el país representa el 56,87% en el 2016. Del 2012 al 2016 se ha producido el incremento en el equipamiento de equipos portátiles de 13,7 puntos. 9 de cada 10 hogares en el país disponen como mínimo de un dispositivo móvil, lo que representa un crecimiento de 8,4 puntos con respecto al 2012. El acceso a internet a nivel nacional representa en 2016 el 36%, 13.5% más que en el 2012, siendo la zona urbana con un 44,6% la que más acceso a internet tiene con respecto la zona rural con un 16,4%, además se conoce que 52,9% de la población a nivel nacional dispone de un dispositivo móvil inteligente (Smartphone) en comparación al 8,2% en 2011 (Censos, 2016)

Figura 1. Indicadores Nacionales del Uso de TICS
https://observatoriotic.mintel.gob.ec/estadistica/

Indicadores internacionales proporcionados por el Observatorio TIC del Ministerio de Telecomunicaciones y de la Sociedad de la Información revelan datos importantes para continuar con la visión de las Tics en el país. Según el Observatorio TIC, el país se encuentra en el número 98 a nivel internacional en el uso de TICS, siendo la Republica de Korea, la que se encuentra en el puesto número 1. En cuanto al valor del indicador para el 2016, el país tiene un valor de 4.6, que representa una gran mejora con respecto al 3.6 obtenido en el 2010, mostrando el progreso que se está teniendo en el ámbito Tics dentro del país. (ObservatorioTIC, 2017)

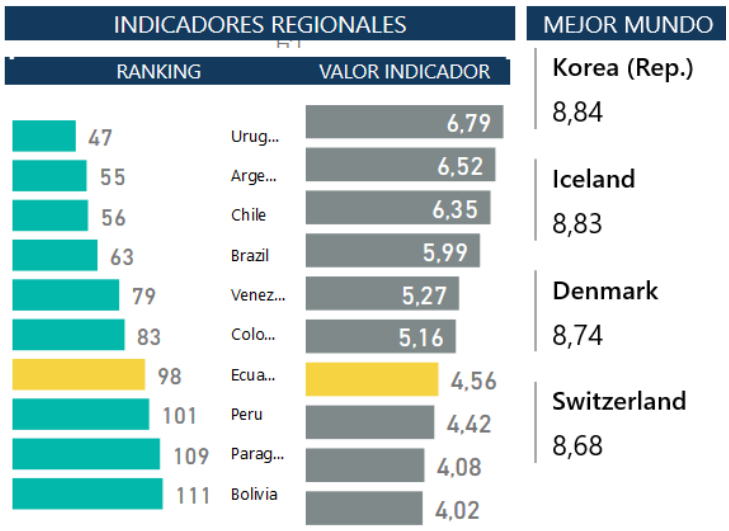


Figura 2. Ranking Internacional de Uso de TICS
https://observatoriotic.mintel.gob.ec/estadistica/

Figura 3. Valor del indicador para Ecuador de Uso de TICS
https://observatoriotic.mintel.gob.ec/estadistica/

1.2 Las Tics en el sector público ecuatoriano.

Ecuador con el fin de mejorar dentro del aspecto de las Tics a presentado por parte del Ministerio de Telecomunicaciones y de la Sociedad de la Información el "Plan Nacional de Telecomunicaciones y Tecnologías de Información del Ecuador 2016-2021". El mismo que está basado en 2 artículos que son: Avance del sector de Telecomunicaciones y Tecnología de la información y Objetivos, políticas, programas y proyectos del Plan Nacional. Con el objetivo de ser una herramienta para la planificación y gestión en el sector de telecomunicaciones y tecnologías de la información y comunicación para que forme parte en "las políticas de desarrollo sectorial e intersectorial en materia de Tecnologías de la información y comunicación, para conseguir una mayor inclusión digital y competitividad del país". (Información, 2017)

Mediante este instrumento se desea posicionar al Ecuador para el año 2021, para ser un referente en la región en el tema de "conectividad, acceso y producción de los servicios TIC, evidenciando en indicadores que demuestren el desarrollo económico y social del país". (Información, 2017)

Para conciliar respecto a este plan se utilizan como base los actuales planes nacionales y la misión del MINITEL, la cual es organismo encargado de desarrollar las Tecnologías de la Información y Comunicación en el Ecuador, y la gestión de todos los planes generales y seguimientos en los sectores estratégicos del país. (Información, 2017)

Al representar el 2.1% del Producto Interno Bruto del País en el 2013, las TICS son un sector estratégico del mismo, por lo tanto, requieren de una regulación para su correcto uso y en el caso del país es la Ley Orgánica de Telecomunicaciones (LOT).

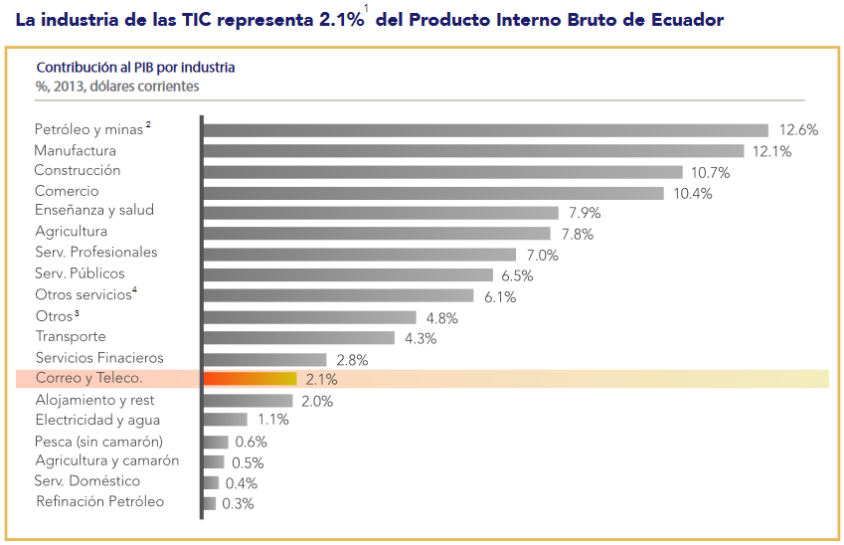


Figura 4. Contribución al PIB por industria

https://www.telecomunicaciones.gob.ec/wp-content/uploads/2016/08/Plan-de-Telecomunicaciones-y-TI..pdf página 18.

En el ámbito de las Tecnologías de Información, el Ecuador estableció una política pública en el año del 2008 que representó un cambio importante en cuanto a las Tics en el sector público pues obliga al uso de software libre para las entidades en la Administración Pública, para fomentar a los desarrolladores de software la priorización del software que se produce en el país, como software libre. De lo contrario, de ser extranjero con componentes nacionales. (Información, 2017)

1.3 Las Tics en la provincia del Azuay.

El Observatorio TIC del Ministerio de Telecomunicaciones y de la Sociedad de la Información nos brinda información de gran importancia sobre las Tics en la provincia del Azuay. Como se puede observar en la Figura 5, el porcentaje de personas que utilizan Tics en la provincia del Azuay es del 62.2%, siendo la cuarta con mayor utilización en el

país y solamente superada por las provincias de: Galápagos, Pichincha y El Oro. (ObservatorioTIC, 2017)

La provincia del Azuay se sitúa en el 3er lugar a nivel nacional, en la provincia con mayor porcentaje de personas que utilizan computadora con un 59.3% en 2016. Además de mantenerse en el mismo 3er lugar a nivel nacional con un 61.1% en cuanto a personas que han utilizado internet en los últimos 12 meses en 2016. Ocupa la provincia del Azuay un 5to lugar en el ranking general del país con un 57,5% en cuanto a personas que tienen teléfono celular activado por provincia en 2016. (Censos, 2016)

Figura 5. Acceso y uso de Tics en las provincias del país. https://observatoriotic.mintel.gob.ec/estadistica/

Conclusiones

El Ecuador pocos años atrás, ha cambiado su postura en cuanto a la modernización y equipamiento de TICS, el crecimiento se puede apreciar en las cifras que se manejan actualmente, y sobre todo del compromiso del gobierno al implementar el Plan Nacional de Telecomunicaciones y Tecnologías de Información del Ecuador 2016-2021. Con esto se puede comprender que el país cada vez se suma a la globalización y al cambio tecnológico, y esto implica que se tiene una mayor cantidad de vectores de posibles ataques a estos equipos y es obligación del gobierno, autoridades y la sociedad en general estar conscientes de los posibles problemas que se puedan presentar, y soluciones de los mismo.

Azuay al encontrarse como cuarta provincia con mayor uso de TICS en el país, se postula como uno de los principales objetivos para cibercriminales que pueden obtener acceso a información privilegiada de una manera ilegitima, con esto poner en riesgo la información de todos los ciudadanos. Existe entidades públicas que manejan la información de los ciudadanos y esta puede llegar en algún punto, a ser filtrada por cibercriminales.

Estas cifras que se presentan con la visión de la TICS tanto en el país como la provincia son solo un indicador de todo lo que implica el proceso de modernización de equipos electrónicos, tanto en beneficios como posibles problemas.

CAPÍTULO 2
2. LOS METADATOS EN DOCUMENTOS INFORMÁTICOS Y BUENAS PRÁCTICAS DE SEGURIDAD DE LA INFORMACIÓN EN DOCUMENTOS INFORMATICOS

Introducción

Como introducción a la hipótesis planteada, este capítulo espera ser el marco teórico para la compresión de los términos utilizados dentro del trabajo de investigación, se plantea que los documentos de algunas entidades públicas dentro del sector de Cuenca son vulnerables al mantener metadatos de manera pública y accesible para cualquier ciudadano, por lo que esta tesis planea demostrar si es real esta problemática.

Los documentos informáticos públicos forman parte de nuestro medio, pues las entidades públicas pueden evidenciar su trabajo hacia los ciudadanos, de una manera que estos puedan conocer de las actividades que realizan las mismas. El problema nace cuando estos documentos informáticos son subidos a internet sin la debida protección, y generan fuga de información privilegiada sin intención pues estos documentos almacenan metadatos, los mismos que poseen información muy valiosa de las personas que crean estos documentos.

Como parte de este capítulo, se espera también dar una visión de cómo los buscadores indexan estos documentos, y como son accesibles al público en general, además de las buenas prácticas de seguridad informática que se recomiendan, sobre todo, las buenas prácticas de seguridad en documentos informáticos.

2.1 Seguridad Informática

La seguridad informática se define como la protección aplicada a dispositivos digitales y a sus canales de comunicación, con el fin de mantener estos confiables, estables y razonablemente seguros de daños o amenazas. Generalmente la protección que se requiere debe ser la suficiente para prevenir o abordar el acceso no autorizado o la intervención antes de que se pueda generar un daño personal, profesional, organizacional, financiero o político. (Meeuwisse, 2017).

Según Meeuwisse (2017, p. 6) un dispositivo digital es "*cualquier aparato electrónico con el cual se puede crear, modificar, almacenar, recuperar, o transmitir*

información en un formato electrónico. Computadores de escritorio, laptops, tablets, smartphones y dispositivos de casa conectados a internet son un ejemplo de dispositivos digitales".

La seguridad informática es más que una disciplina que se encarga de proteger computadores, es más, se refiere a mucho más que proteger cada una de las tecnologías, la seguridad informática trata sobre la protección de las personas, que directa o indirectamente son las que confían en todos los dispositivos electrónicos. (Meeuwisse, 2017).

Actualmente se acepta que la seguridad informática también abarque la necesidad de mantener dispositivos electrónicos y los servicios digitales estables y confiables. Específicamente en seguir una estrategia de seguridad informática que confía solamente en la prevención, ya no funciona. Es necesario que las organizaciones modernas tengan la habilidad de detectar interrupciones inesperadas o no autorizadas. Posteriormente, generar un rápido diagnóstico de los problemas, y resolverlos, direccionarlos y finalmente restablecer los servicios afectados. (Meeuwisse, 2017)

2.2 Los metadatos

Los metadatos están en nuestro alrededor, todo el tiempo. En una era en la que los dispositivos electrónicos están conectados durante todo el tiempo, casi todos los dispositivos que las persona utilizan, confían en los metadatos, generan metadatos, o ambos. Cuando los metadatos realizan correctamente su trabajo, estos se desvanecen en segundo plano, y pasan desapercibidos y casi invisibles (Pomerantz, 2015).

En los años 90s, los metadatos eran términos que principalmente fueron utilizados por comunidades que estaban involucradas con la administración e interoperabilidad de datos geoespaciales y también con administración de datos, diseños de sistemas y mantenimientos en general. En estos tiempos, el termino hacía referencia hacia un conjunto de normas industriales, así como a la documentación que se presenta tanto interna como externa de manera adicional. Y de otra información necesaria para la identificación, presentación, interoperabilidad, gestión de manera técnica, rendimiento y el uso de datos que se encontraban contenidos en un sistema de información (Baca, 2016).

Para explicar el termino metadato, partiremos desde su descomposición etimológica, pues el prefijo meta proviene del griego que significa *acerca*, información

acerca de algo. Así pues, metadato, quiere decir información sobre los datos, en otros términos, es definido como datos acerca de los datos (Gartner, 2016).

Los metadatos se pueden definir como datos que contienes información sobre un documento o fichero en particular. Pues un documento puede poseer metadatos con gran variedad de información respecto a la procedencia de este, datos sobre el autor de este documento, la fecha en la que fue creado y modificado, otros usuarios que han manipulado este documento, incluso el software con el que este documento fue redactado o modificado. Solamente como un par de ejemplos de toda la información que pueden almacenar los metadatos. Como ejemplo en ficheros, una fotografía podría almacenar entre sus metadatos, información sobre la marca y el modelo de la cámara con la que fue tomada esa foto, resolución, o incluso, hasta las coordenadas de posicionamiento geográfica GPS, desde el lugar desde el cual se tomó esta fotografía (Alonso, y otros, 2013).

Los metadatos facilitan la clasificación de información, facilitan también su localización, pues la información que mantienen es utilizada para la optimización en las búsquedas, pues son utilizados de forma masiva por Sistemas de Gestión Documental de algunas empresas o por motores de búsqueda en Internet. Estos metadatos de los fiches almacenados por los sistemas, simplifican el conseguir filtros para la manipulación de archivos, por ejemplo, en la búsqueda de archivos creados en una fecha determinada (Alonso, y otros, 2013).

Además, cabe acotar que los metadatos son la base de una Web Semántica, una extensión de las Web en la que, de manera ideal, las aplicaciones podrían generar interacción sin la intervención humana pues conocerán el significado de los datos y las relaciones que se presentan entre ellos, con este propósito es necesario que la información se encuentre autodocumentada. (Alonso, y otros, 2013)

2.3 Documentos informáticos

Se entiende por documentos informáticos a los documentos que son producidos, receptados o almacenados por una persona en el transcurso y como un medio de apoyo en las actividades y testimonio de las mismas. Utilizando medios electrónicos que permiten la conservación de estos y que se transmiten por medios electrónicos en lugares de almacenamiento para su conversación permanente, con una previa selección con la

identificación y valoración con medidas de autentificación y preservación de manera adecuada, además de una organización correcta, para garantizar el valor informativo legal y también cultural. Así como permitir el acceso y el uso mediante medios electrónicos correspondientes (Navarro, 2017).

Un documento informático desde su estructura está compuesto de señales digitales, por lo tanto, carece de las características que presenta un documento físico tradicional. Las características que cada documento informático posee son en gran medida funciones del software con el cual han sido desarrollados, como puede ser: su extensión, formato, etc. Y estos están diferenciados a gran medida del texto que contenga el mismo (Rodríguez Bravo, 2017).

Los documentos informáticos presentan dos problemáticas en concreto: El primero es la creación y la manutención de documentos que permanecen con características de activos y semiactivos de manera fiables y auténticos, es decir que se pueda utilizar este documento como evidencia de trabajo en cualquier proceso de una empresa. Y el segundo, es la conservación de documentos inactivos que se tienen que conservar por el valor de la información que contienen (Serra Serra, 2017).

2.4 Indexación de documentos informáticos a buscadores

Partiremos del precepto que los buscadores de internet buscan facilitarnos la vida a los usuarios permitiéndonos hacer búsquedas con el objetivo de encontrar con mayor facilidad la información que los usuarios requieran. Como ejemplo para la explicación de este punto partiremos del funcionamiento de la indexación y rastreo de contenido del buscador número uno de internet, Google.

2.4.1 Cómo encontrar la información con el rastreo de contenido

Google, encuentra y descubre páginas web de dominio público mediante un software que ellos han denominado como “rastreador web”, este “rastreador” es más conocido como Googlebot. El funcionamiento de este rastreador es simple, consulta páginas web y dentro de estas, igualmente consulta los enlaces que se encuentran en las páginas, como si se tratara de un usuario normal dentro del sitio web. Así pues, pasan de enlace en enlace, y en este camino recopilan datos de estas páginas, los mismos que son enviados a los servidores de Google (Google, 2017).

El proceso de rastreo inicia cuando se tiene una lista de direcciones web de rastreos que se han realizado con anterioridad y de sitemaps que el propietario del sitio ha proporcionado a Google. Cuando se accede a estos sitios, estos rastreadores buscan enlaces que redirijan hacia otras páginas para posteriormente ser visitadas. Este software hace énfasis en los sitios nuevos, en los cambios que se presentan en el sitio visitado actualmente y en los enlaces que se encuentran inactivos (Google, 2017).

El software es el que determina cuáles serán los sitios que serán rastreados, la frecuencia con la que se realiza ese proceso y cuál será el número de páginas que serán exploradas en cada sitio. "*Google no acepta pagos para rastrear un sitio con más frecuencia. Nos preocupamos más por tener los mejores resultados posibles porque, a largo plazo, es lo mejor para los usuarios y también para nosotros*." (Google, 2017).

2.4.1 Cómo organizar la información que es indexada con el contenido

Internet se podría definir como una biblioteca pública en la que diariamente se agregan más libros y que no dispone de un sistema de archivos. Por lo que Google ayuda en este proceso, pues una vez que recopila las paginas durante el proceso de rastreo, posteriormente crea un índice, pues conoce exactamente donde tiene que buscar. Al igual que los libros disponen de un índice al final del mismo, Google dispone de un índice que incluye información sobre las palabras y en qué lugar aparecen. Cuando un usuario realiza una búsqueda, en un nivel más básico, los algoritmos de Google, consultan estos términos en los índices para encontrar las paginas indicadas (Google, 2017).

Una vez que se realiza este proceso, la complejidad aumenta, pues si buscamos una palabra por ejemplo "perro" no aparecerán todas las páginas que incluyan gran cantidad de veces esta palabra, puesto que la persona que busca este término, probablemente está buscando imágenes, videos, o los tipos de razas de perros que existen. Aquí entra en funcionamiento el grafico de conocimiento de Google, que es un término que no compete tratar ahora (Google, 2017).

Igualmente, Google permite a los administradores de los sitios web, plantearse restricciones para rastrear, indexar o publicar contenido, para que estos no aparezcan en los resultados de las búsquedas. Aquí los administradores de los sitios tienen algunas opciones para controlar como Google rastrea e indexa los sitios a internet, uno de estos y el más conocidos es el archivo "robots.txt". En este archivo, los administradores de los

sitios pueden indicar a Googlebot que no rastree sus sitios o generar instrucciones más específicas sobre como este procesa sus páginas web. Es decir, se puede permitir que se rastree solamente una porción de sitio y no todo (Google, 2017).

Ahora como se conoce todo el funcionamiento de la indexación de sitios a Google, los sitios web, suelen contener en su interior documentos informáticos que sirven para que los usuarios puedan leer sobre diferentes tipos de consultas, al indexar un sitio a Google, por defecto si no existen restricciones, se indexan sus documentos informáticos, lo que automáticamente con los términos indicados, le permite a un usuario consultar directamente estos desde el buscador de Google.

2.5 Buenas prácticas de seguridad informática

En la actualidad el tema de la seguridad informática ha tenido un gran auge y su importancia dentro de las Tics en general, es por eso que existen estándares y modelos de referencia para manejar la seguridad de la manera correcta. Generalmente se divide la seguridad informática en 5 o más etapas, pero para el estudio de este proyecto de investigación. la dividiremos en 5 etapas: Identificar, Proteger, Detectar, Responder, Recuperar (Meeuwisse, 2017).

Dividiendo estas 5 etapas en 2 grupos: Identificar y Proteger como Proactivo, y Detectar, Responder y Recuperar como Reactivo. Dentro de la etapa proactiva es cuando la seguridad informática se puede aplicar de la manera más eficiente y con mayor impacto. Aunque las medidas reactivas son importantes, cuesta mucho más tiempo corregir un problema de seguridad, que incluir medidas de seguridad correctas en primer lugar (Meeuwisse, 2017).

Entre las medidas que se tiene es la clasificación, por ejemplo, la clasificación de la información: Confidencialidad, Integridad, Disponibilidad y Consentimiento. Los puntos de defensa de seguridad: Datos, Dispositivos, Aplicaciones, Sistemas y Redes. Tipos de control de seguridad: Física, Procesal, Legal y Técnica. Modos de control de la seguridad: Preventiva, Detectiva y Correctiva (Meeuwisse, 2017).

La clasificación, controles y conceptos relacionados a estos son de hecho, de mucha relevancia en el cumplimiento de los objetivos primarios en cualquier tipo de seguridad.

2.6 Buenas prácticas de seguridad en documentos informáticos

Este se convierte en el punto más importante de la investigación, pues indica como eliminar los metadatos de los documentos informáticos, para poder mitigar el problema de la fuga de información en caso de existir dentro de la hipótesis planteada.

2.6.1 Documentos en Office

La herramienta para la limpieza de metadatos en documentos Office es la opción de "inspeccionar documento", esta herramienta es la encarga de buscar todos los metadatos del documento, que son introducidos por el usuario, información del documento, metadatos ocultos que son introducidos por el programa con el que se crea el documento, información de las impresoras e información oculta. Esta herramienta permite la eliminación de los metadatos que el usuario no desea incluir en el documento (Alonso, y otros, 2013).

Paso 1: Ingresar en la ventana "Archivo" del documento que se desea eliminar los metadatos, después damos clic en la opción información, posteriormente un clic en "Comprobar si hay problemas".

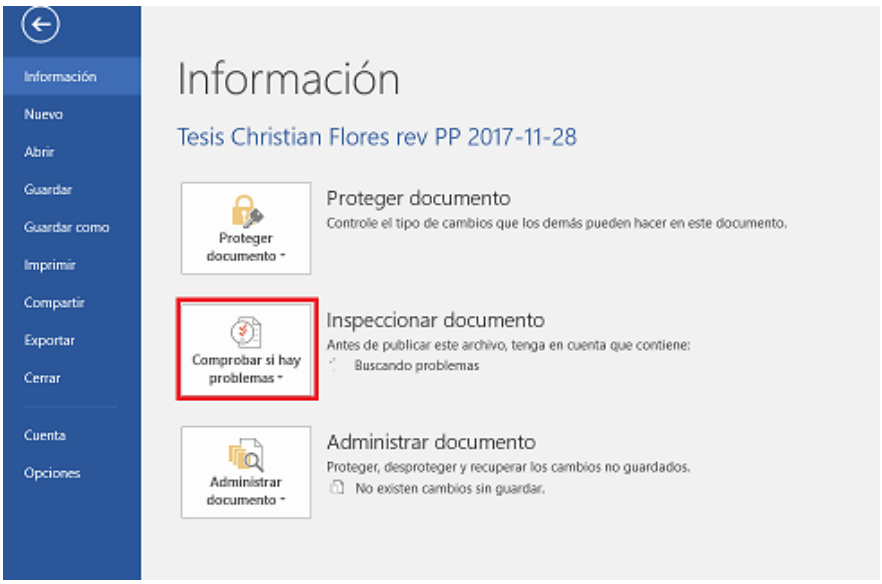


Figura 6. Opciones de la opción información de la ventana Archivo.

Paso 2: Damos clic en “Inspeccionar Documento”.

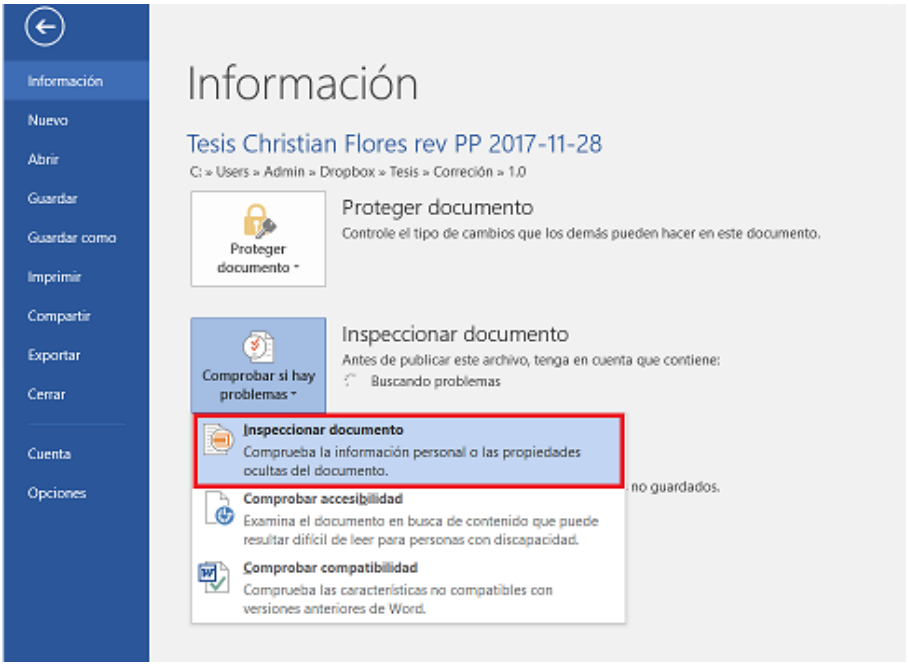


Figura 7. Opciones de la opción Comprobar Si Hay Problemas.

Paso 3: Posteriormente damos clic en la opción “Inspeccionar”, para inspeccionar toda la información marcada en los cuadros de texto.

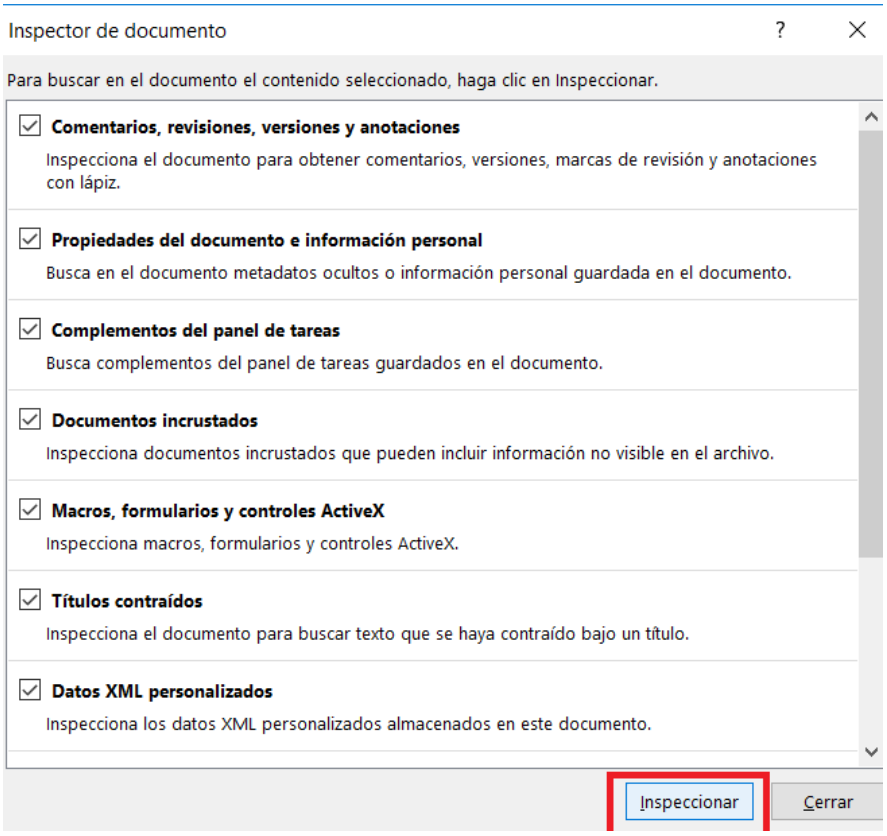


Figura 8. Ventana del Inspector de Documento.

Paso 4: Aparecerán automáticamente junto al documento, los resultados de la inspección, en cada categoría de información encontrada se marcará con un signo de interrogación en la categoría que se tenga metadatos que pueden ser eliminados. Procedemos a dar clic en "Quitar todo" de cada categoría que deseamos eliminar los metadatos. Para comprobar que los metadatos han sido eliminados, damos clic en la opción "Volver a Inspeccionar".

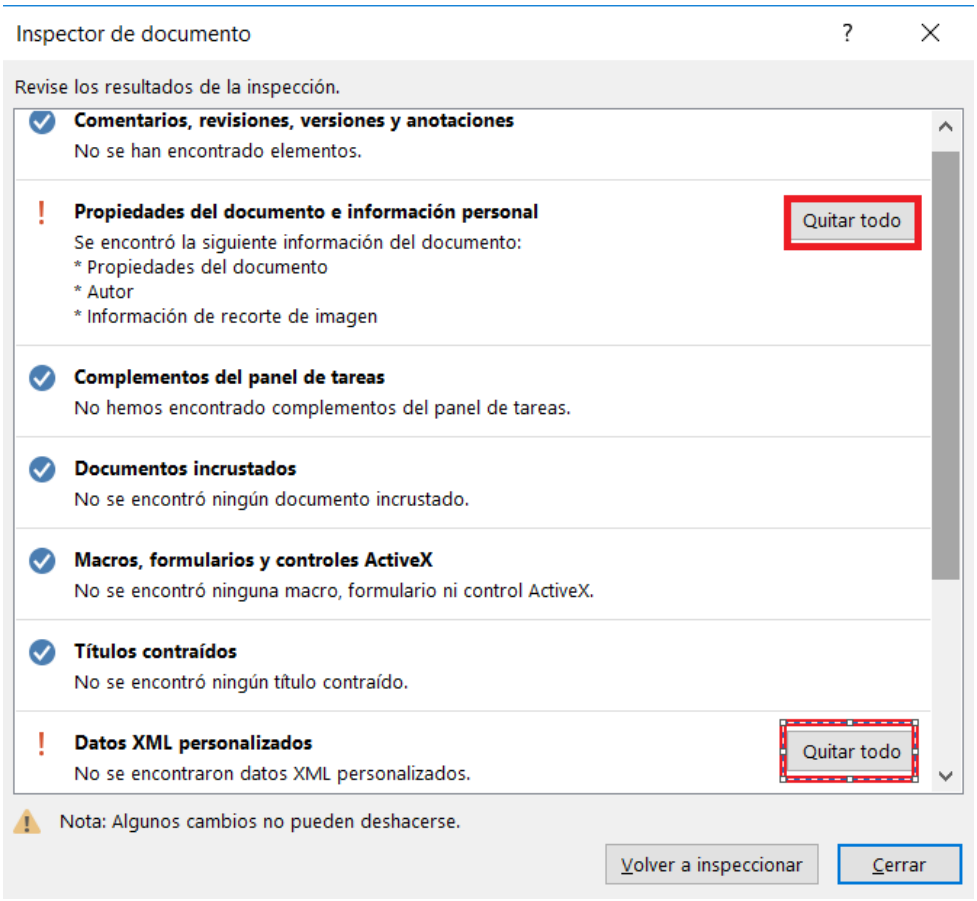


Figura 9. Metadatos para eliminar en el Inspector de Documento.

Paso 5: Podemos revisar que todos los metadatos del documento han sido eliminados.

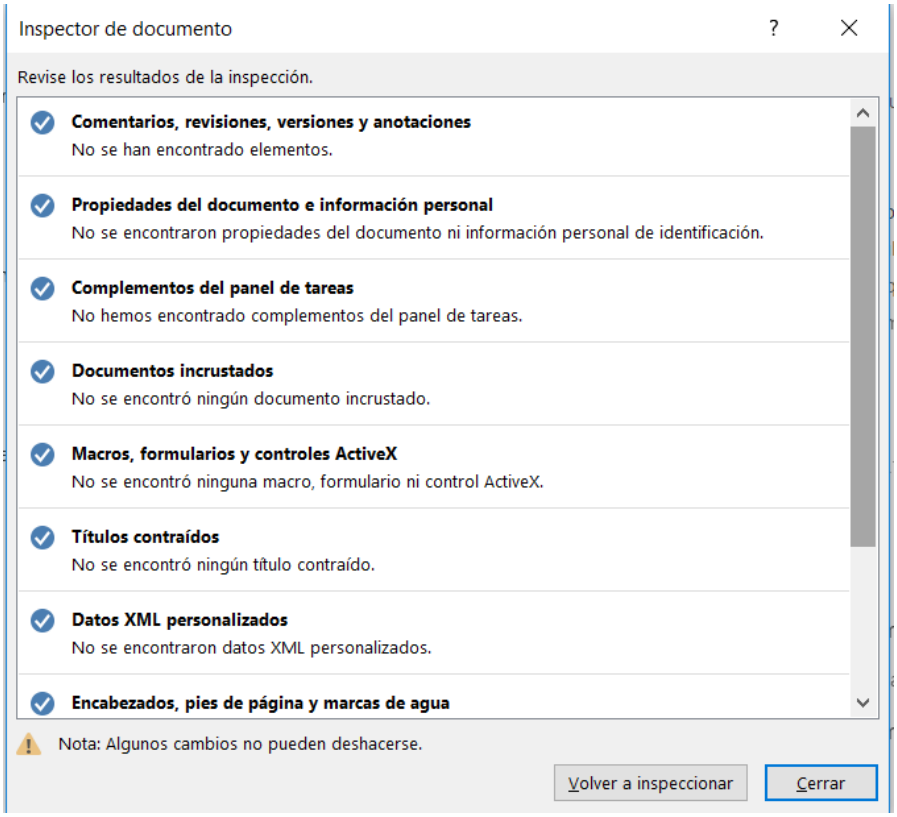


Figura 10. Ventana del Inspector de Documento.

Una vez seguido este proceso, podemos asegurarnos que los metadatos del documento han sido eliminados de manera correcta.

2.6.2 Documentos en PDF con Acrobat DC

La eliminación de metadatos en archivos pdf es simple, solamente tenemos que buscar en las propiedades del archivo con Adobe Acrobat DC y seleccionar el esquema de metadatos que deseamos eliminar (Adobe, 2017).

Paso 1: Damos clic en la opción “Archivo”.

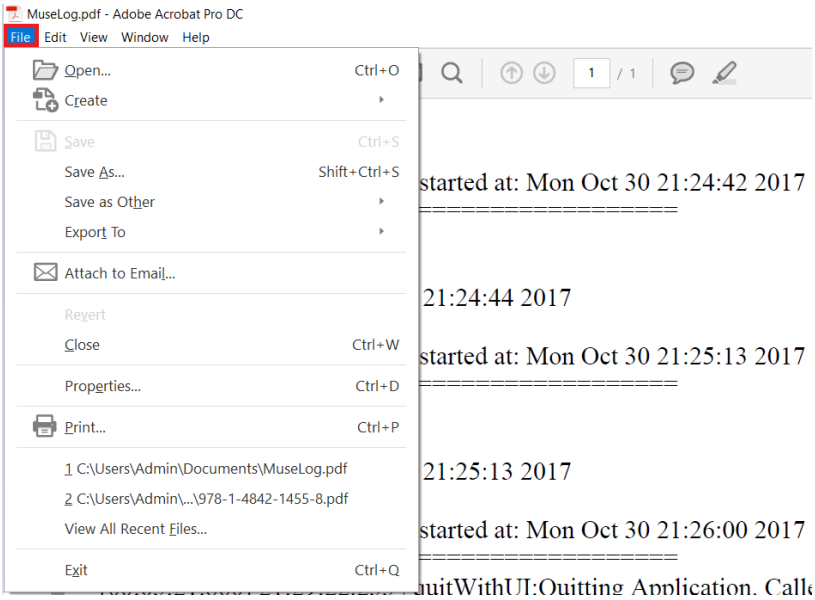


Figura 11. Opciones de la ventana Archivo.

Paso 2: Damos clic en “Propiedades”.

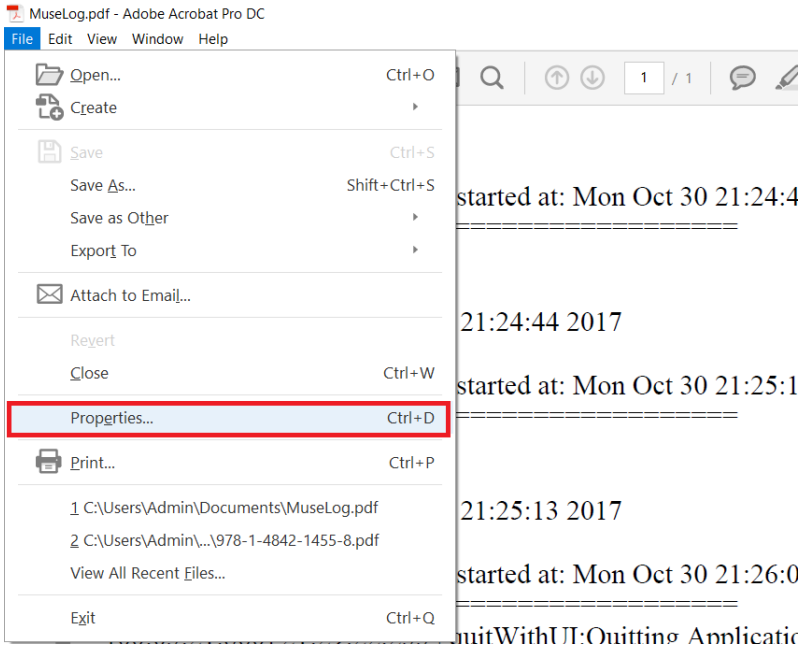


Figura 12. Opciones de la ventana Archivo.

Paso 3: En la ventana Propiedades del Documento, damos clic en la opción "Metadatos Adicionales".

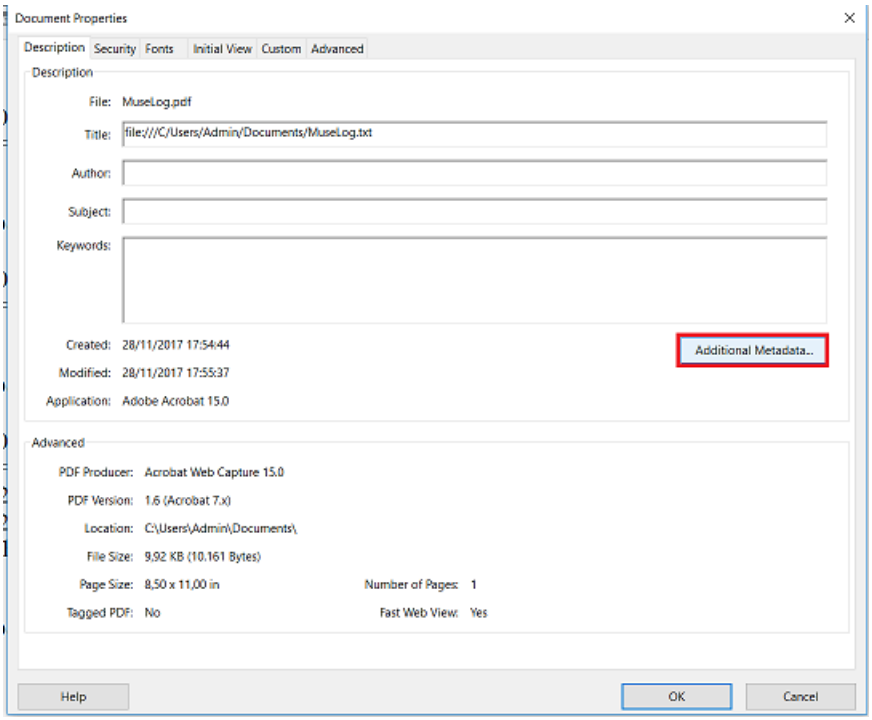


Figura 13. Ventana de Propiedades del Documento.

Paso 4: Seleccionamos la opción "Avanzado"

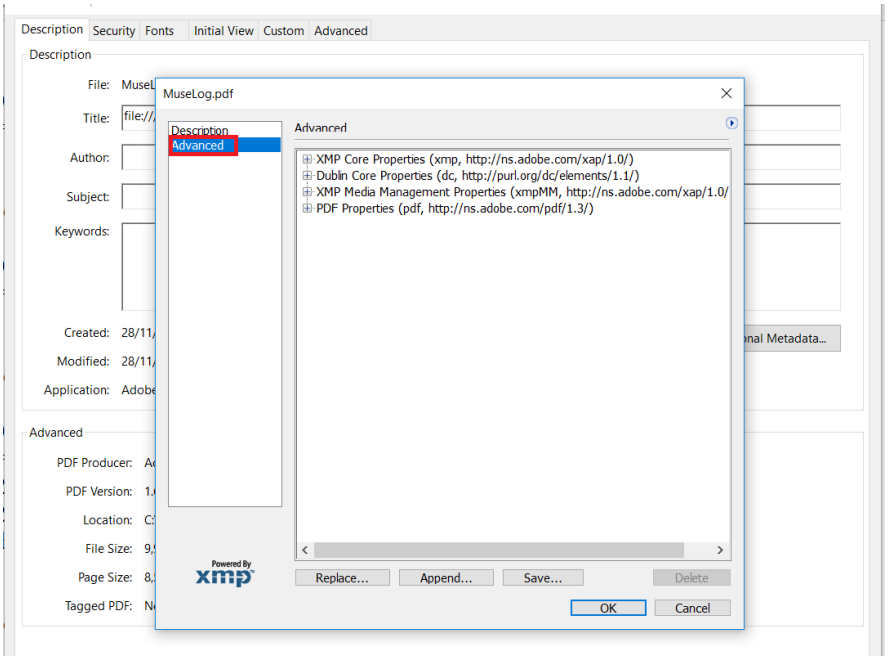


Figura 14. Ventana de Metadatos Adicionales del Documento.

Paso 5: Seleccionamos el esquema de metadatos que deseamos eliminar y damos clic en la opción “Eliminar”.

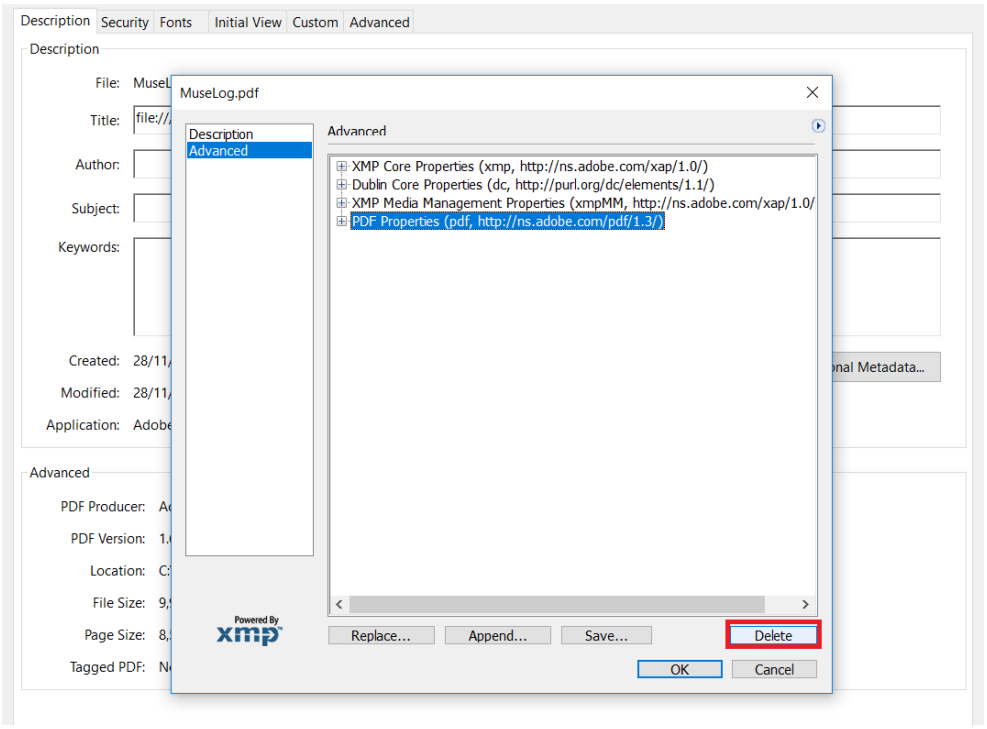


Figura 15. Ventana de Metadatos Adicionales del Documento.

Una vez seguido este proceso, podemos asegurarnos que los metadatos del documento han sido eliminados de manera correcta.

Conclusiones

En este capítulo se puede conocer de todo el marco teórico necesario para la entender la teoría detrás de la hipótesis propuesta, este capítulo es la base de conocimiento necesarios para la compresión del capítulo siguiente en el que se pondrá en práctica la prueba de la hipótesis y requiere de un conocimiento previo adquirido en este capítulo.

Se puede entender que los metadatos son la base fundamental de la hipótesis, por lo tanto, conocemos un concepto claro de los metadatos, que son datos de los datos. Estos aportan gran información para el manejo de grandes cantidades de información, pero a su vez al ser públicos exponen estos datos para ser accedidos por cualquier usuario que lo dese.

Así mismo, este capítulo tiene la sección más importante, pues indica cómo se pueden mitigar el problema con los metadatos mediante la eliminación de los mismo, tanto en documentos office como en documentos PDF, que son los tipos de archivos públicos más utilizados.

De esta manera se tiene un conocimiento base teórico del tema, aclaración sobre los metadatos y su mitigación para no generar fuga de información privilegiada.

CAPÍTULO 3
3. DIAGNÓSTICO DE LA VULNERABILIDAD DE LA INFORMACIÓN DE DOCUMENTACIÓN PÚBLICA DE ENTIDADES DEL SECTOR PÚBLICO DE LA CIUDAD DE CUENCA

Introducción

Ahora que se conoce un poco más sobre la teoría de los metadatos, la forma en la que los documentos son indexados a internet y la eliminación de los mismos, procedemos a probar la hipótesis, de que existen entidades públicas que tienen esa vulnerabilidad en sus documentos públicos.

Además de dar una visión una poco más extensa sobre el software de análisis de metadatos y toda la información necesaria sobre La FOCA, que es la herramienta para el análisis y extracción de metadatos que ha sido seleccionados para este trabajo de investigación.

Finalmente, se hará un análisis de los resultados, obtenidos al buscar metadatos en los documentos de las entidades públicas seleccionadas.

3.1 Software de Análisis de Metadatos

Los metadatos pueden ser extraídos desde los documentos informáticos de manera manual, y se puede acceder a la información contenida dentro de la misma, pero es un trabajo realmente agotador, sobre todo si se dispone de una gran cantidad de documentos, pues se tiene que realizar un proceso varias veces por la cantidad de documentos que se tenga o se quiera analizar (Alonso, y otros, 2013).

Para esto existe software de Análisis de Metadatos, los cuales nos permiten la automatización del proceso, permitiendo analizar los documentos, extraer sus metadatos y obtener información privilegiada (Alonso, y otros, 2013).

Con el tiempo este tipo de software se han robustecido, y realizan la búsqueda automatizada de documentos de un sitio web en específico, realizando búsquedas por los principales motores de búsqueda de internet. Por esto, para esta investigación y probar la hipótesis planteada se utilizará el software de análisis de metadatos, LA FOCA (Alonso, y otros, 2013).

3.2 La FOCA

"*FOCA (Fingerprinting Organizations with Collected Archives)"* es una herramienta que le permite a los usuarios, buscar metadatos e información que parece estar oculta en los documentos que son examinados con esta herramienta. Los documentos pueden encontrarse tanto de manera local donde se corre el software, como en sitios web, desde los cuales la herramienta se encarga de descargar y analizar los documentos (Telefonica, 2017).

Los tipos de documentos que es capaz de analizar la FOCA, son variados, pero comúnmente los archivos de Microsoft Office, Open Office, o ficheros PDF, pero este software también permite el análisis de otro tipo de ficheros como son Adobe InDesing o svg (Telefonica, 2017).

Los documentos son buscados con tres buscadores que son Google, Bing y DuckDuckGo. Con este respaldo de buscadores, se puede conseguir gran número de documentos para su análisis. Permitiendo así mismo, analizar ficheros de manera local, o desde una URL desde internet (Telefonica, 2017).

Con toda la información que ha sido extraída con la herramienta, la FOCA, se encarga de unir y trata de reconocer los documentos que han sido generados por el mismo equipo, usuario y con qué servidores y clientes están unidos (Telefonica, 2017).

3.3 Funcionamiento de la FOCA

Primero necesitamos descargar el software desde el siguiente link: https://www.elevenpaths.com/es/labstools/foca-2/index.html , una vez que tenemos el programa procedemos a correr el ejecutable y comenzamos a demostrar el funcionamiento del mismo.

Primero procedemos a crear un nuevo proyecto, dando clic en la ventana “Project”.

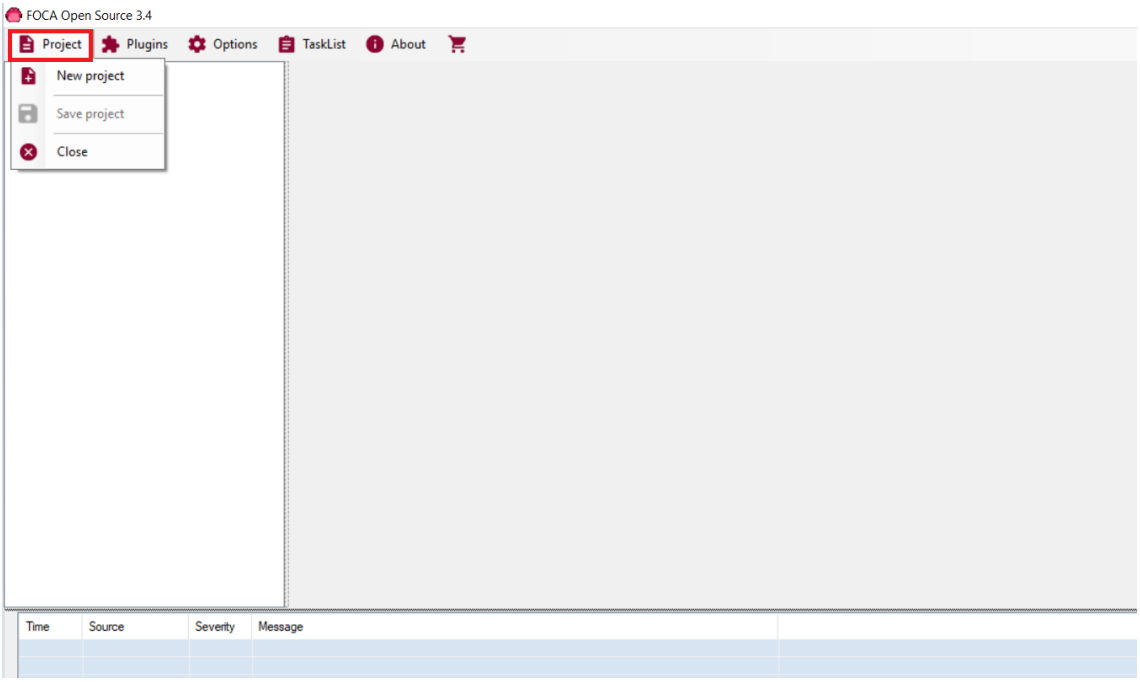


Figura 16. Herramienta La FOCA.

Posteriormente, damos clic en “New Project”, para crear un nuevo proyecto.

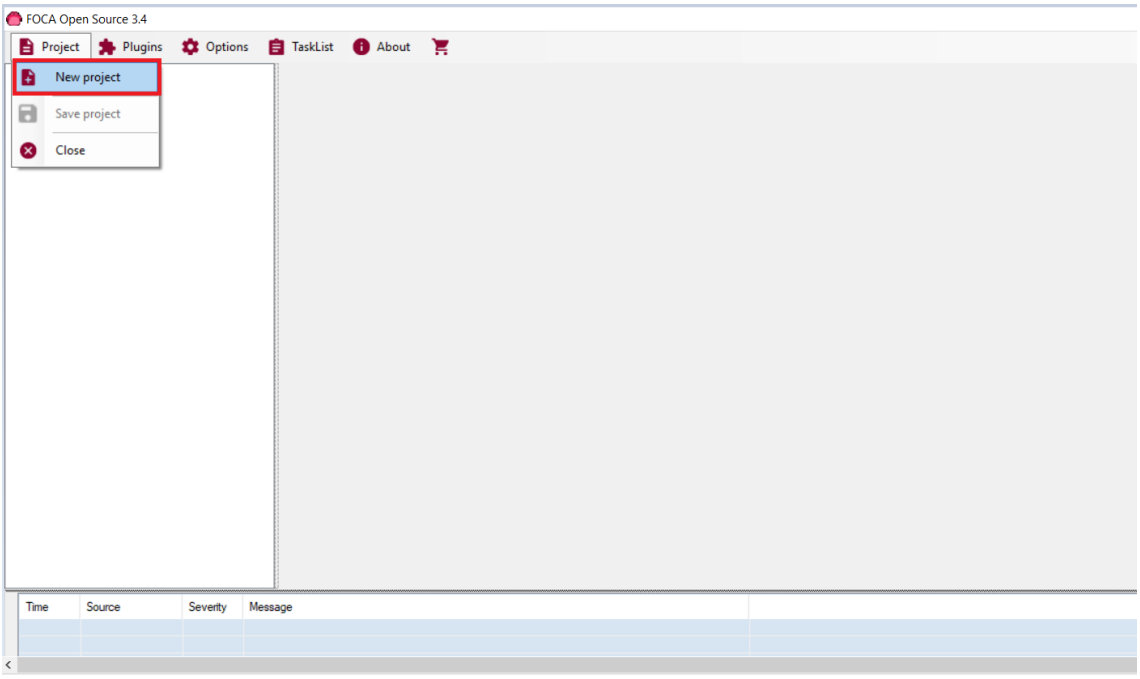


Figura 17. Herramienta La FOCA.

Una vez creado el proyecto, procedemos a llenar los campos para el mismo, como son el nombre del proyecto, el dominio de la página web de donde obtendremos los documentos, la carpeta donde se almacenará el proyecto y procedemos a dar clic en "Create" para crear el proyecto.

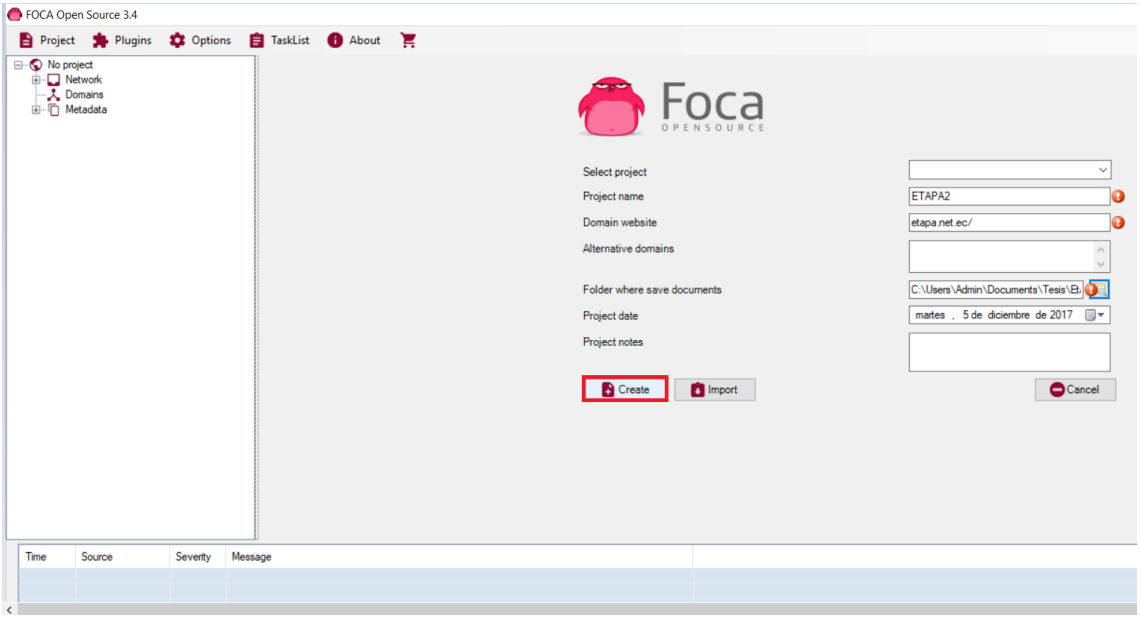


Figura 18. Creación de nuevo proyecto en La FOCA.

Nos indica un mensaje que el proyecto ha sido creado con éxito.

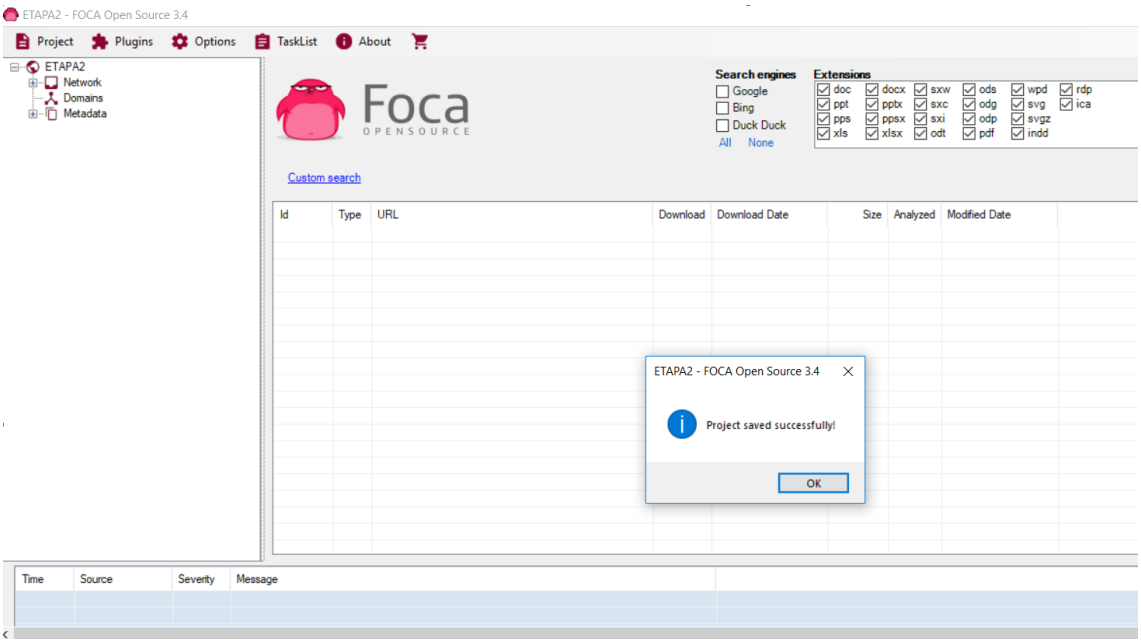


Figura 19. Creación de nuevo proyecto en La FOCA.

En la sección de “Search Engines”, seleccionamos las 3 opciones, de esta manera podremos obtener todos los documentos indexados de estos 3 buscadores, y seleccionamos todas las extensiones de archivos que se desean buscar (por defecto, están marcada todas las casillas). Finalmente damos clic en la opción “Search All” para empezar la búsqueda de los documentos.

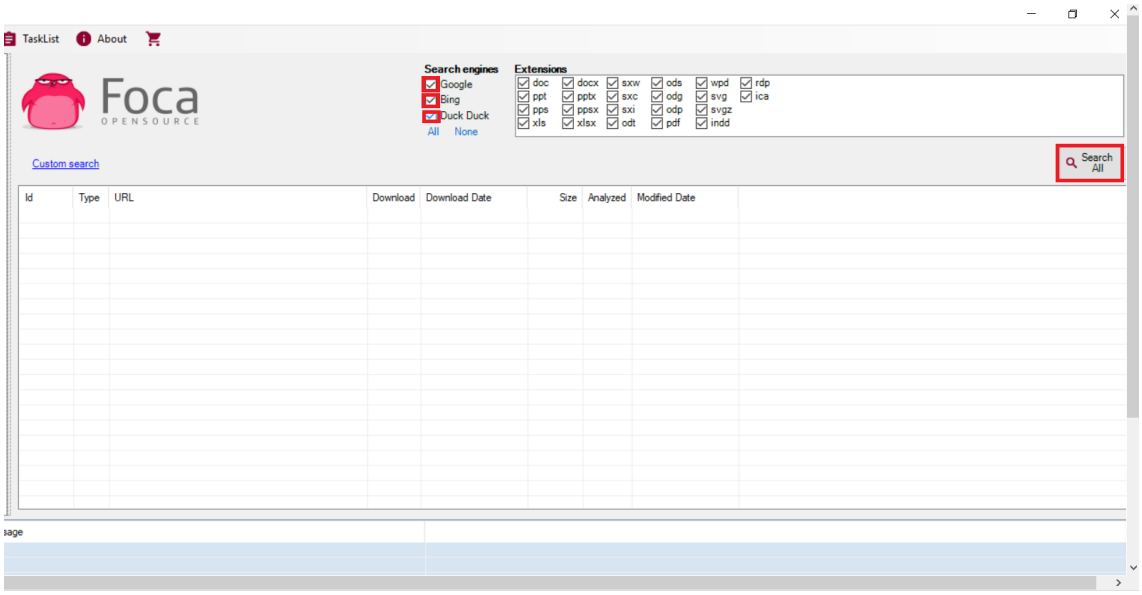


Figura 20. Búsqueda de documentos en La FOCA.

Una vez que se han descubierto todos los documentos, seleccionamos todos los documentos y con un clic derecho buscamos la opción “Download All” y damos clic para comenzar a descargar en nuestro proyecto todos los documentos encontrados en los buscadores.

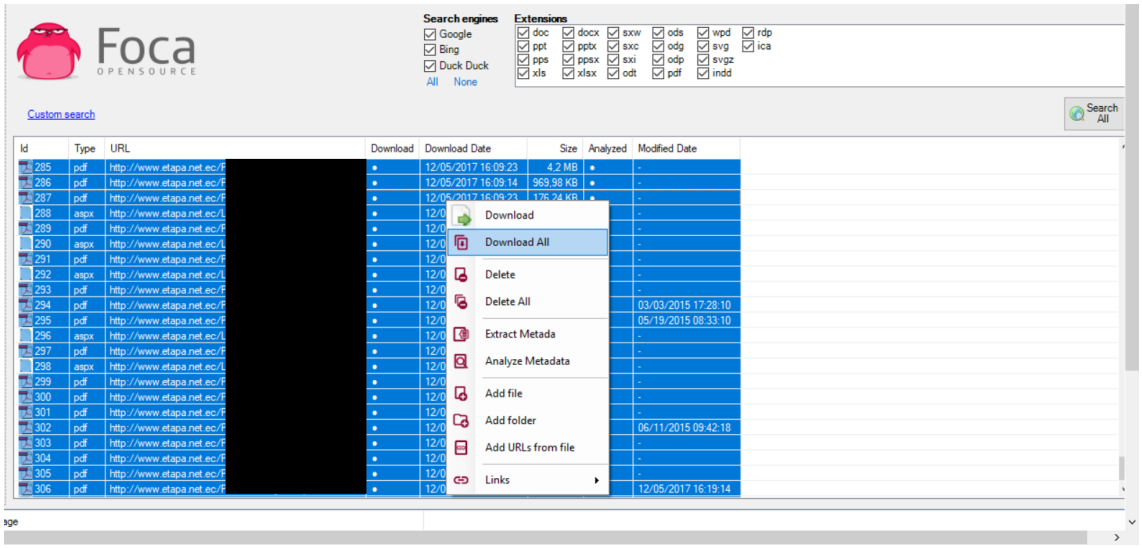


Figura 21. Descarga de documentos en La FOCA.

Podemos observar que en la columna de “Download”, se tiene un circulo verde, lo que indica que el documento ha sido descargado de manera correcta, caso contrario de tener una x roja significaría que aún no está descargado o existió un problema en su descarga.

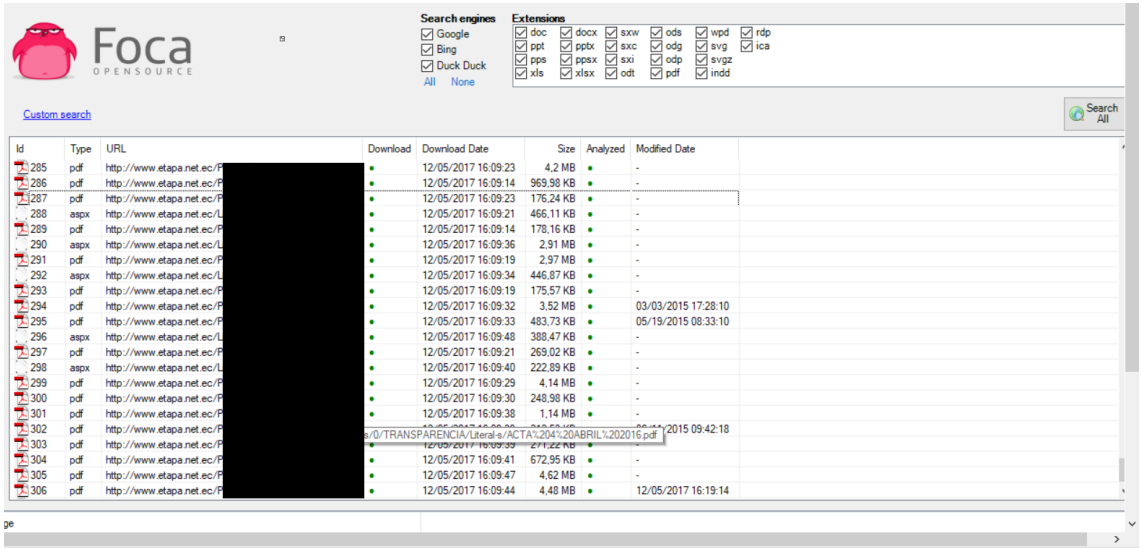


Figura 22. Descarga de documentos en La FOCA.

Posteriormente, seleccionamos todos los archivos y damos clic derecho, buscamos la opción “Extract Metadata”, para extraer todos los metadatos de los archivos descargados,

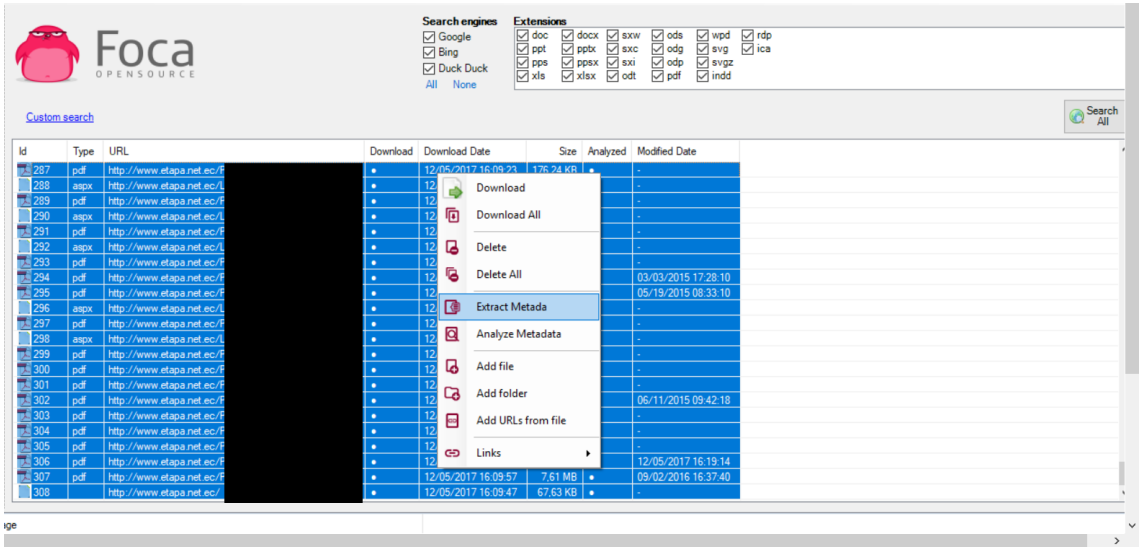


Figura 23. Extracción de metadatos de documentos en La FOCA.

Ahora podemos encontrar en la parte izquierda, información respecto a los metadatos obtenidos, por ejemplo, la cantidad de documentos que son de tipo: .doc, .docx, .xls, .xlsx, .pdf, etc.

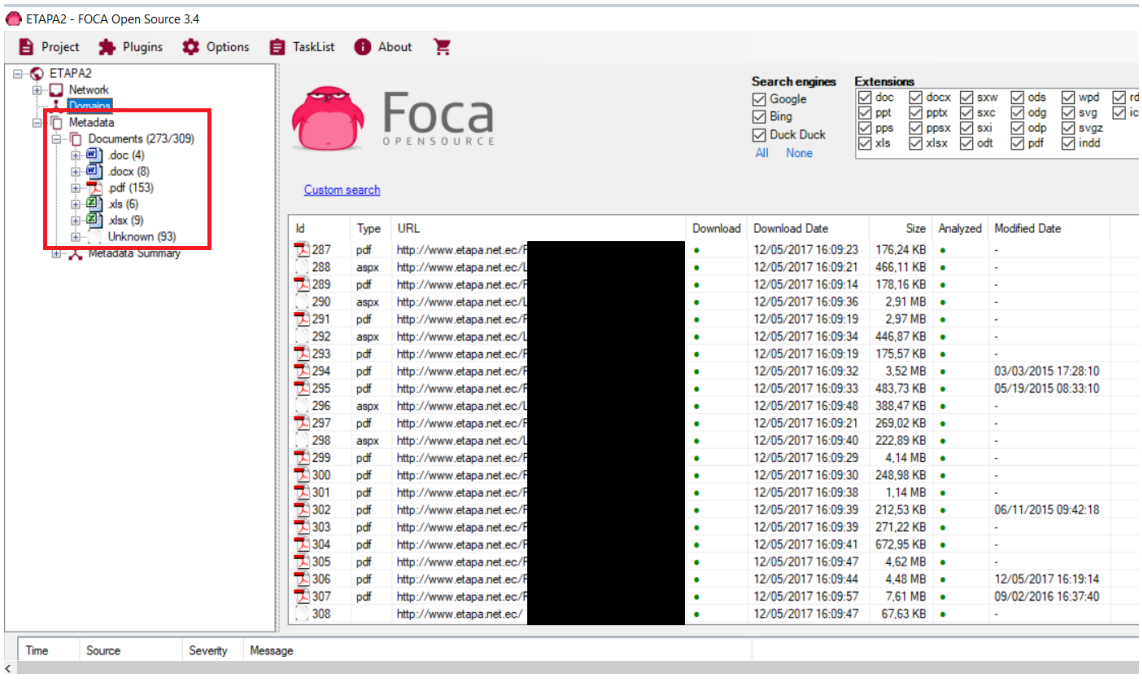


Figura 24. Extracción de metadatos de documentos en La FOCA.

Ahora seleccionamos todos los documentos y damos clic derecho, buscamos la opción “Analyze Metadata” y le damos clic.

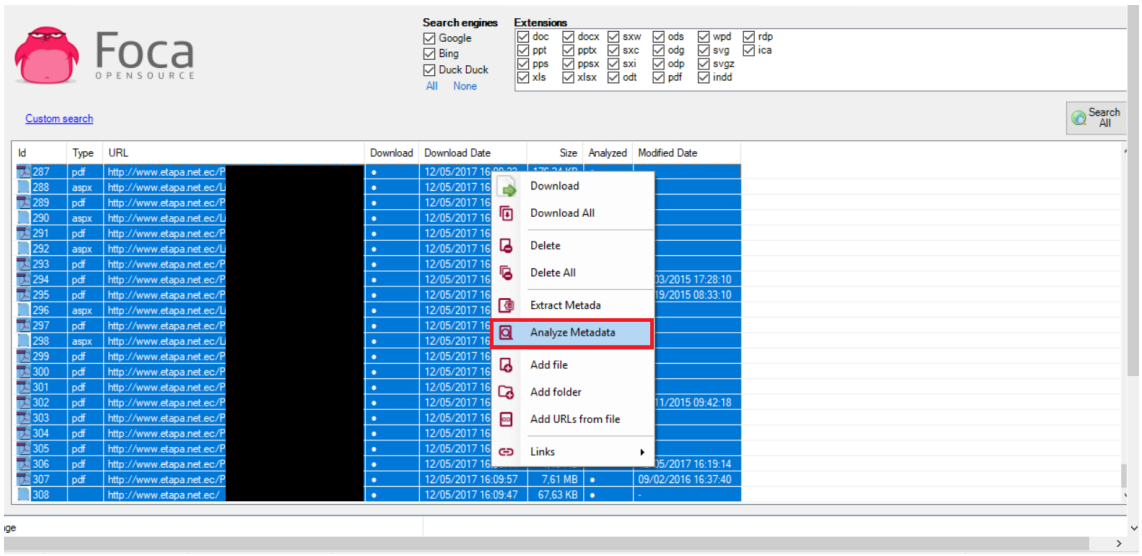


Figura 25. Análisis de metadatos de documentos en La FOCA.

Como se puede observar, el programa analiza por su cuenta todos los metadatos obtenidos de los documentos, y nos presenta en la parte izquierda toda la información obtenida de los mismo. Primero tenemos en Clientes, en este caso 26, que se refiere a la cantidad de usuarios que manipularon estos documentos.

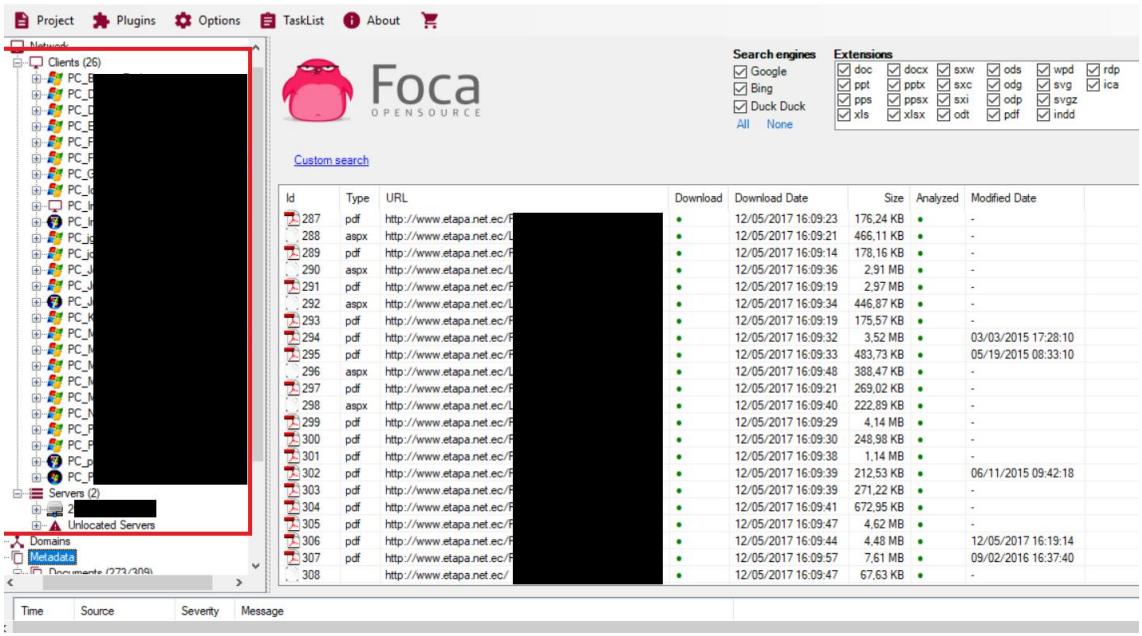


Figura 26. Análisis de metadatos de documentos en La FOCA.

Seleccionamos dentro de Clients, cualquiera de los equipos, solamente para una prueba, podemos observar que tenemos información de: el nombre de la persona, usuario en el sistema operativo, versión del sistema operativo, versión del software con el cual fue creado el documento, la última persona que modifico el documento y todos los usuarios que han modificado el mismo.

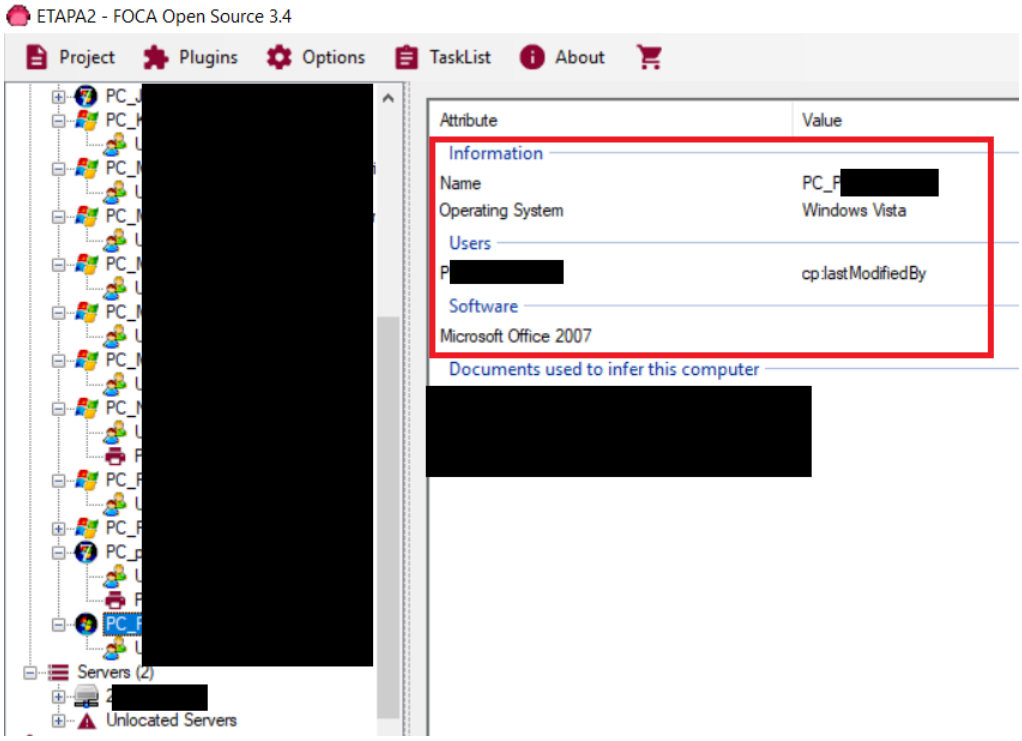


Figura 27. Análisis de metadatos de documentos en La FOCA.

Vamos a “Metadata Summary”, aquí desplegamos el menú y tenemos toda la información que se puede obtener, en este caso vamos a “Users” y damos clic, podemos ver que tenemos 33 usuarios encontrados entre los 26 documentos analizados.

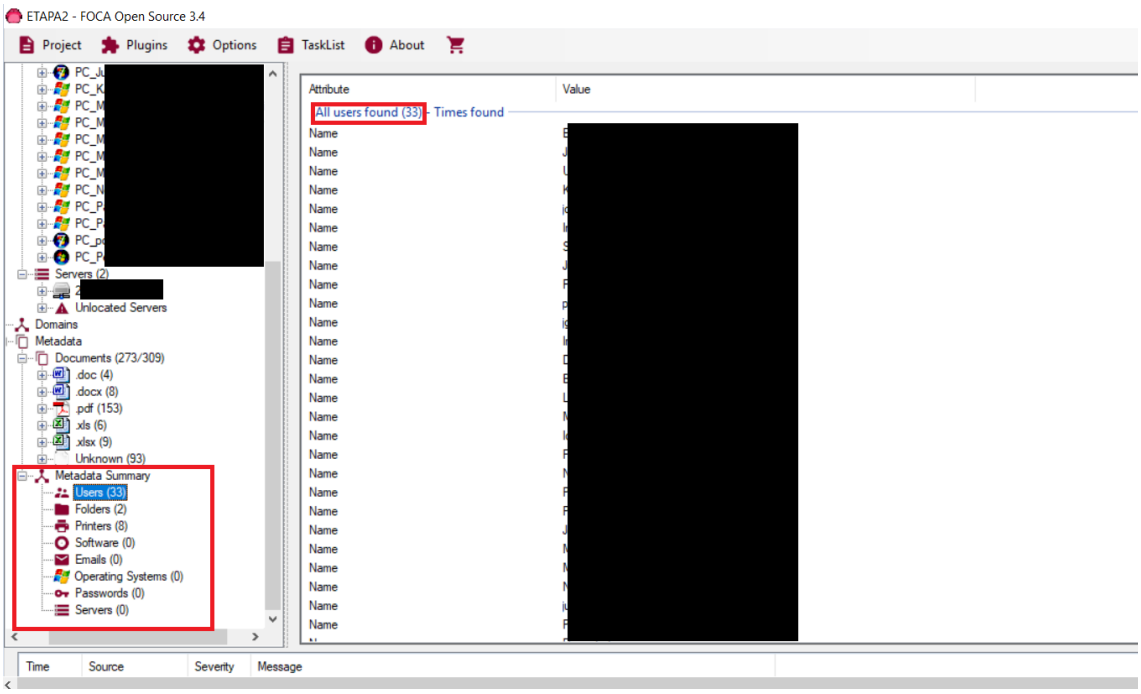


Figura 28. Análisis de metadatos de documentos en La FOCA.

En la opción de carpetas, podemos encontrar las direcciones posiblemente de almacenamiento, indexadas a estos archivos, en este caso tenemos 2 direcciones.

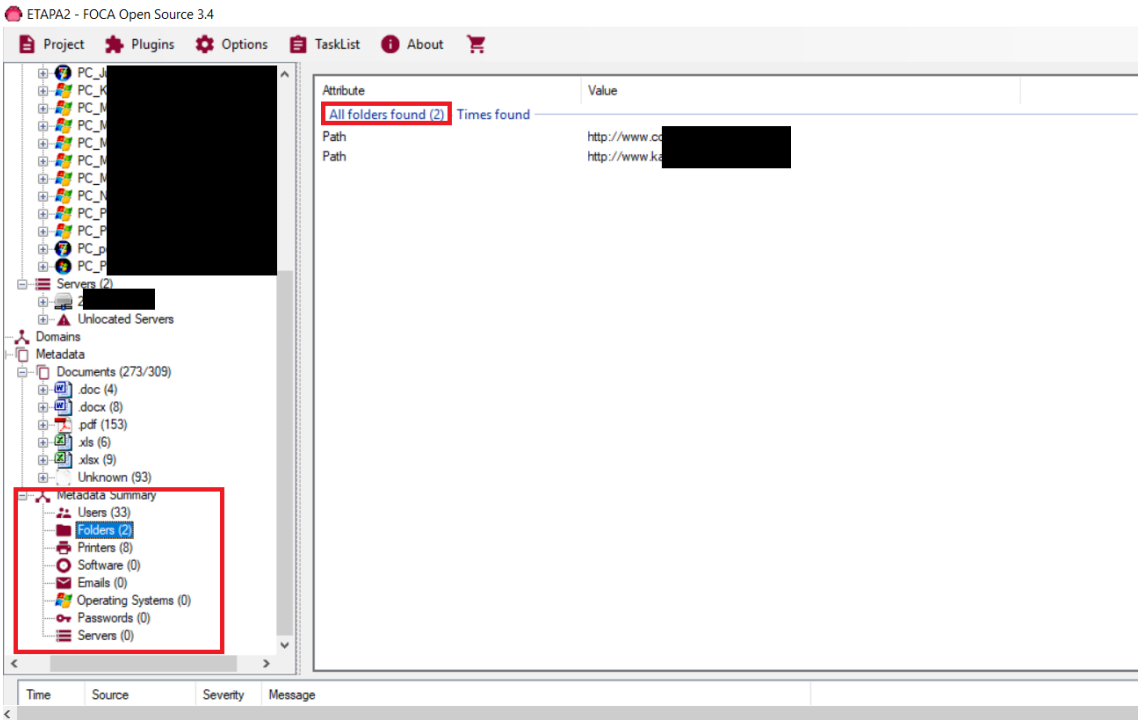


Figura 29. Análisis de metadatos de documentos en La FOCA.

En la opción de impresoras podemos ver que se tiene el nombre de las impresoras conectadas a los equipos con los que fueron creados los documentos.

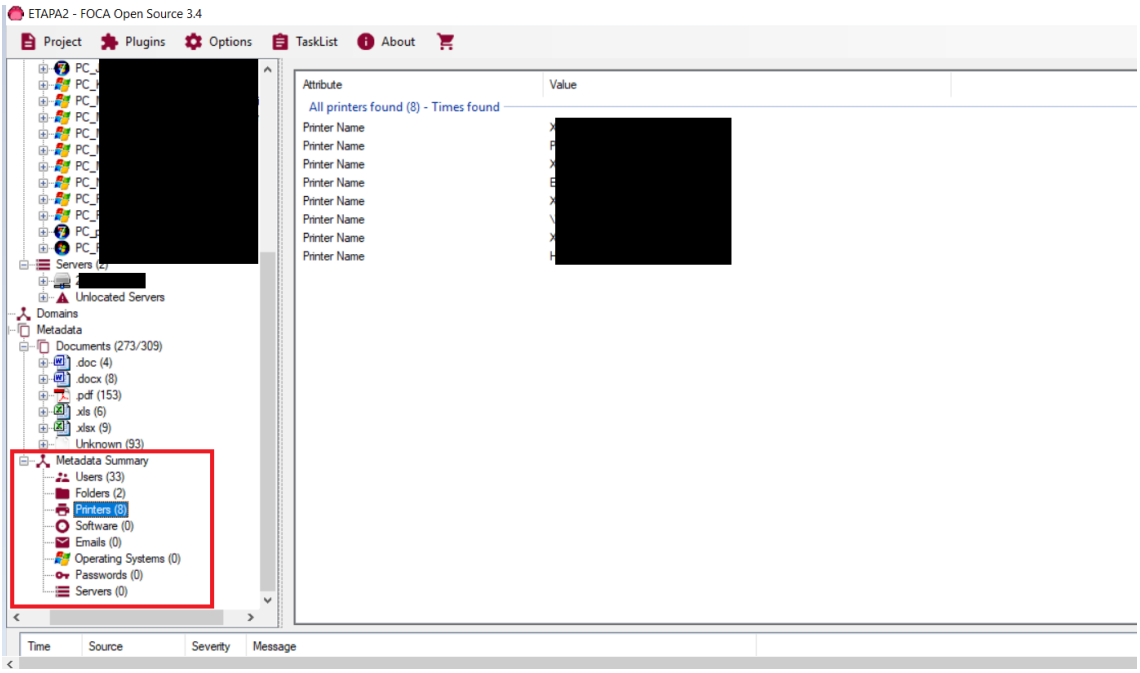


Figura 30. Análisis de metadatos de documentos en La FOCA.

Y de esta manera podemos revisar las demás opciones como son las versiones del software que se utiliza, los mails, sistemas operativos, passwords almacenados, servidores conectados, etc.

3.4 Análisis de metadatos en documentos públicos en entidades públicas de Cuenca

A todos los documentos públicos de las entidades públicas seleccionadas se les realizará el proceso anterior (3.3 Funcionamiento de La FOCA), este proceso para encontrar los metadatos y posteriormente se procederá a mostrar los resultados obtenidos con cada una de las entidades estatales.

3.4.1 Etapa

Dirección web: http://www.etapa.net.ec/

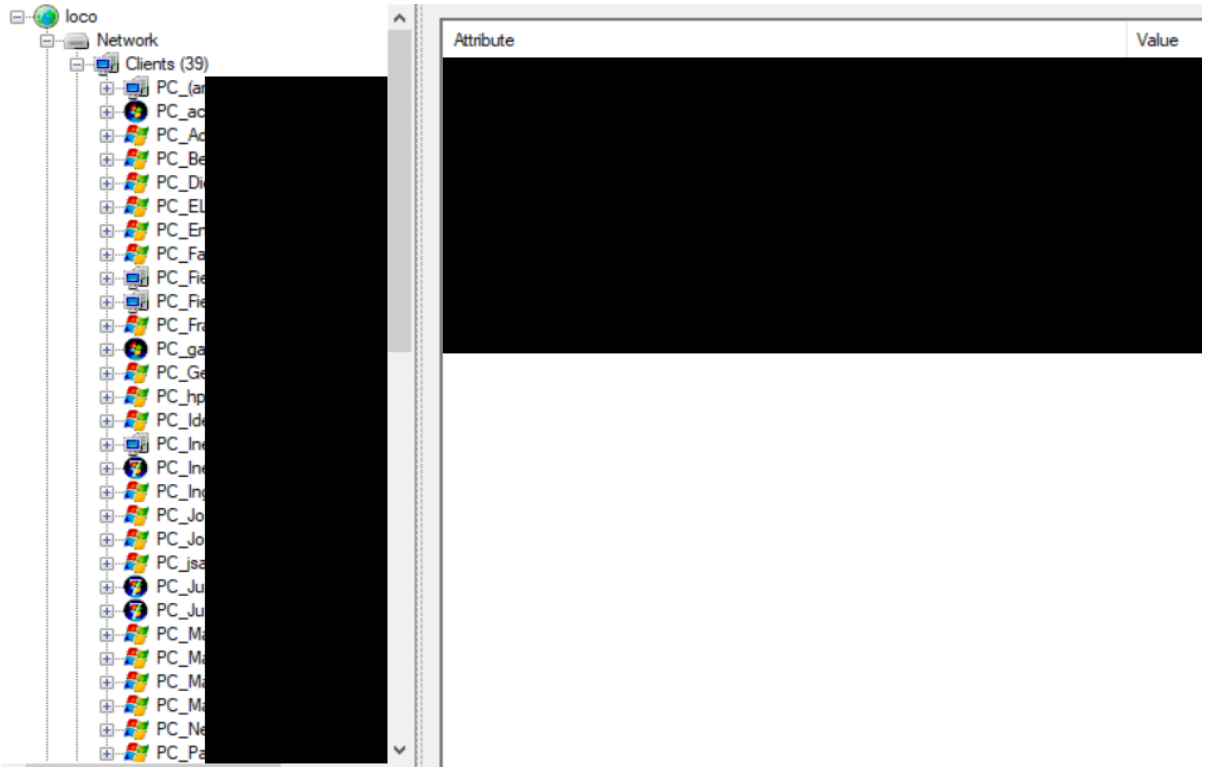


Figura 31. Equipos descubiertos en ETAPA.

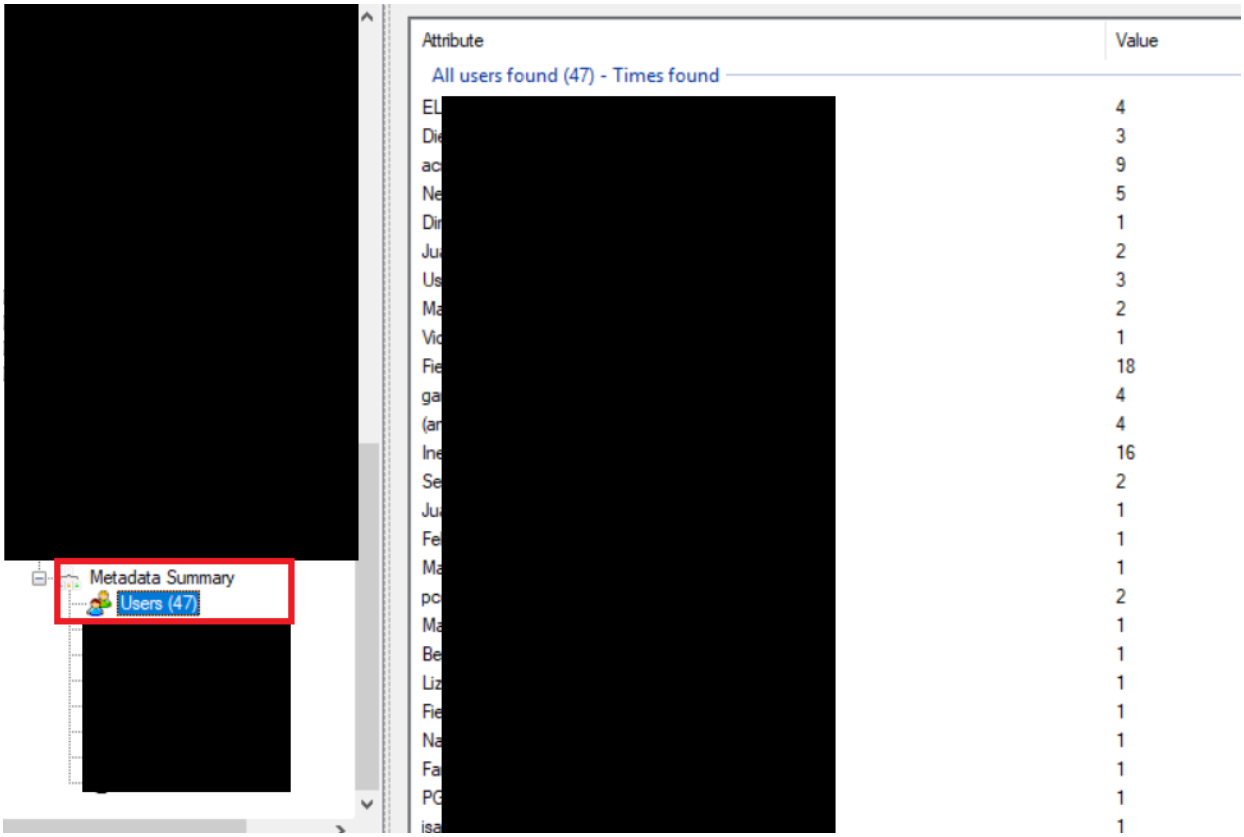


Figura 32. Usuarios descubiertos en ETAPA.

Dispositivo	Cantidad	Sistema Operativo
Equipos	39	Windows
	4	Windows Vista
	7	Windows 7
	27	Otra Versión de Windows
	1	Macintosh
Usuarios	47	

Tabla 1. Datos de equipos descubiertos en ETAPA.

En la Figura 31 y Figura 32. Tenemos los datos de los equipos y los usuarios encontrados en ETAPA, datos similares a los que se encuentran en la Tabla 1, que es una tabla donde se resume los datos de las 2 Figuras anteriores.

Como podemos observar en la Tabla 1, en ETAPA, logramos obtener los datos de 39 equipos utilizados para crear los documentos que fueron subidos a su sitio web, y tenemos la información de 47 usuarios, por lo tanto, se puede saber que al menos 8 de esos 47 usuarios comparten un mismo equipo, eso quiere decir que existe más de un usuario por equipo, en algunos equipos. Lo que permitiría hacer más fácil un ataque informático, pues existe mayor superficie de exposición. Cerca del 98% de las maquinas utilizadas para subir archivos a su sitio web son Windows, cerca del 10% de estas máquinas Windows son Windows Vista, 18% son Windows 7 y el resto son otra versión Superior de Windows. Solamente una máquina de todos sus equipos es Macintosh.

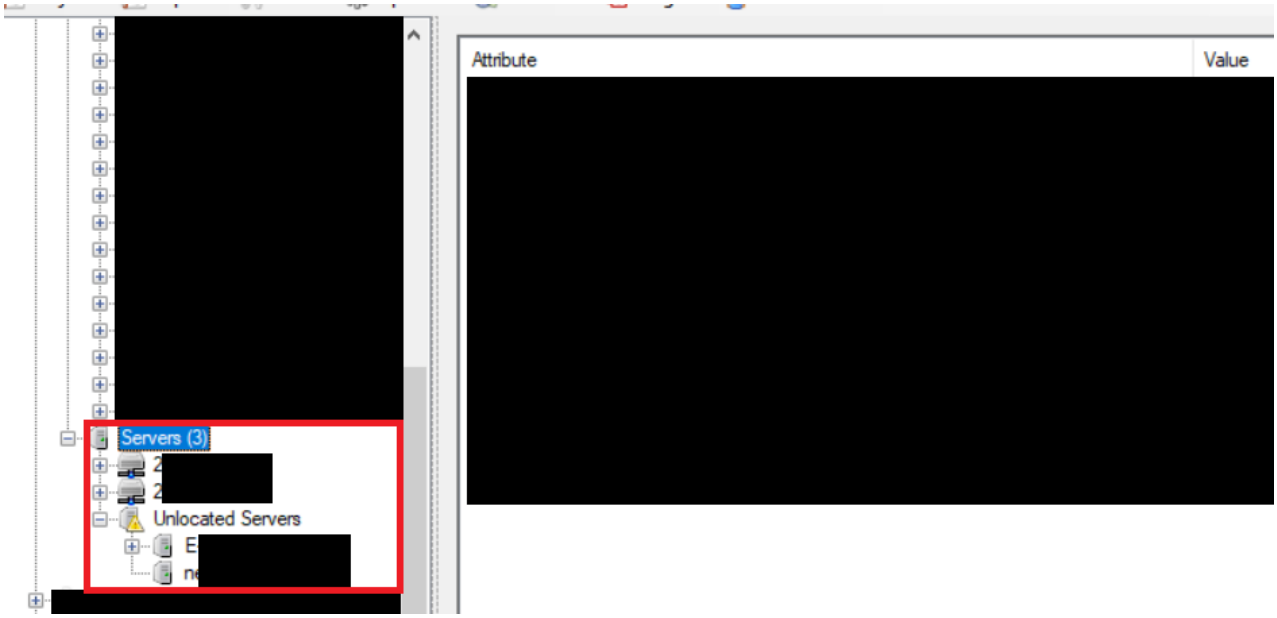


Figura 33. Servidores descubiertos en ETAPA.

Dispositivo	Cantidad	Locación
Servidor	4	Dirección IP y No Asignado
	2	Servidores con Dirección IP
	2	Sin Dirección Asignada

Tabla 2. Datos de servidores descubiertos en ETAPA.

En la Figura 33. Tenemos los datos de los servidores encontrados en ETAPA, los mismos datos que se encuentran en la Tabla 2, que es una tabla donde se resume datos similares que se pueden apreciar en la Figura 33.

Como podemos observar en la Tabla 2, en ETAPA, logramos obtener los datos de 4 servidores conectados, tanto externos como internos. De los cuales 2 servidores logramos observar las direcciones ip. De los otros 2 servidores no se logra obtener la dirección ip, pero si el nombre y por supuesto se conoce que tiene conexión con las computadoras en la empresa, por lo que se puede asumir que son servidores internos de la empresa.

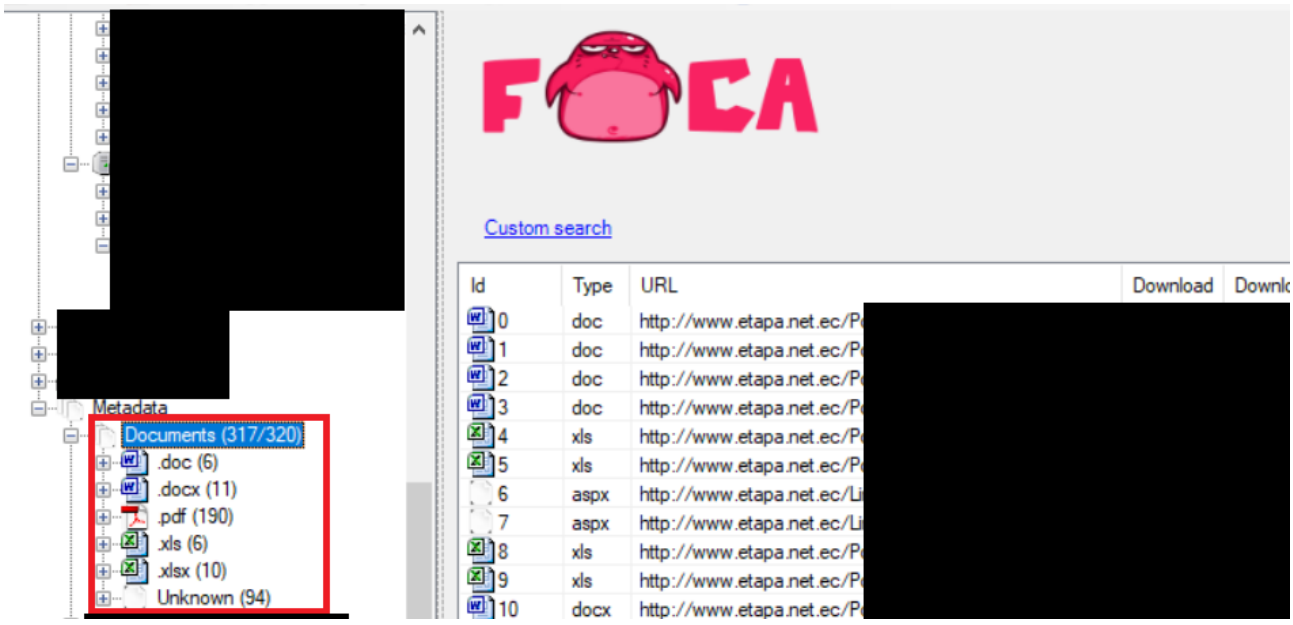


Figura 34. Documentos descubiertos en ETAPA.

En la Figura 34. Tenemos los datos de los documentos encontrados en ETAPA. Logramos obtener los datos de 320 documentos indexados a su sitio web. De los cuales: 17 son documentos de Word que representan un poco más del 5%, 16 son documentos de Excel que representan el 5%, 190 son documentos PDF que representan el 59% de los documentos, el resto son documentos de un formato desconocido. Esto quiere decir que en su mayoría los documentos son PDF, por lo que podemos entender que la mayoría de documentos que se generan en la empresa son de este tipo de documento, entonces deberíamos enfocarnos en el software que utilizan para crear este tipo de documentos para buscar fallos de seguridad en estos programas.

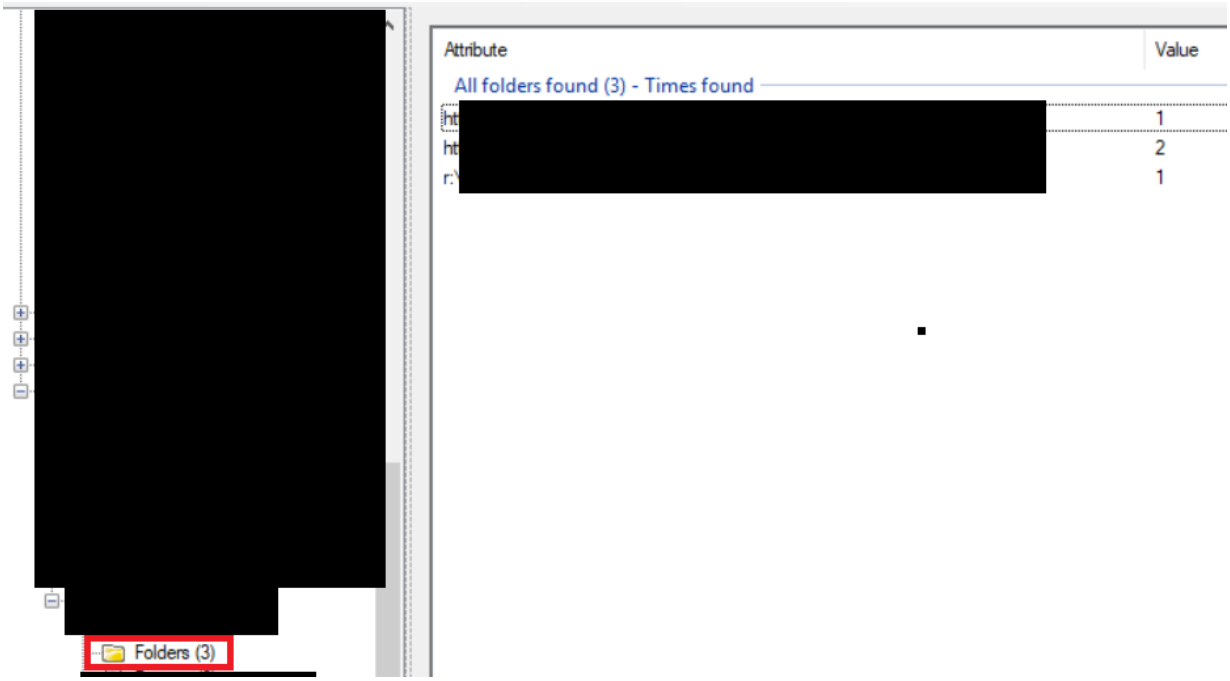


Figura 35. Directorios descubiertos en ETAPA.

Tipo	Cantidad	Cantidad Directorios en Documentos
Directorio	3	4

Tabla 3. Datos de directorios descubiertos en ETAPA.

En la Figura 35. Tenemos los datos de los directorios encontradas en ETAPA, los mismos datos que se encuentran en la Tabla 3, la misma resume datos similares que se pueden apreciar en la Figura 35.

Como podemos observar en la Tabla 3, en ETAPA, logramos obtener los datos de 3 directorios indexadas en los documentos de publicados en el sitio web de ETAPA, estos 3 directorios fueron indexadas en 4 documentos, lo que permite conocer directorios (folders) hacia los cuales los trabajadores de ETAPA que publican los documentos se conectan y los metadatos almacenados en sus documentos.

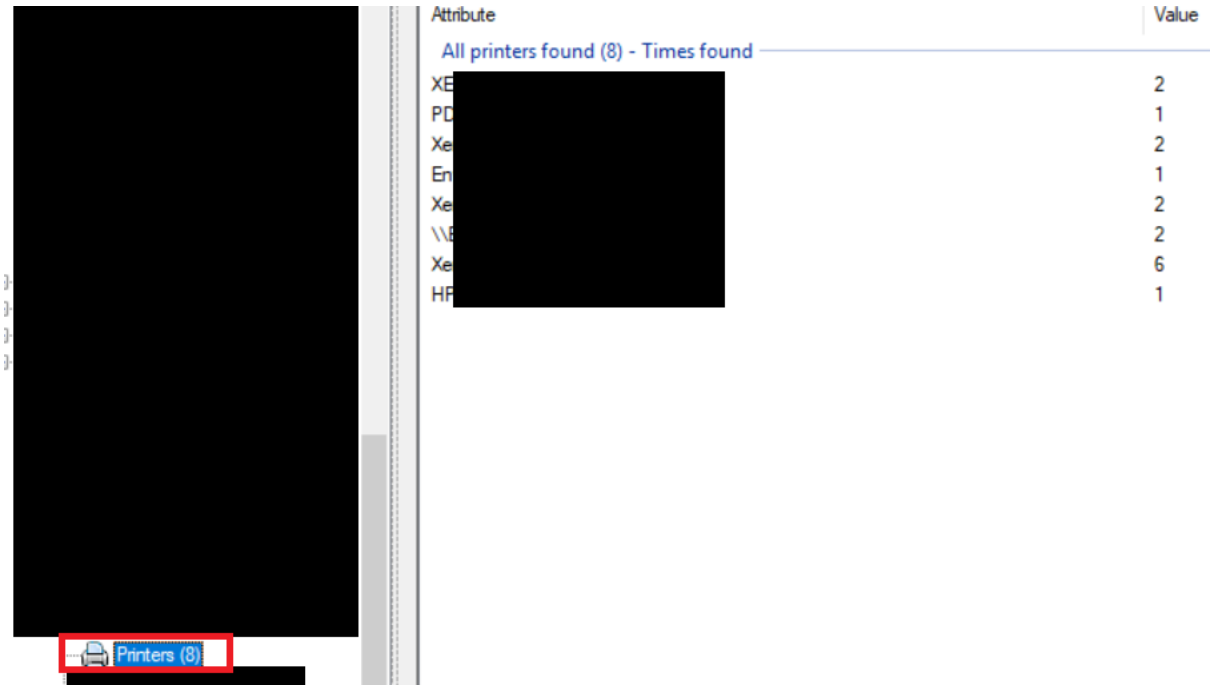


Figura 36. Impresoras descubiertas en ETAPA.

Dispositivo	Cantidad	Veces Adjuntadas a los Archivos
Impresora	8	17

Tabla 4. Datos de impresoras descubiertas en ETAPA.

En la Figura 36. Tenemos los datos de las impresoras encontradas en ETAPA, los mismos datos que se encuentran en la Tabla 5, la misma resume datos similares que se pueden apreciar en la Figura 36.

Como podemos observar en la Tabla 5, en ETAPA, logramos obtener los datos de 8 impresoras localizas en ETAPA, presenten en 17 de sus documentos subidos a internet. Las impresoras permiten a los atacantes conocer los fallos de seguridad en estos equipos y convertirse en vectores de ataque. Además de saber que personas comparten un mismo espacio físico en un área determinada.

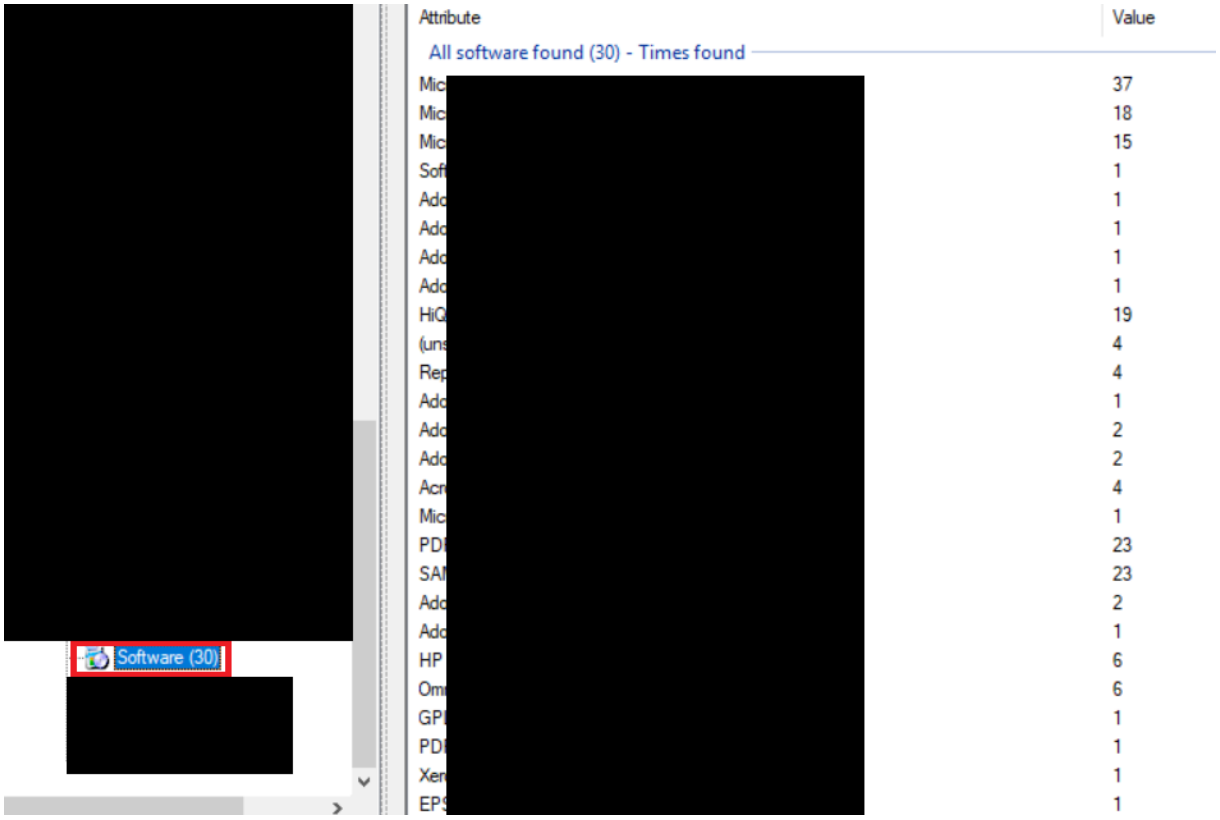


Figura 37. Software descubierto en ETAPA.

Nombre	**Cantidad de Apariciones en Documentos**
Microsoft Office	37
Microsoft Office XP	18
Microsoft Office 2007	15
Software de escaneo de documentos inteligentes HP	1
Adobe PDF Library 15.00	1
Adobe Illustrator CC 2015 (Macintosh)	1
Adobe PDF Library 10.0.1	1
Adobe InDesign CS6 (Macintosh)	1

HiQPdf 5.7	19
ReportLab PDF Library	4
Adobe Photoshop CS6	1
Adobe PDF Library 9.0	2
Adobe InDesign CS4 (6.0)	2
Acrobat Distillier 7.0	4
Microsoft Office 95	1
PDFsam Basic v3.0.2.RELEASE	23
SAMBox 1.0.0.M23 (www.sejda.org)	23
Adobe PDF Library 10.01	2
Adobe Illustrator CS6 (Windows)	1
HP Smart Document Scan Software 2.70	6
GPL Ghostscript 9.02	1
PDFCreator 1.2.2Windows	1
Win2PDF	1
PDFlib 3.03	1
Adobe Illustrator CS6 (Macintosh)	1
PScript5.dll Version 5.2	3

Tabla 5. Datos de software descubierto en ETAPA.

En la Figura 37. Tenemos los datos del software encontrado en ETAPA, los mismos datos que se encuentran en la Tabla 6, la misma resume datos similares que se pueden apreciar en la Figura 37, pero con la diferencia que en esta tabla se presentan menos datos

que en la Figura 37. El software indexa falsos positivos, y en esta tabla están solamente los datos del software eliminando estos falsos positivos.

Como podemos observar en la Tabla 6, en ETAPA, logramos obtener los datos del software que se utilizada en ETAPA. Tenemos que entender bien la indexación de estos datos, pues como podemos apreciar en cifrar se puede ver que existe una mayor cantidad de apariciones del Software Microsoft Office, y se podría pensar que la mayoría de documentos indexados a la página igualmente debería ser de extensión: docx, xlxs, y más extensión de Office, pero no es así.

El por qué es simple, estos documentos son creados con las herramientas de Microsoft Office, pero para mayor facilidad de distribución y lectura de los usuarios son transformados a PDF. Es por esto que la mayoría de documentos como podemos apreciar en la Figura 34 son PDF.

Una vez que se tiene la versión del software con el que se crean los documentos, cualquier pirata informático pudiera tomar esta información y conseguir el exploit para explotar esta vulnerabilidad.

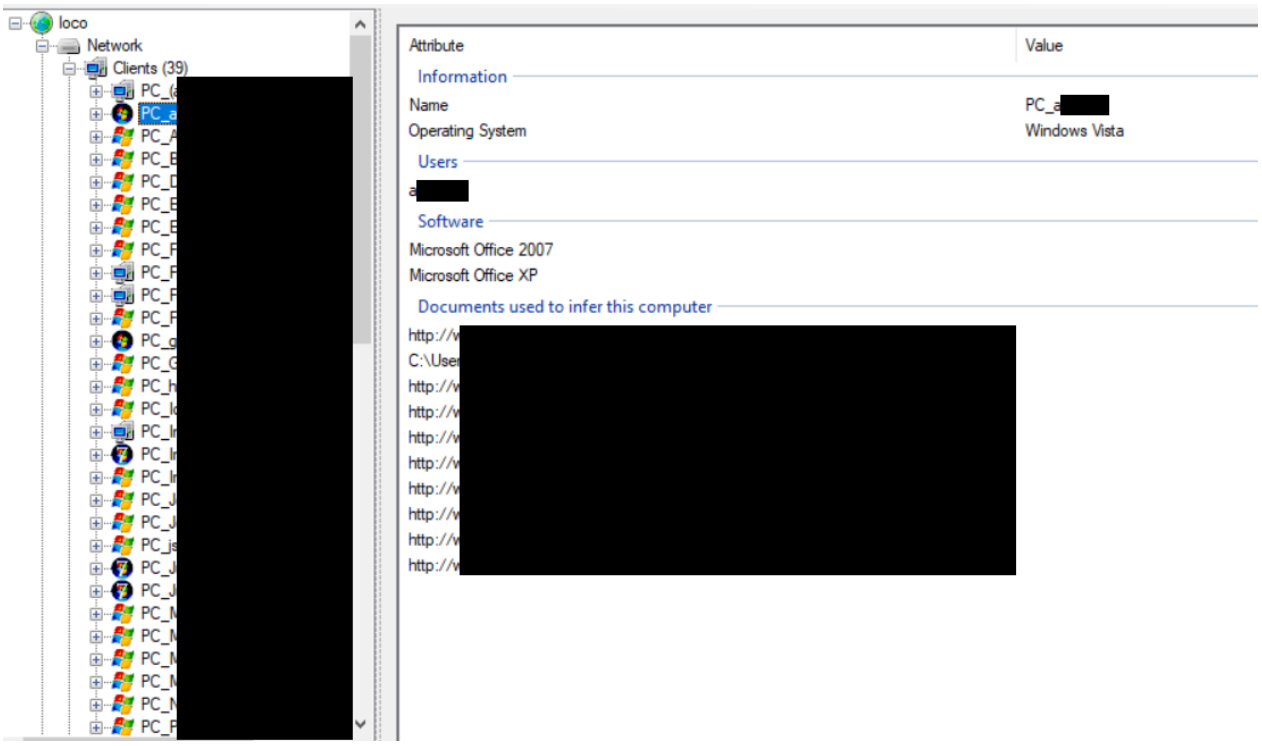


Figura 38. Detalle de información de un equipo descubierto en ETAPA.

En la Figura 38. Podemos apreciar que se ha seleccionado un equipo de la toda la lista de equipos de ETAPA, solamente por medios de investigación para conocer más a profundidad toda la información que se puede obtener de un usuario y su máquina.

Podemos conocer el nombre del usuario de esa máquina, por lo tanto, el nombre de la persona que trabaja en ETAPA, en caso de ser más de uno se podrá visualizar los usuarios pertenecientes a esa máquina. El sistema operativo que tiene esa máquina, en este caso Windows Vista. El software con el que se crea los documentos en este equipo, como son Microsoft Office 2007 Y Microsoft XP. Además de los documentos que han sido creados desde este equipo, este es un punto muy importante pues podemos ver de qué tipo son los archivos y por ejemplo si el enfoque de estos es netamente financiero podemos deducir que esta persona está en el área financiera de ETAPA. Finalmente, los archivos que se indexan desde el equipo almacenan direcciones internas del equipo, como se puede ver en la Figura 38. Se cita la ruta de donde se sacan los archivos, por lo tanto, tenemos la ruta del equipo, lo cual nos aporta más información, obviamente hemos difuminado toda la ruta por medidas de seguridad.

3.4.2 EMOV

Dirección web: http://www.emov.gob.ec/

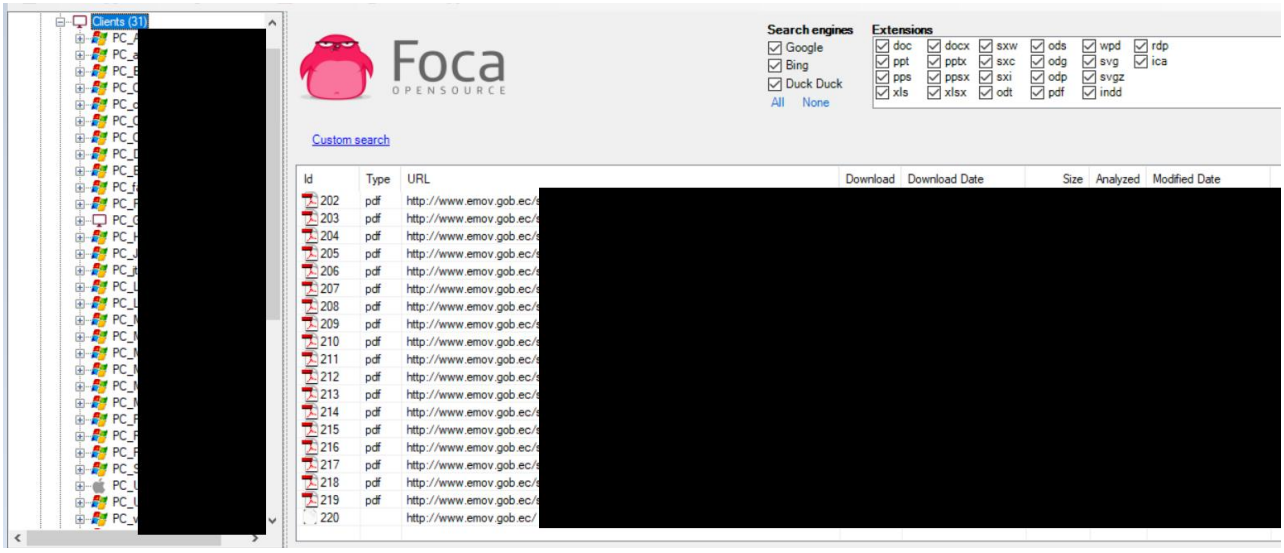


Figura 39. Equipos descubiertos en EMOV.

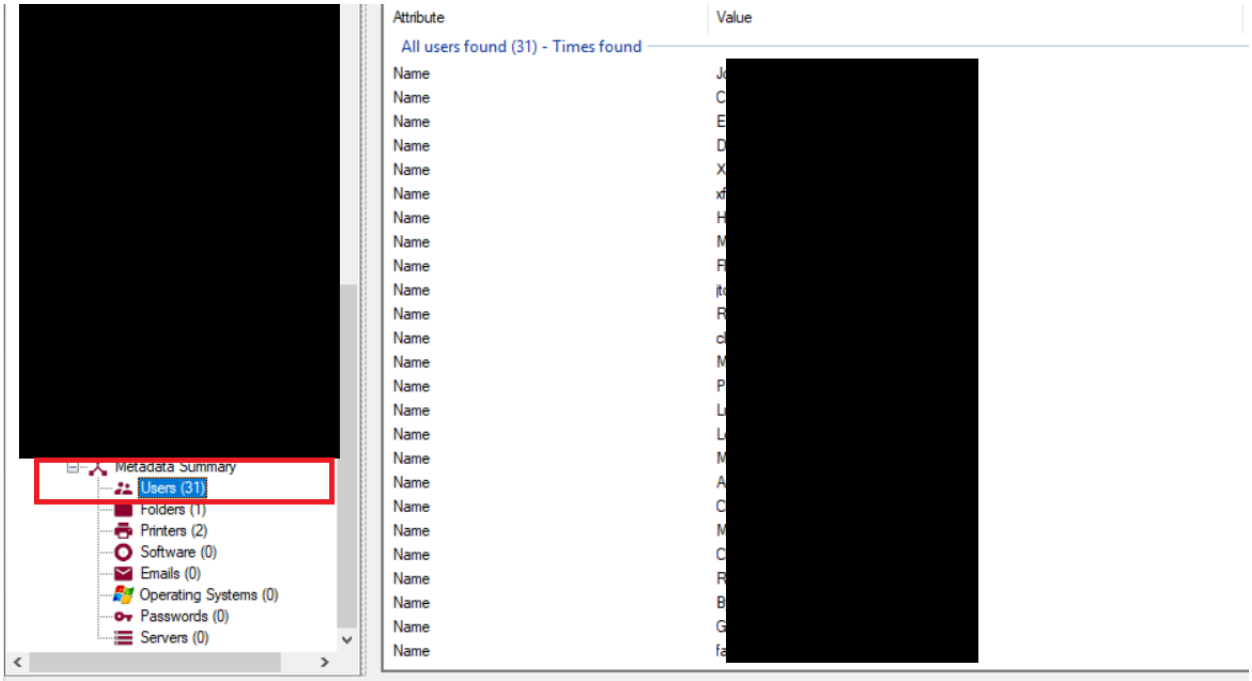


Figura 40. Usuarios descubiertos en EMOV.

Dispositivo	Cantidad	Sistema Operativo
Equipos	31	Windows
	1	Windows Vista
	29	Otra Versión de Windows
	1	Macintosh
Usuarios	31	

Tabla 6. Datos de equipos descubiertos en EMOV.

En la Figura 39 y Figura 40. Tenemos los datos de los equipos y los usuarios encontrados en la EMOV, datos similares a los que se encuentran en la Tabla 6, que es una tabla donde se resume los datos las 2 Figuras anteriores.

Como podemos observar en la Tabla 6, en la EMOV, logramos obtener los datos de 31 equipos utilizados para crear sus documentos que fueron subidos a su sitio web, y tenemos la información de 31 usuarios. Cerca del 97% de las maquinas utilizadas para subir archivos a su sitio web son Windows, cerca del 3% de estas máquinas Windows, son Windows Vista, 94% son otra versión Superior de Windows. Solamente una máquina de todos sus equipos es Macintosh lo que representa el 3%. Además, se conoce que se tiene una maquina destinada al soporte en EMOV, de la cual se conoce información privilegiada, y una maquina registrada con el nombre de EMOV, que es la máquina que más documentos genera, se puede deducir que es la maquina encargada de subir la mayoría de documentos.

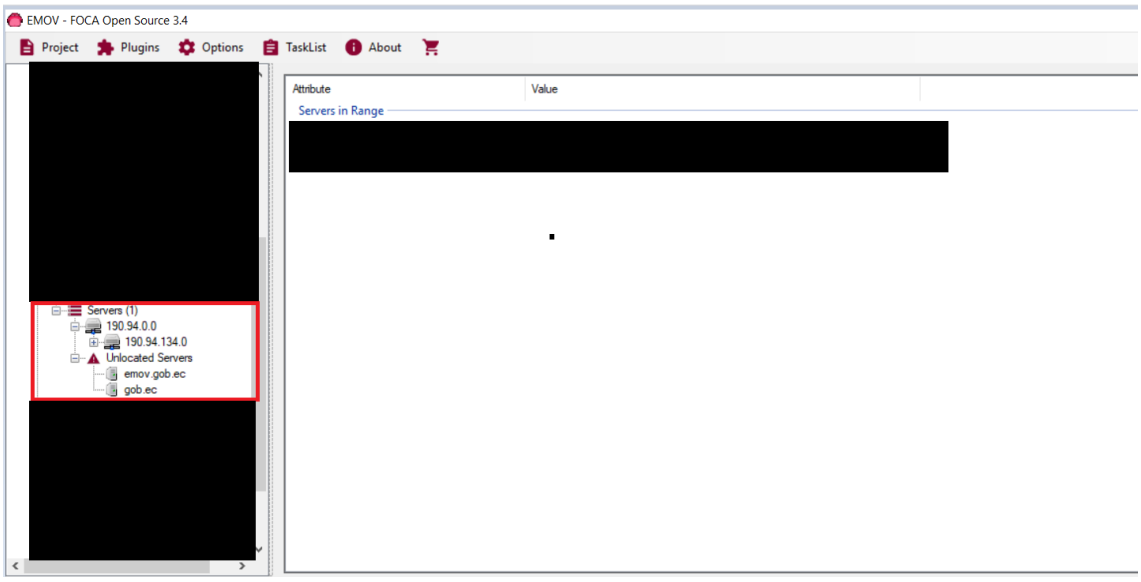


Figura 41. Servidores descubiertos en EMOV.

Dispositivo	Cantidad	Locación
Servidor	3	Dirección IP y No Asignado
	1	Servidores con Dirección IP
	2	Sin Dirección Asignada

Tabla 7. Datos de servidores descubiertos en EMOV.

En la Figura 41. Tenemos los datos de los servidores encontrados en la EMOV, los mismos datos que se encuentran en la Tabla 7, que es una tabla donde se resume datos similares que se pueden apreciar en la Figura 41 con un contexto más comprensible.

Como podemos observar en la Tabla 7, en la EMOV, logramos obtener los datos de 3 servidores conectados, tanto externos como internos. De los cuales de 1 servidor logramos observar la dirección ip. De los otros 2 servidores no se logra obtener la dirección ip, pero si el nombre y por supuesto se conoce que tiene conexión con las computadoras en la empresa, por lo que se puede asumir que son servidores internos de la empresa.

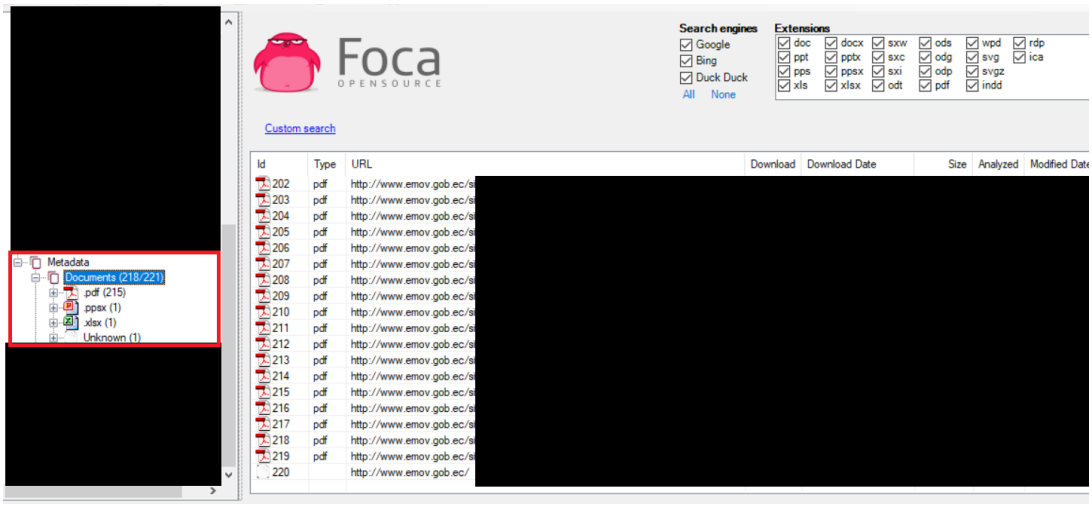


Figura 42. Documentos descubiertos en EMOV.

En la Figura 42. Tenemos los datos de los documentos encontrados en la EMOV. Logramos obtener los datos de 221 documentos indexados a su sitio web. De los cuales: 1 es un documento de Excel que representa el 0.43%, 1 es un documento de Power Point que representa el 0.43%, 215 son documentos PDF que representan el 97.28% de los documentos, el resto son documentos de un formato desconocido. Esto quiere decir que en su mayoría los documentos son PDF, por lo que podemos entender que la mayoría de documentos que se generan en la empresa son de este tipo de documento, entonces deberíamos enfocarnos en el software que utilizan para crear este tipo de documentos para buscar fallos de seguridad en estos programas.

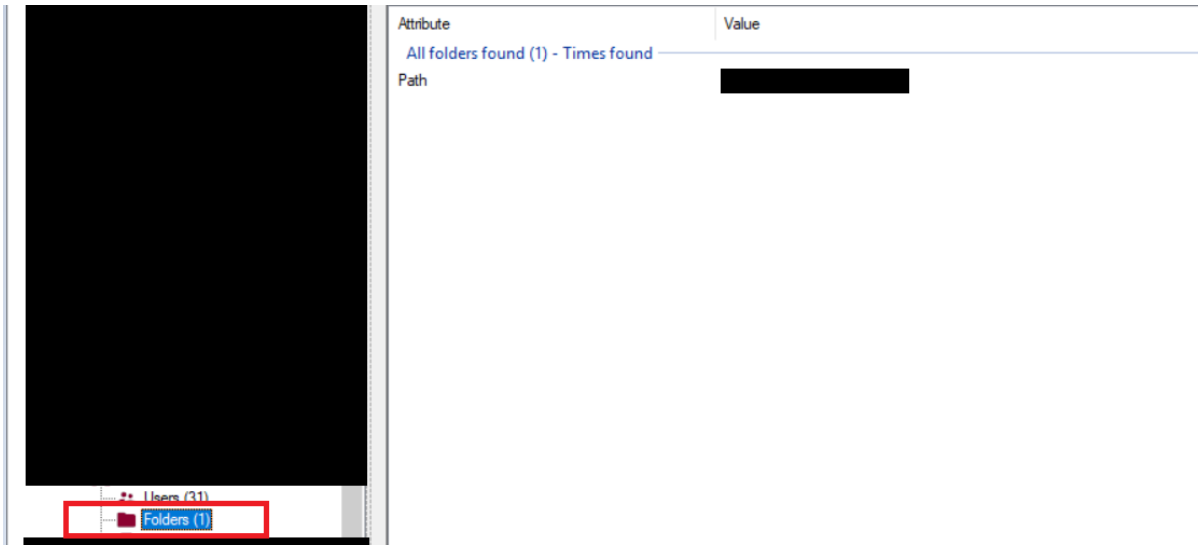


Figura 43. Directorios descubiertos en EMOV.

Tipo	Cantidad	Cantidad Directorios en Documentos
Directorio	1	1

Tabla 8. Datos de directorios descubiertos en EMOV.

En la Figura 43. Tenemos los datos de los directorios encontradas en EMOV, los mismos datos que se encuentran en la Tabla 8, la misma resume datos similares que se pueden apreciar en la Figura 43.

Como podemos observar en la Tabla 8, en EMOV, logramos obtener los datos de 1 directorio indexado en los documentos de publicados en el sitio web de la EMOV, este directorio fue indexado en 1 documento, lo que permite conocer directorios (folders) hacia los cuales los trabajadores de EMOV que publican los documentos se conectan y los metadatos almacenados en sus documentos. En este caso se conoce el directorio que incluso guarda información de la carpeta llamada TESIS, por lo que se puede asumir que este proyecto pudo ser un proyecto de grado de algún estudiante.

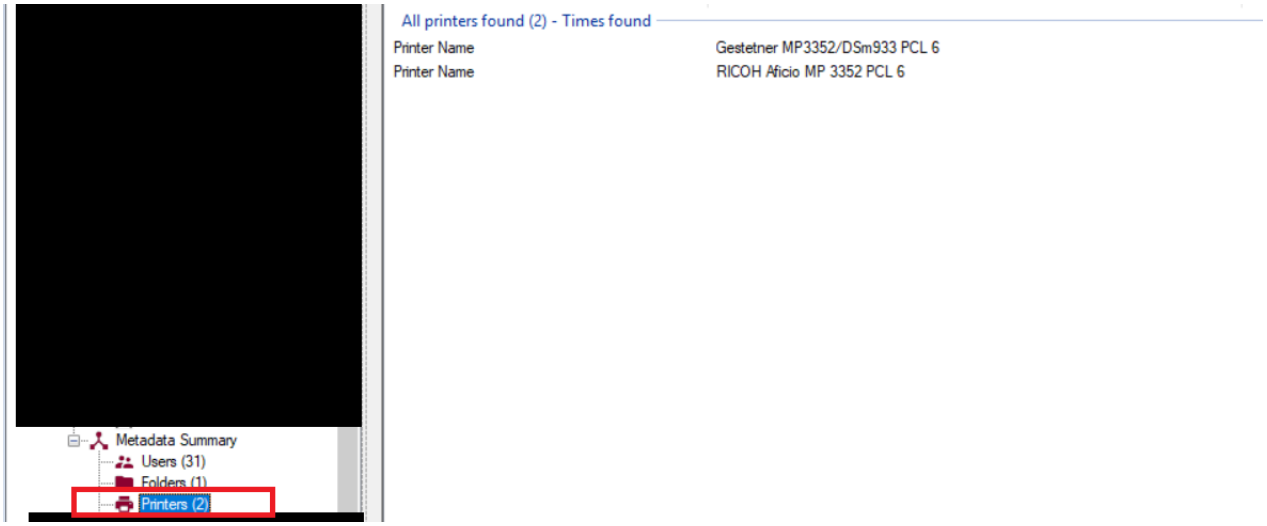


Figura 44. Impresoras descubiertas en EMOV.

Dispositivo	Cantidad	Veces Adjuntadas a los Archivos
Impresora	2	2

Tabla 9. Datos de impresoras descubiertas en EMOV.

En la Figura 44. Tenemos los datos de las impresoras encontradas en la EMOV, los mismos datos que se encuentran en la Tabla 9, la misma resume datos similares que se pueden apreciar en la Figura 44.

Como podemos observar en la Tabla 9, en la EMOV, logramos obtener los datos de 2 impresoras localizas en la EMOV, presenten en 2 de sus documentos subidos a internet. Las impresoras permiten a los atacantes conocer los fallos de seguridad en estos equipos y convertirse en vectores de ataque. Y las personas que comparten un mismo espacio físico en un área determinada.

Nombre	Cantidad de Apariciones en Documentos
Microsoft Office	144
Microsoft Office XP	5
Microsoft Office 2007	3
HP Smart Document Scan Software 3 3.10	10
OmniPageCSDK18	10
Adobe PDF Library 10.01	4
Adobe Illustrator CC (Windows)	2
GeneXus PDF Report Generator	1
iText 2.1.7 by 1T3XT	1
Adobe PDF Library 10.0.1	1

Adobe InDesign CS6 (Macintosh)	1
JasperReports	1
iText1.3.1	1
PDFium	1
Adobe Illustrator CS6 (Macintosh)	2
intsig.com pdf producer	1
Nitro Pro 8 (8. 0. 7. 3)	2
Nitro Pro	2
Nitro Pro 8	1

Tabla 10. Datos de software descubierto en EMOV.

En la Tabla 10. Tenemos los datos del software encontrado en la EMOV, en esta tabla se presentan menos datos que en los obtenidos por el software. El software indexa falsos positivos, y en esta tabla están solamente los datos del software eliminando estos falsos positivos.

Como podemos observar en la Tabla 10, logramos obtener los datos del software que se utilizada en la EMOV. Tenemos que entender bien la indexación de estos datos, pues como podemos apreciar en cifras, se puede ver que existe una mayor cantidad de apariciones del Software Microsoft Office, y se podría pensar que la mayoría de documentos indexados a la página igualmente debería ser de extensión: docx, xlxs, y más extensión de Office, pero no es así.

El por qué es simple, estos documentos son creados con las herramientas de Microsoft Office, pero para mayor facilidad de distribución y lectura de los usuarios son transformados a PDF. Es por esto que la mayoría de documentos como podemos apreciar en la Figura 42, son PDF.

Una vez que se tiene la versión del software con el que se crean los documentos, cualquier pirata informático podría tomar esta información y conseguir el exploit para explotar esta vulnerabilidad.

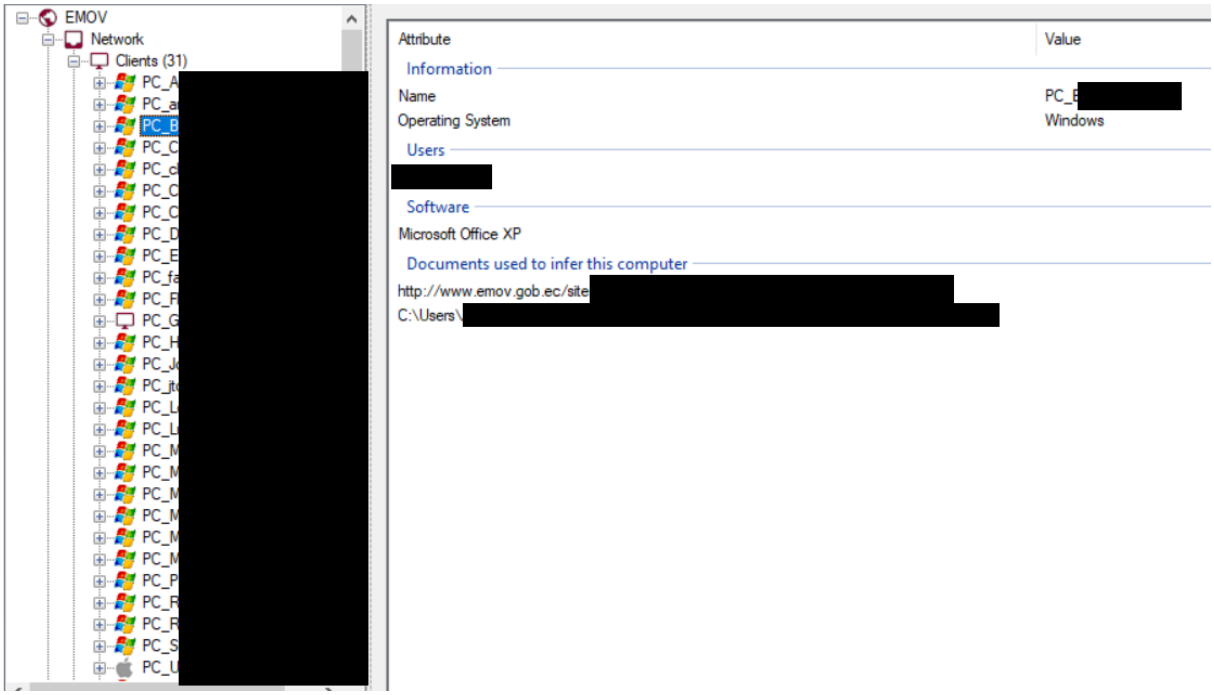


Figura 45. Detalle de información de un equipo descubierto en EMOV.

En la Figura 45. Podemos apreciar que se ha seleccionado un equipo de la toda la lista de equipos de la EMOV, solamente por medios de investigación para conocer más a profundidad toda la información que se puede obtener de un usuario y su máquina.

Podemos conocer el nombre del usuario de esa máquina, por lo tanto, el nombre de la persona que trabaja en la EMOV, en caso de ser más de uno, se podrá visualizar los usuarios pertenecientes a esa máquina. El sistema operativo que tiene esa máquina, en este caso Windows. El software con el que se crea los documentos en este equipo, como son Microsoft XP. Además de los documentos que han sido creados desde este equipo, este es un punto muy importante pues podemos ver de qué tipo son los archivos y por ejemplo si el enfoque de estos es netamente financiero podemos deducir que esta persona está en el área financiera de la EMOV. Finalmente, los archivos que se indexan desde el equipo almacena direcciones internas del equipo, como se puede ver en la Figura 43. Se cita la ruta de donde se sacan los archivos, por lo tanto, tenemos la ruta del equipo. Esto nos aporta más información, obviamente hemos difuminado toda la ruta por medidas de seguridad.

3.4.3 CENTROSUR

Dirección web: http://www.centrosur.gob.ec

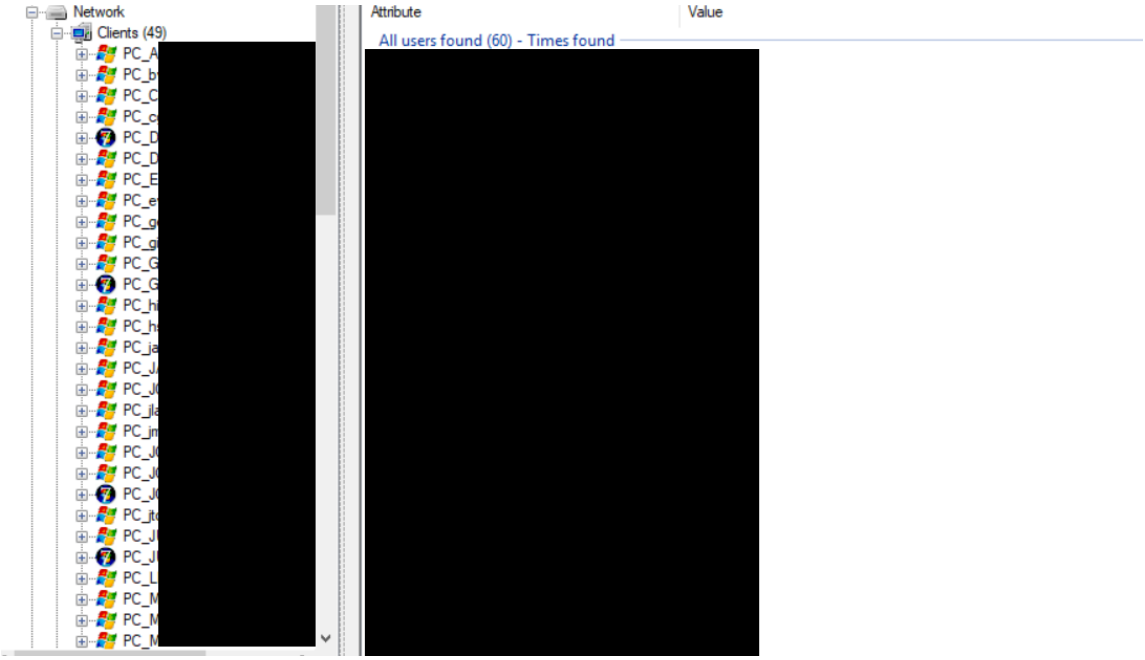


Figura 46. Equipos descubiertos en CENTROSUR.

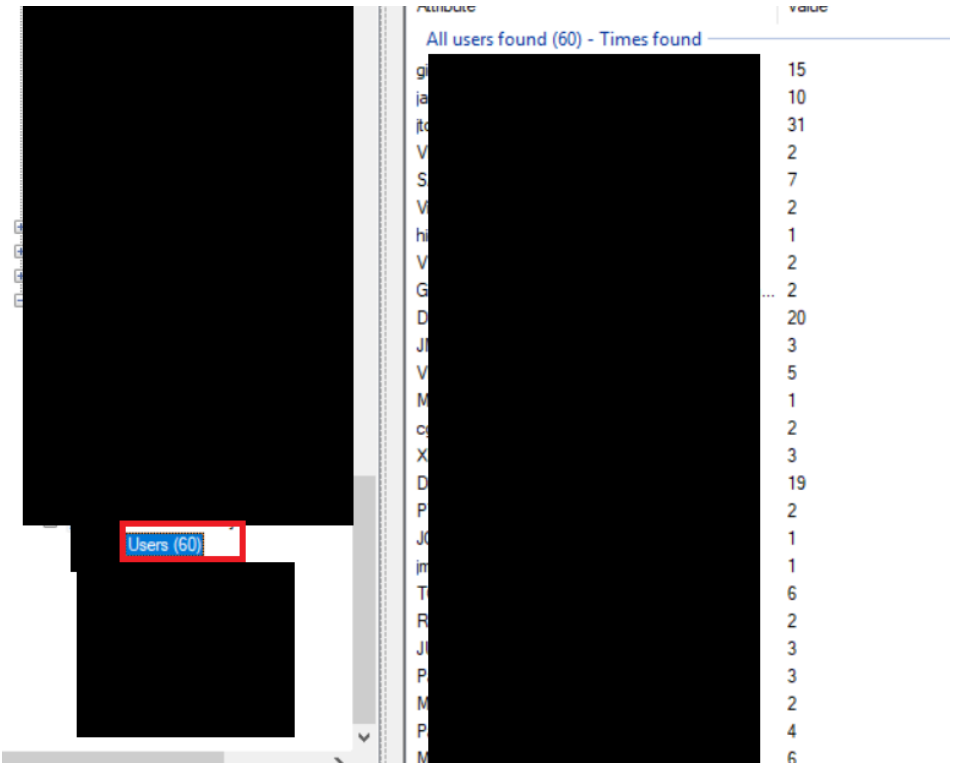


Figura 47. Usuarios descubiertos en CENTROSUR.

Dispositivo	Cantidad	Sistema Operativo
Equipos	49	Windows
	16	Windows 7
	32	Otra Versión de Windows
	1	Macintosh
Usuarios	60	

Tabla 11. Datos de equipos descubiertos en CENTROSUR.

En la Figura 46 y Figura 47. Tenemos los datos de los equipos y los usuarios encontrados en la CENTROSUR, datos similares a los que se encuentran en la Tabla 11, que es una tabla donde se resume los mismos datos que se puede apreciar en las 2 Figuras anteriores.

Como podemos observar en la Tabla 11, en la CENTROSUR, logramos obtener los datos de 49 equipos utilizados para crear sus documentos que fueron subidos a su sitio web, y tenemos la información de 60 usuarios. Cerca del 98% de las maquinas utilizadas para subir archivos a su sitio web son Windows, 32.65% de estas máquinas son Windows 7, 65.30% son otra versión Superior de Windows. Solamente una máquina de todos sus equipos es Macintosh lo que representa el 2%. Conociendo que la mayoría de sus equipos son Windows.

Figura 48. Servidores descubiertos en CENTROSUR.

Dispositivo	Cantidad	Locación
Servidor	8	Dirección IP y No Asignado
	8	Sin Dirección Asignada

Tabla 12. Datos de servidores descubiertos en CENTROSUR.

En la Figura 48. Tenemos los datos de los servidores encontrados en la CENTROSUR, los mismos datos que se encuentran en la Tabla 12, que es una tabla donde se resume datos similares que se pueden apreciar en la Figura 48 con un contexto más comprensible.

Como podemos observar en la Tabla 12, en la CENTROSUR, logramos obtener los datos 8 servidores, no se logra obtener la dirección ip, pero si el nombre y por supuesto se conoce que tiene conexión con las computadoras en la empresa. Por lo que se puede asumir que son servidores internos de la empresa. De estos 8 servidores se conoce cuáles son los usuarios que tienen acceso al mismo, por lo que, si nuestro vector de ataque son estos servidores, tenemos a los usuarios que serían nuestras victimas para el ataque.

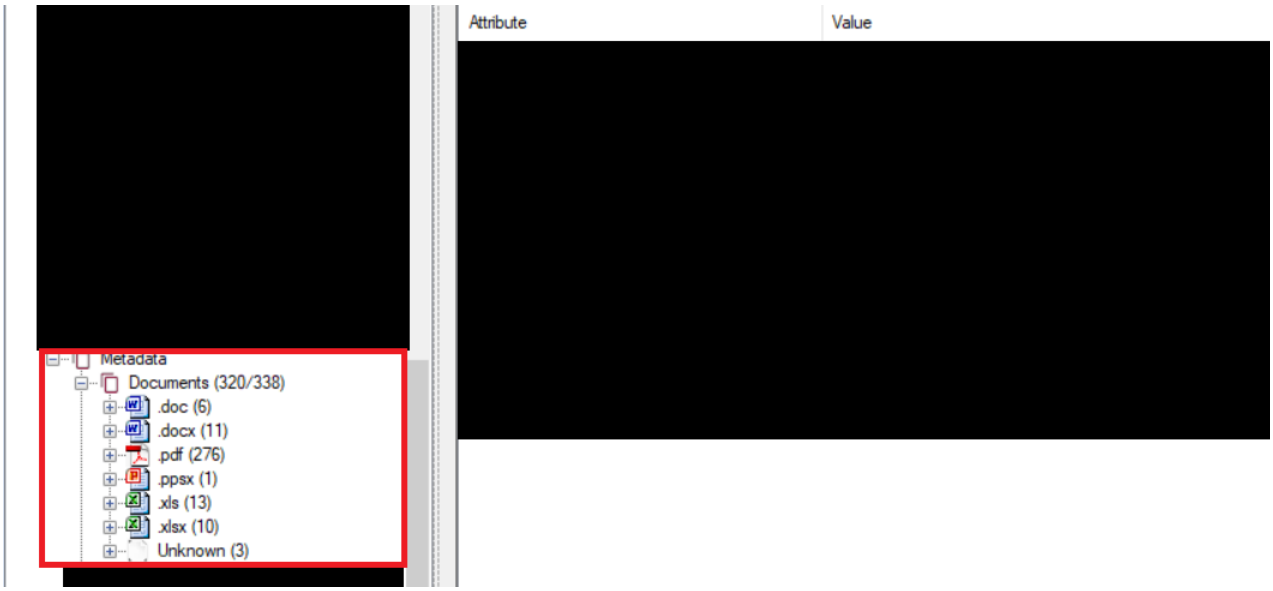


Figura 49. Documentos descubiertos en CENTROSUR.

En la Figura 49. Tenemos los datos de los documentos encontrados en la CENTROSUR. Logramos obtener los datos de 338 documentos indexados a su sitio web. De los cuales: 23 son documentos de Excel que representan el 6.80%, 1 es un documento de Power Point que representa el 0.29%, 17 son documentos de Word que representan el 5%, 276 son documentos PDF que representan el 81.65% de los documentos, el resto son documentos de un formato desconocido. Esto quiere decir que en su mayoría los documentos son PDF, por lo que podemos entender que la mayoría de documentos que se generan en la empresa son de este tipo de documento, entonces deberíamos enfocarnos en el software que utilizan para crear este tipo de documentos para buscar fallos de seguridad en estos programas.

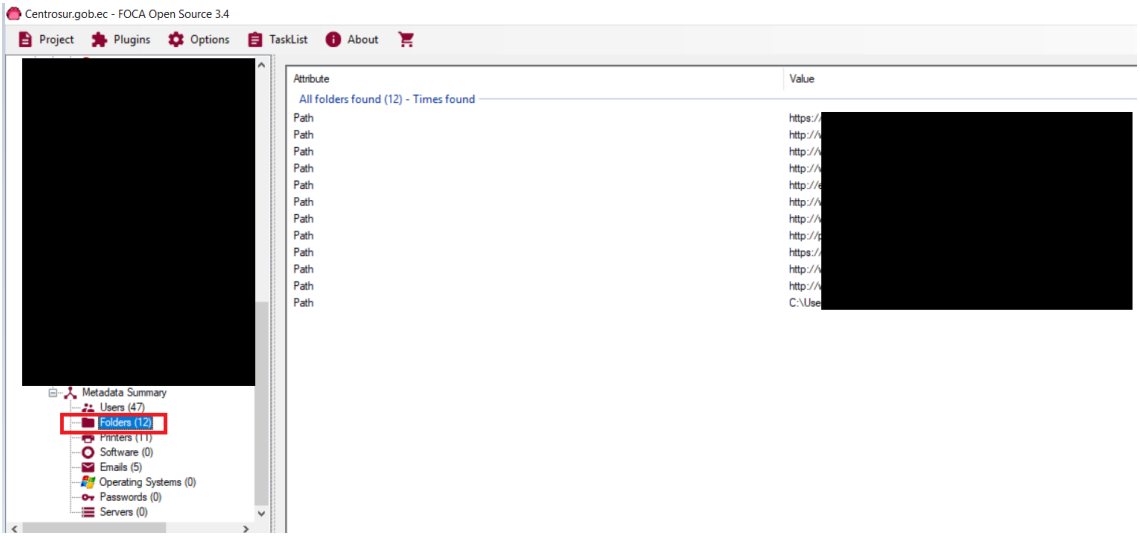


Figura 50. Directorios descubiertos en CENTROSUR.

Tipo	Cantidad	Cantidad Directorios en Documentos
Directorio	12	68

Tabla 13. Datos de directorios descubiertos en CENTROSUR.

En la Figura 50. Tenemos los datos de los directorios encontrados en la CENTROSUR, los mismos datos que se encuentran en la Tabla 13, la misma resume datos similares que se pueden apreciar en la Figura 50.

Como podemos observar en la Tabla 13, en la CENTROSUR, logramos obtener los datos de 12 directorios indexados en los documentos publicados en el sitio web de la CENTROSUR, estos directorios fueron indexados en 68 documentos, lo que permite conocer los directorios (folders) hacia los cuales los trabajadores de la CENTROSUR que publican los documentos se conectan y los metadatos almacenados en sus documentos. En estos documentos se almacenaron el directorio personal de un usuario, e incluso la información de la dirección de donde fue adquirido el software.

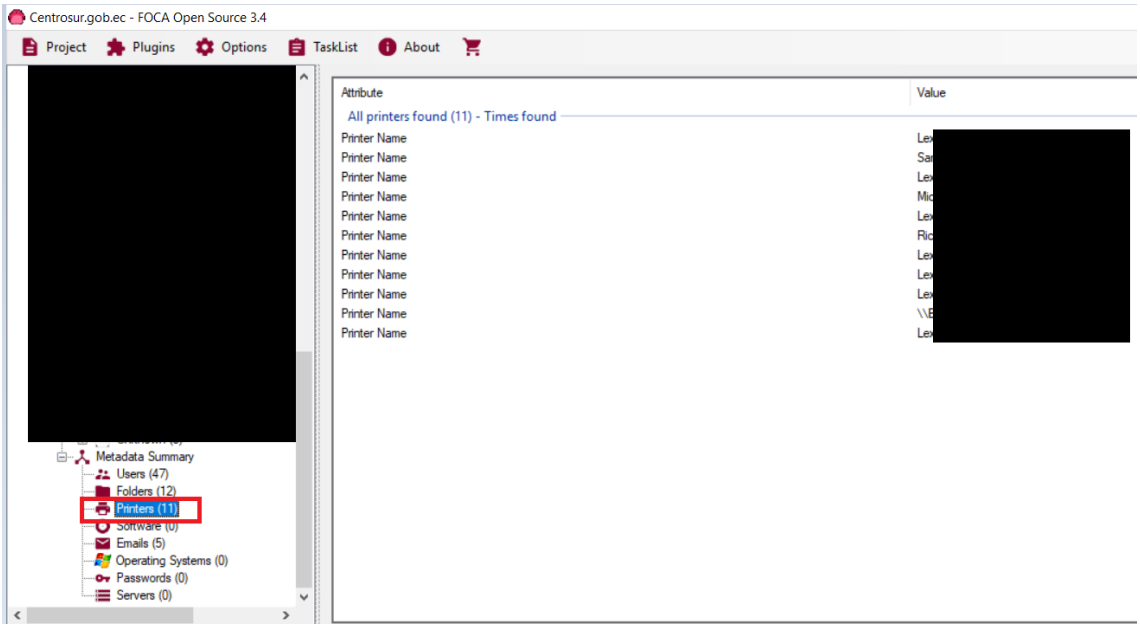


Figura 51. Impresoras descubiertas en CENTROSUR.

Dispositivo	**Cantidad**	**Veces Adjuntadas a los Archivos**
Impresora	10	24

Tabla 14. Datos de impresoras descubiertas en CENTROSUR.

En la Figura 51. Tenemos los datos de las impresoras encontradas en la CENTROSUR, los mismos datos que se encuentran en la Tabla 14, la misma resume datos similares que se pueden apreciar en la Figura 51.

Como podemos observar en la Tabla 14, en la CENTROSUR, logramos obtener los datos de 10 impresoras localizas en la CENTROSUR, presenten en 24 de sus documentos subidos a internet. Las impresoras permiten a los atacantes conocer los fallos de seguridad en estos equipos y convertirse en vectores de ataque. Y las personas que comparten un mismo espacio físico en un área determinada.

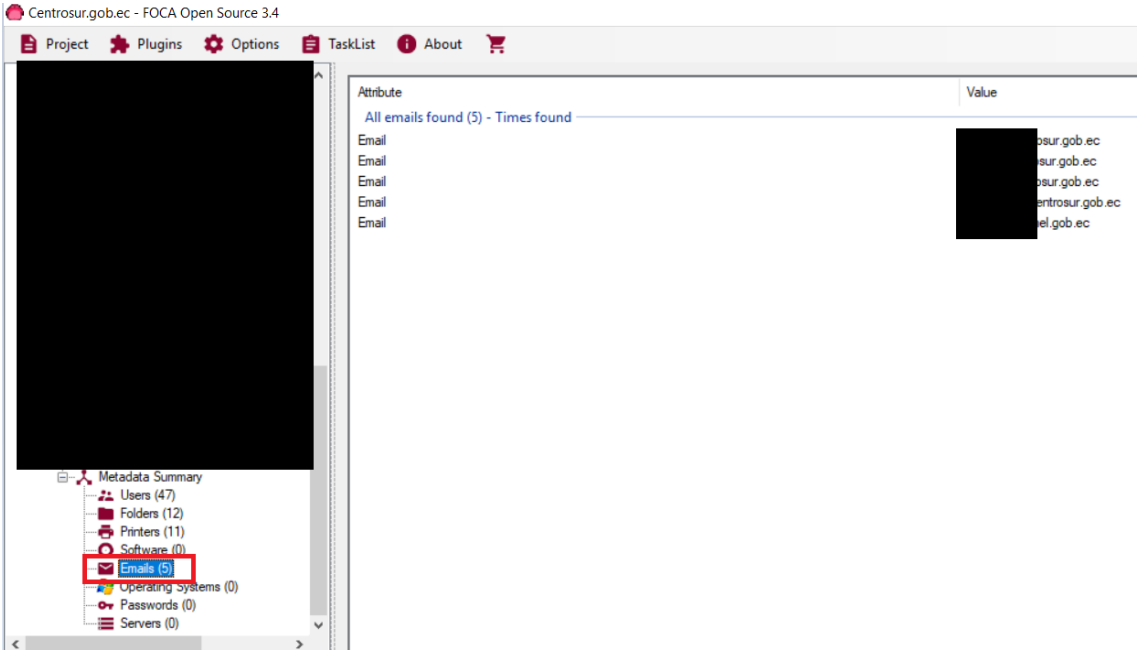


Figura 52. Correos Electrónicos descubiertos en CENTROSUR.

Como podemos observar en la Figura 52, en la CENTROSUR, logramos obtener los datos de 5 emails localizados en la CENTROSUR. Con esto podemos conocer información privilegiada de la empresa de manera externa.

Nombre	**Cantidad de Apariciones en Documentos**
Microsoft Office	41
Microsoft Office XP	106
GPL Ghostscript 9.04	33
PDFCreator 1.2.3Windows	33

Adobe PDF Library 10.01	17
Adobe Illustrator CC (Windows)	1
Adobe Fireworks CS5 11.0.1.7 Windows	1
Adobe Illustrator CS6 (Windows)	16
PDF Complete version 3.5.1.1	1
GPL Ghostscript 9.10	9
PDFCreator 1.7.3 Windows	9
PDFCreator 3.0.2.8660 Windows	1
Adobe PDF Library 11.0	1
Adobe InDesign CC 2014 (Macintosh)	1
PDFCreator 3.0.1.8040 Windows	1
GPL Ghostscript 8.64	1
PDFCreator 0.9.8 Windows	1
Adobe PDF Library 9.90	1
Adobe Illustrator CS5	1

Tabla 15. Datos de software descubierto en CENTROSUR.

En la Tabla 15. Tenemos los datos del software encontrado en la CENTROSUR, en esta tabla se presentan menos datos que en los obtenidos por el software. El software indexa falsos positivos, y en esta tabla están solamente los datos del software eliminando estos falsos positivos.

Como podemos observar en la Tabla 15, logramos obtener los datos del software que se utilizada en la CENTROSUR. Tenemos que entender bien la indexación de estos

datos, pues como podemos apreciar en cifras, se puede ver que existe una mayor cantidad de apariciones del Software Microsoft Office, y se podría pensar que la mayoría de documentos indexados a la página igualmente debería ser de extensión: docx, xlxs, y más extensión de Office, pero no es así.

El por qué es simple, estos documentos son creados con las herramientas de Microsoft Office, pero para mayor facilidad de distribución y lectura de los usuarios son transformados a PDF. Es por esto que la mayoría de documentos como podemos apreciar en la Figura 49, son PDF.

Una vez que se tiene la versión del software con el que se crean los documentos, cualquier pirata informático podría tomar esta información y conseguir el exploit para explotar esta vulnerabilidad.

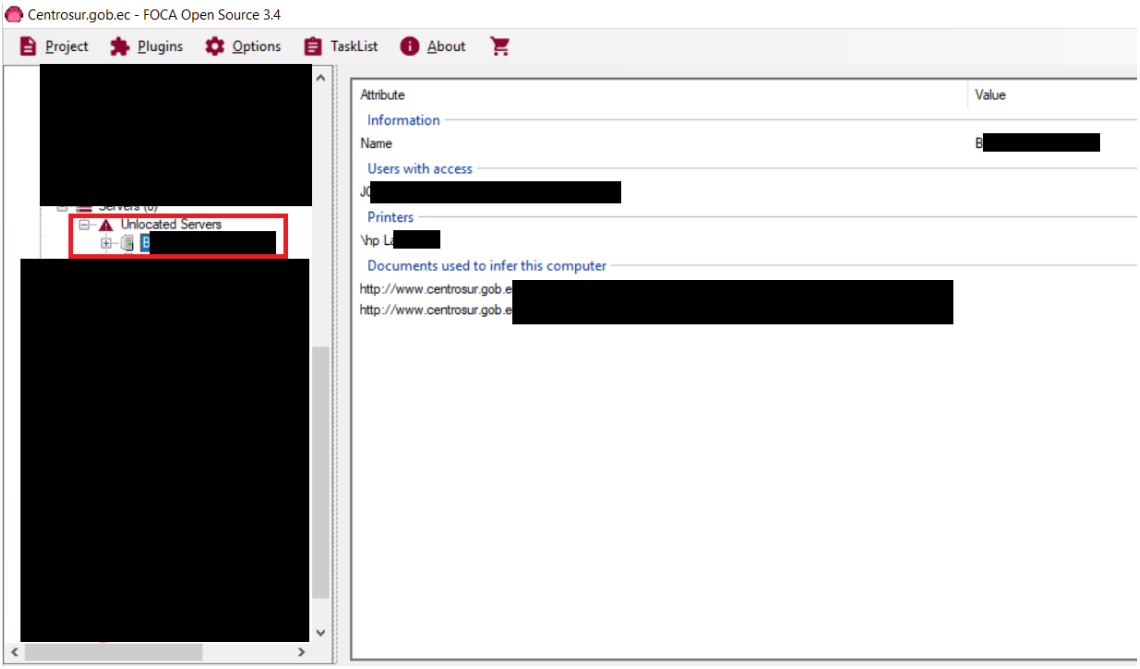


Figura 53. Detalle de información de un servidor descubierto en CENTROSUR.

En la Figura 53. Podemos apreciar que se ha seleccionado un servidor de la toda la lista de servidores de la CENTROSUR, solamente por medios de investigación para conocer más a profundidad toda la información que se puede obtener de un usuario y su máquina.

Podemos conocer el nombre asignado a este servidor, y tenemos conocimiento de cuáles son los usuarios que tiene acceso al miso, pues se despliega una lista. Un dato muy importante es la impresora que esté conectada a ese servidor, pues si queremos acceder a ese servidor podemos atacar a todos los usuarios que usen esa impresora y después movernos internamente hasta el usuario que tiene el acceso al servidor. Además de los archivos utilizados o que han pasado por este servidor antes seleccionado.

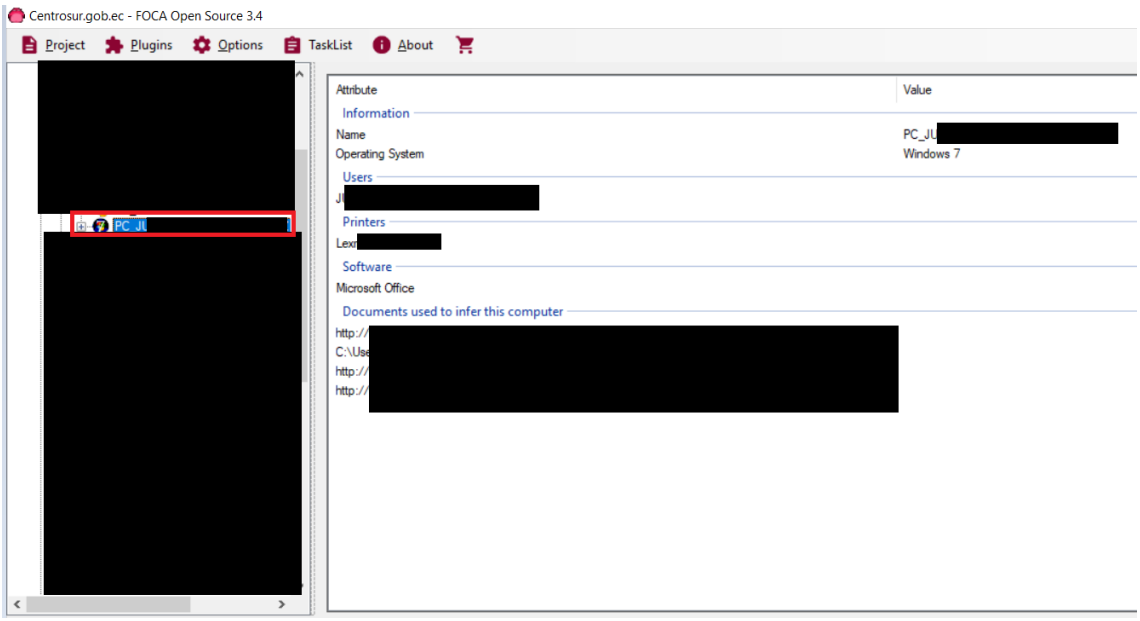


Figura 54. Detalle de información de un equipo descubierto en CENTROSUR.

En la Figura 54. Podemos apreciar que se ha seleccionado un equipo de la toda la lista de equipos de la CENTROSUR, solamente por medios de investigación para conocer más a profundidad toda la información que se puede obtener de un usuario y su máquina.

Podemos conocer el nombre del usuario de esa máquina, por lo tanto, el nombre de la persona que trabaja en la CENTROSUR, en caso de ser más de uno, se podrá visualizar los usuarios pertenecientes a esa máquina. El sistema operativo que tiene esa máquina, en este caso Windows 7. El software con el que se crea los documentos en este equipo, como son Microsoft Office. Además de los documentos que han sido creados desde este equipo, este es un punto muy importante pues podemos ver de qué tipo son los archivos y por ejemplo si el enfoque de estos es netamente financiero podemos deducir que esta persona está en el área financiera de la CENTROSUR. Finalmente, los archivos que se indexan desde el equipo almacena direcciones internas del equipo, como se puede ver en la Figura

50. Se cita la ruta de donde se sacan los archivos, por lo tanto, tenemos la ruta del equipo, lo cual nos aporta más información, obviamente hemos difuminado toda la ruta por medidas de seguridad.

3.4.4 EMAC

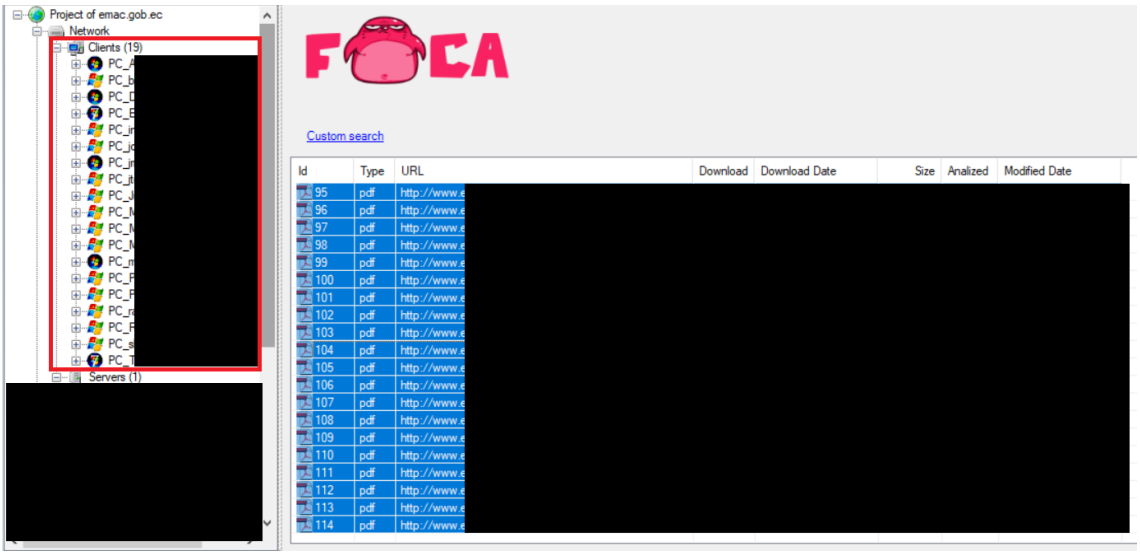


Figura 55. Equipos descubiertos en EMAC.

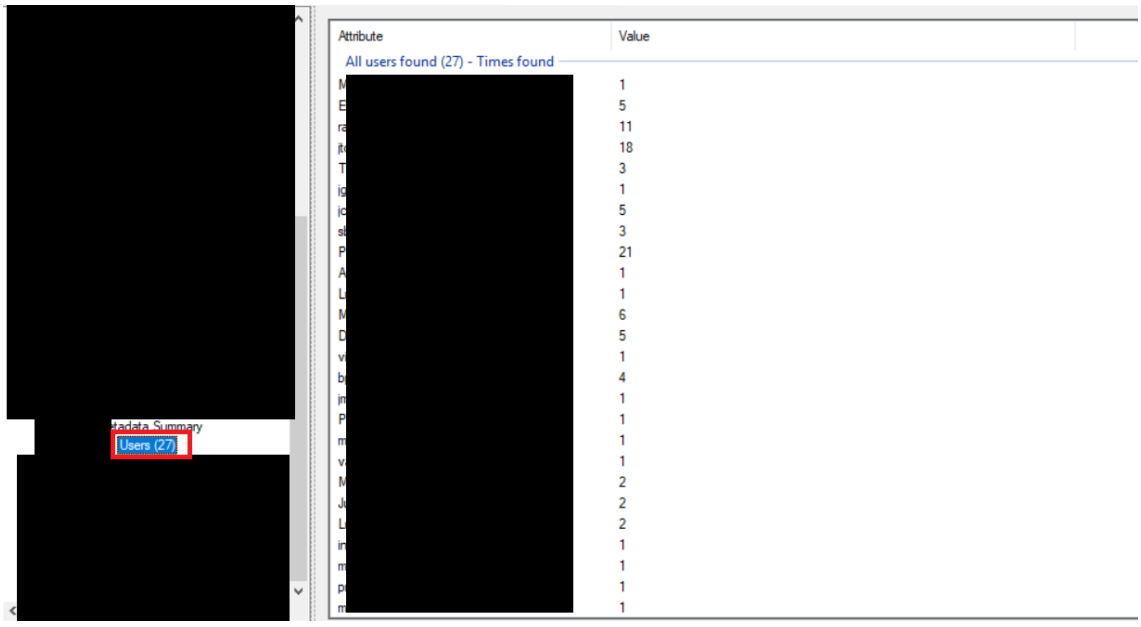


Figura 56. Usuarios descubiertos en EMAC.

Dispositivo	Cantidad	Sistema Operativo
Equipos	19	Windows
	5	Windows 7
	1	Windows Vista
	13	Otra Versión de Windows
Usuarios	27	

Tabla 16. Datos de equipos descubiertos en EMAC.

En la Figura 55 y Figura 56. Tenemos los datos de los equipos y los usuarios encontrados en la EMAC, datos similares a los que se encuentran en la Tabla 16, que es una tabla donde se resume datos similares a las 2 Figuras anteriores.

Como podemos observar en la Tabla 16, en la EMAC, logramos obtener los datos de 19 equipos utilizados para crear sus documentos que fueron subidos a su sitio web, y tenemos la información de 27 usuarios. 100% de las maquinas utilizadas para subir archivos a su sitio web son Windows, 26.31% de estas máquinas son Windows 7, 5.26% de estas máquinas son Windows Vista, 68.42% son otra versión Superior de Windows. Conociendo que la totalidad de sus equipos son Windows.

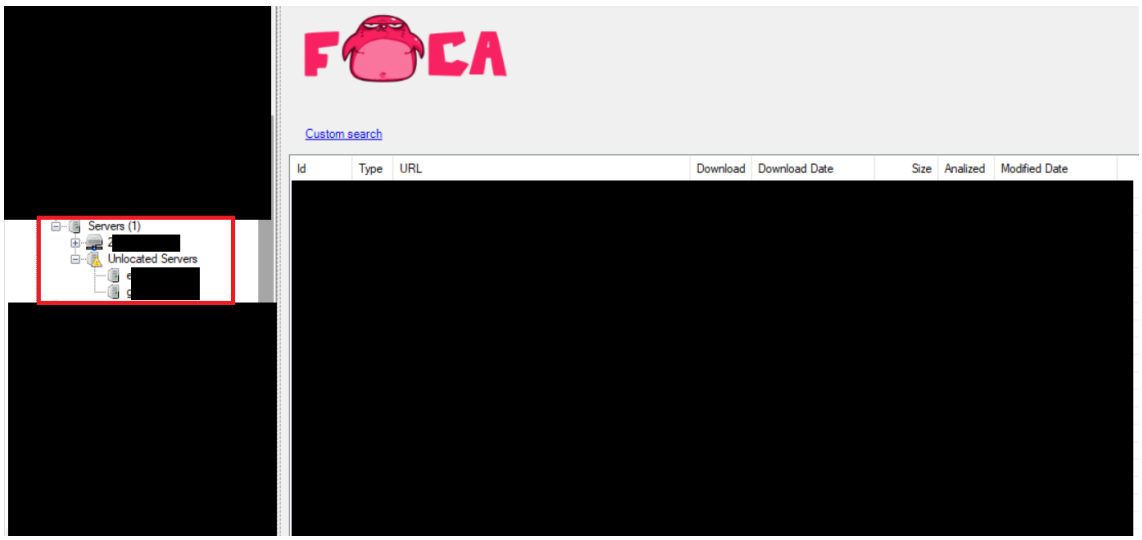


Figura 57. Servidores descubiertos en EMAC.

Dispositivo	Cantidad	Locación
Servidor	3	Dirección IP y No Asignado
	1	Servidores con Dirección IP
	2	Sin Dirección Asignada

Tabla 17. Datos de servidores descubiertos en EMAC.

En la Figura 57. Tenemos los datos de los servidores encontrados en la EMAC, los mismos datos que se encuentran en la Tabla 17, que es una tabla donde se resume datos similares que se pueden apreciar en la Figura 57 con un contexto más comprensible.

Como podemos observar en la Tabla 17, en la EMAC, logramos obtener los datos de 3 servidores, 1 servidor con la dirección ip y 2 servidores que no se logran obtener la dirección ip, pero si el nombre y por supuesto se conoce que tiene conexión con las computadoras en la empresa, por lo que se puede asumir que son servidores internos de la empresa.

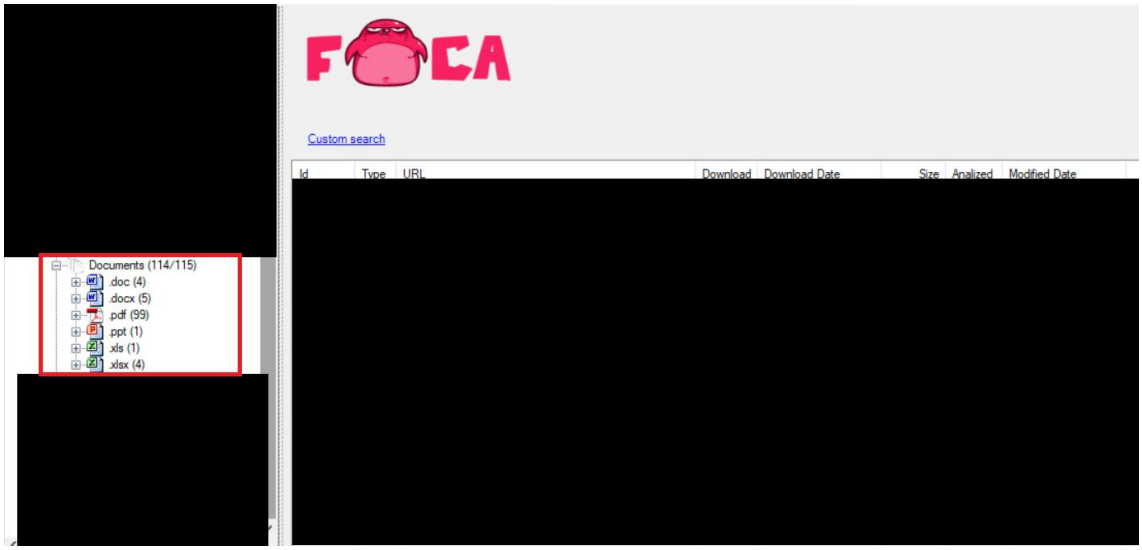


Figura 58. Documentos descubiertos en EMAC.

En la Figura 58. Tenemos los datos de los documentos encontrados en la EMAC. Logramos obtener los datos de 115 documentos indexados a su sitio web. De los cuales: 5 son documentos de Excel que representan el 4.34%, 1 es un documento de Power Point

que representa el 0.86%, 9 son documentos de Word que representan el 7.82%, 99 son documentos PDF que representan el 86.08% de los documentos, el resto son documentos de un formato desconocido. Esto quiere decir que en su mayoría los documentos son PDF, por lo que podemos entender que la mayoría de documentos que se generan en la empresa son de este tipo de documento, entonces deberíamos enfocarnos en el software que utilizan para crear este tipo de documentos para buscar fallos de seguridad en estos programas.

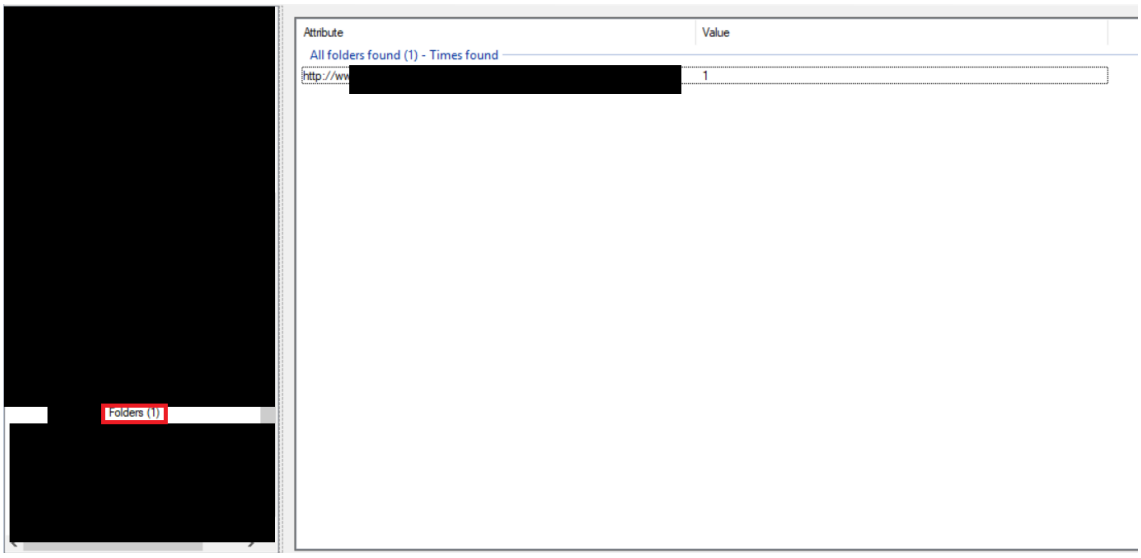


Figura 59. Directorios descubiertos en EMAC.

Tipo	Cantidad	Cantidad Directorios en Documentos
Directorio	1	1

Tabla 18. Datos de directorios descubiertos en EMAC.

En la Figura 59. Tenemos los datos de los directorios encontradas en la EMAC, los mismos datos que se encuentran en la Tabla 18, la misma resume datos similares que se pueden apreciar en la Figura 59.

Como podemos observar en la Tabla 18, en la EMAC, logramos obtener los datos de 1 directorio indexado en los documentos publicados en el sitio web de la EMAC, este directorio fue indexado en 1 documento, lo que permite conocer el directorio (folder)

hacia el cual los trabajadores de la EMAC, que publican los documentos se conectan y los metadatos almacenados en sus documentos. En estos documentos se almacenó el directorio personal de un usuario, e incluso la información de la dirección de donde fue adquirido el software.

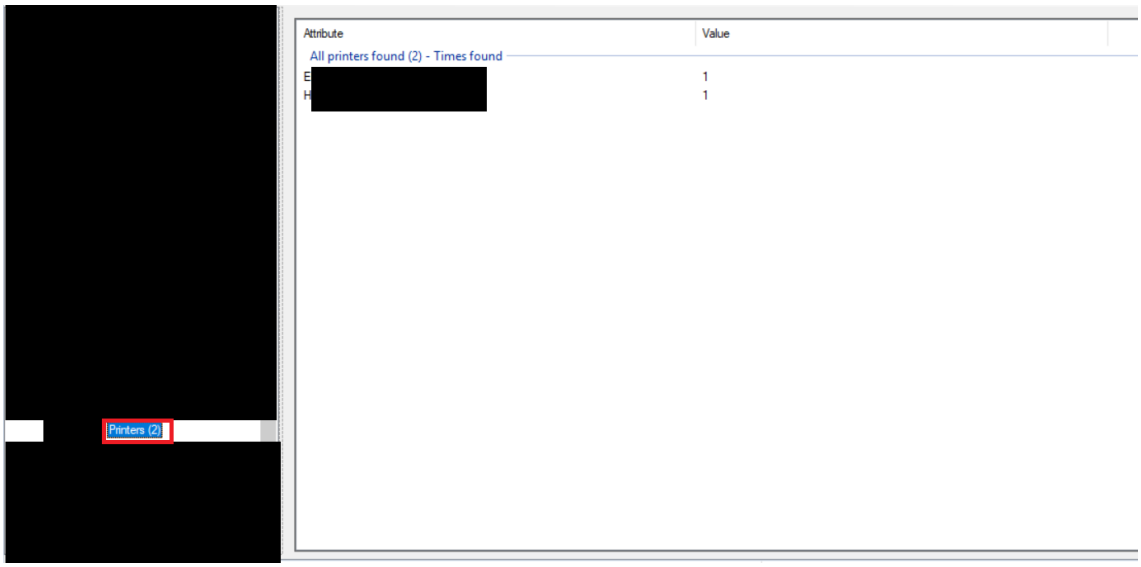


Figura 60. Impresoras descubiertas en EMAC.

Dispositivo	**Cantidad**	**Veces Adjuntadas a los Archivos**
Impresora	2	2

Tabla 19. Datos de impresoras descubiertas en EMAC.

En la Figura 60. Tenemos los datos de las impresoras encontradas en la EMAC, los mismos datos que se encuentran en la Tabla 19, la misma resume datos similares que se pueden apreciar en la Figura 60.

Como podemos observar en la Tabla 19, en la EMAC, logramos obtener los datos de 2 impresoras localizas en la EMAC, presenten en 2 de sus documentos subidos a internet. Las impresoras permiten a los atacantes conocer los fallos de seguridad en estos equipos y convertirse en vectores de ataque. Y las personas que comparten un mismo espacio físico en un área determinada.

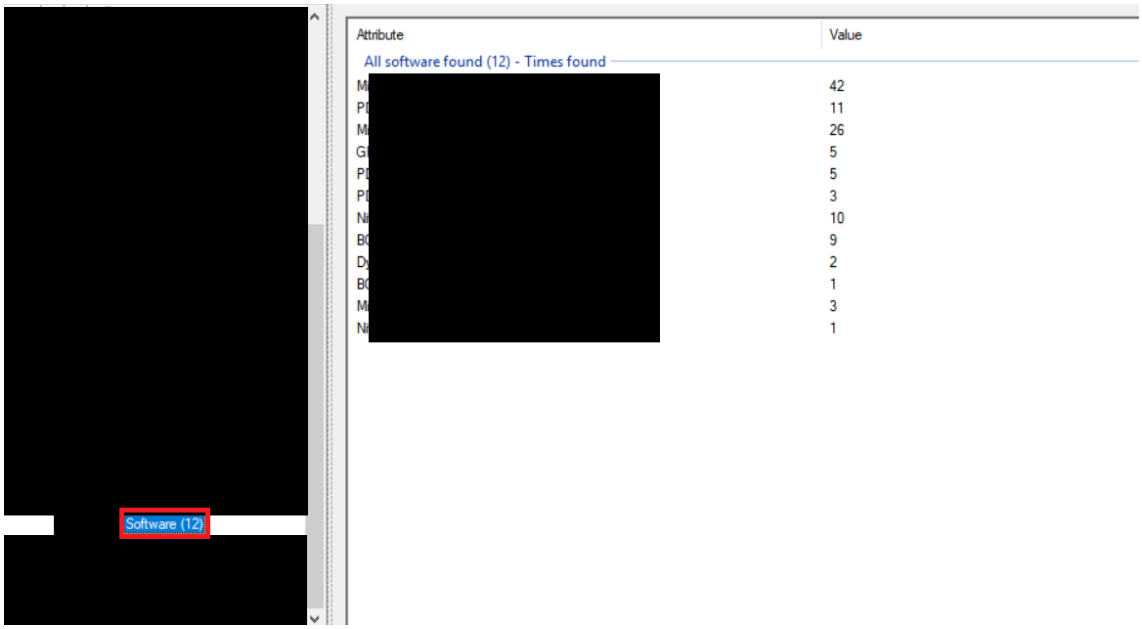


Figura 61. Software descubierto en EMAC.

Nombre	**Cantidad de Apariciones en Documentos**
Microsoft Office	42
Microsoft Office XP	26
Microsoft 2007	3
GPL Ghostscript 9.06	5
PDFCreator 1.6.0 Windows	5
PDFCreator 2.1.1.0 Windows	11
PDFCreator 1.9.3.0 Windows	3
NitroPDF 6.0	10
Nitro Pro 9.0.2.37	1
BCL easyPDF 6.00.20	1
BCL easyPDF 6.00 (0320)	9

Tabla 20. Datos de software descubierto en EMAC.

En la Tabla 20. Tenemos los datos del software encontrado en la EMAC, en esta tabla se presentan menos datos que en los obtenidos por el software. El software indexa falsos positivos, y en esta tabla están solamente los datos del software eliminando estos falsos positivos.

Como podemos observar en la Tabla 20, logramos obtener los datos del software que se utilizada en la EMAC. Tenemos que entender bien la indexación de estos datos, pues como podemos apreciar en cifras, se puede ver que existe una mayor cantidad de apariciones del Software Microsoft Office, y se podría pensar que la mayoría de documentos indexados a la página igualmente debería ser de extensión: docx, xlxs, y más extensión de Office, pero no es así.

El por qué es simple, estos documentos son creados con las herramientas de Microsoft Office, pero para mayor facilidad de distribución y lectura de los usuarios son transformados a PDF. Es por esto que la mayoría de documentos como podemos apreciar en la Figura 58, son PDF.

Una vez que se tiene la versión del software con el que se crean los documentos, cualquier pirata informático podría tomar esta información y conseguir el exploit para explotar esta vulnerabilidad.

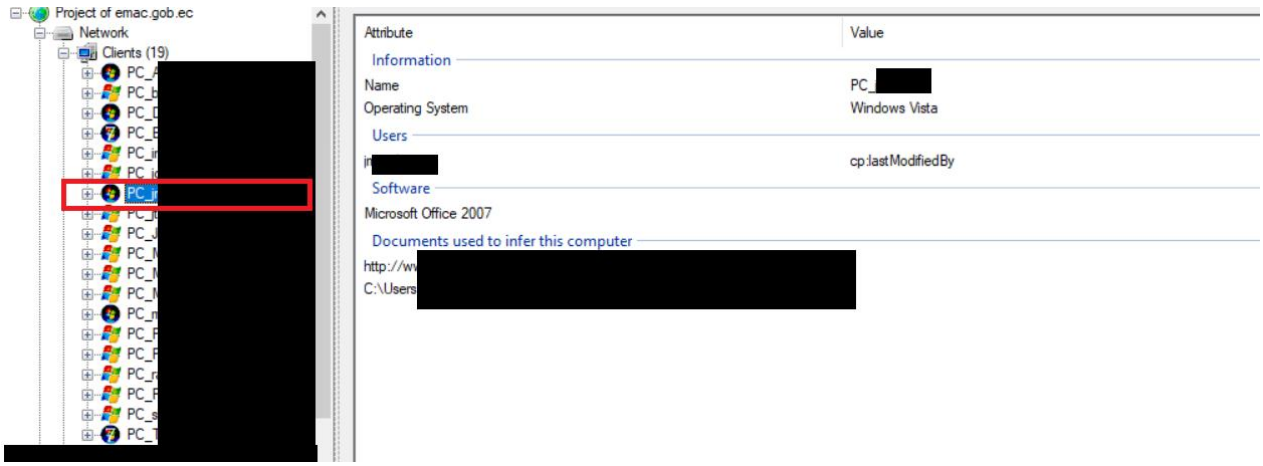


Figura 62. Detalle de información de un equipo descubierto en EMAC.

En la Figura 62. Podemos apreciar que se ha seleccionado un equipo de la toda la lista de equipos de la EMAC, solamente por medios de investigación para conocer más a profundidad toda la información que se puede obtener de un usuario y su máquina.

Podemos conocer el nombre del usuario de esa máquina, por lo tanto, el nombre de la persona que trabaja en la EMAC, en caso de ser más de uno, se podrá visualizar los usuarios pertenecientes a esa máquina. El sistema operativo que tiene esa máquina, en este caso Windows 7. El software con el que se crea los documentos en este equipo, como son Microsoft Office. Además de los documentos que han sido creados desde este equipo, este es un punto muy importante pues podemos ver de qué tipo son los archivos y por ejemplo si el enfoque de estos es netamente financiero podemos deducir que esta persona está en el área financiera de la EMAC. Finalmente, los archivos que se indexan desde el equipo almacena direcciones internas del equipo, como se puede ver en la Figura 50. Se cita la ruta de donde se sacan los archivos, por lo tanto, tenemos la ruta del equipo, lo cual nos aporta más información, obviamente hemos difuminado toda la ruta por medidas de seguridad.

3.4.5 FARMASOL

Figura 63. Equipos descubiertos en FARMASOL

Figura 64. Usuarios descubiertos en FARMASOL.

Dispositivo	Cantidad	Sistema Operativo
Equipos	17	Windows
	10	Windows 7
	7	Windows Vista
Usuarios	19	

Tabla 21. Datos de equipos descubiertos en FARMASOL.

En la Figura 63 y Figura 64. Tenemos los datos de los equipos y los usuarios encontrados en FARMASOL, datos similares a los que se encuentran en la Tabla 21, que es una tabla donde se resume los datos similares que en las 2 Figuras anteriores.

Como podemos observar en la Tabla 21, en FARMASOL, logramos obtener los datos de 17 equipos utilizados para crear sus documentos que fueron subidos a su sitio web, y tenemos la información de 19 usuarios. 100% de las maquinas utilizadas para subir archivos a su sitio web son Windows, 58.82% de estas máquinas son Windows 7, 41.17% de estas máquinas son Windows Vista. Conociendo que la totalidad de sus equipos son Windows.

Figura 65. Servidores descubiertos en FARMASOL.

Dispositivo	Cantidad	Locación
Servidor	4	Dirección IP y No Asignado
	1	Servidores con Dirección IP
	3	Sin Dirección Asignada

Tabla 22. Datos de servidores descubiertos en FARMASOL.

En la Figura 65. Tenemos los datos de los servidores encontrados en FARMASOL, los mismos datos que se encuentran en la Tabla 22, que es una tabla donde se resume datos similares que se pueden apreciar en la Figura 65. con un contexto más comprensible.

Como podemos observar en la Tabla 22, en FARMASOL, logramos obtener los datos 4 servidores tanto con ip como sin ip. 1 servidor con la dirección ip y de 3 servidores no se logra obtener la dirección ip, pero si el nombre y por supuesto se conoce que tiene conexión con las computadoras en la empresa, por lo que se puede asumir que son servidores internos de la empresa. A un servidor de estos, se puede acceder a la versión del software del servidor como son: apache, php, openssl, usuarios que tiene acceso y a que carpetas tienen acceso.

Figura 66. Documentos descubiertos en FARMASOL.

En la Figura 66. Tenemos los datos de los documentos encontrados en FARMASOL. Logramos obtener los datos de 144 documentos indexados a su sitio web. De los cuales: 16 son documentos de Excel que representan el 11.11%, 1 es un documento de Power Point que representa el 0.87%, 4 son documentos de Word que representan el 2.77%, 118 son documentos PDF que representan el 81.94% de los documentos, el resto son documentos de un formato desconocido. Esto quiere decir que en su mayoría los documentos son PDF, por lo que podemos entender que la mayoría de documentos que se generan en la empresa son de este tipo de documento, entonces deberíamos enfocarnos en el software que utilizan para crear este tipo de documentos para buscar fallos de seguridad en estos programas.

Figura 67. Directorios descubiertos en FARMASOL.

Tipo	Cantidad	Cantidad Directorios en Documentos
Directorio	14	88

Tabla 23. Datos de directorios descubiertos en FARMASOL.

En la Figura 67. Tenemos los datos de los directorios encontradas en FARMASOL, los mismos datos que se encuentran en la Tabla 23, la misma resume datos similares que se pueden apreciar en la Figura 67.

Como podemos observar en la Tabla 23, en FARMASOL, logramos obtener los datos de 14 directorios indexados en los documentos publicados en el sitio web de FARMASOL, estos directorios fueron indexados en 88 documentos, lo que permite conocer los directorios (folders) hacia los cuales los trabajadores de FARMASOL, que publican los documentos se conectan y los metadatos almacenados en sus documentos. En estos documentos se almaceno el directorio personal de un usuario, e incluso la información de la dirección de donde fue adquirido el software.

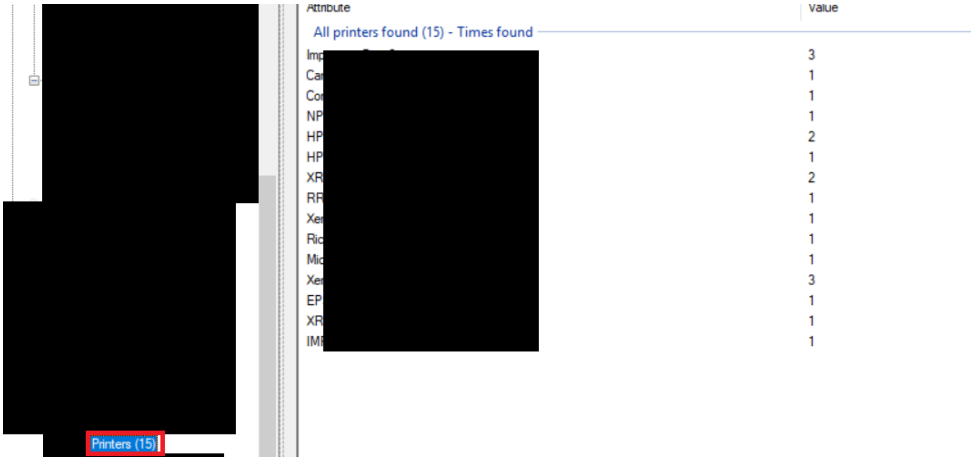


Figura 68. Impresoras descubiertas en FARMASOL.

Dispositivo	Cantidad	Veces Adjuntadas a los Archivos
Impresora	15	21

Tabla 24. Datos de impresoras descubiertas en FARMASOL.

En la Figura 68. Tenemos los datos de las impresoras encontradas en la FARMASOL, los mismos datos que se encuentran en la Tabla 24, la misma resume datos similares que se pueden apreciar en la Figura 68.

Como podemos observar en la Tabla 24, en la FARMASOL, logramos obtener los datos de 15 impresoras localizas en la FARMASOL, presenten en 21 de sus documentos subidos a internet. Las impresoras permiten a los atacantes conocer los fallos de seguridad en estos equipos y convertirse en vectores de ataque. Y las personas que comparten un mismo espacio físico en un área determinada.

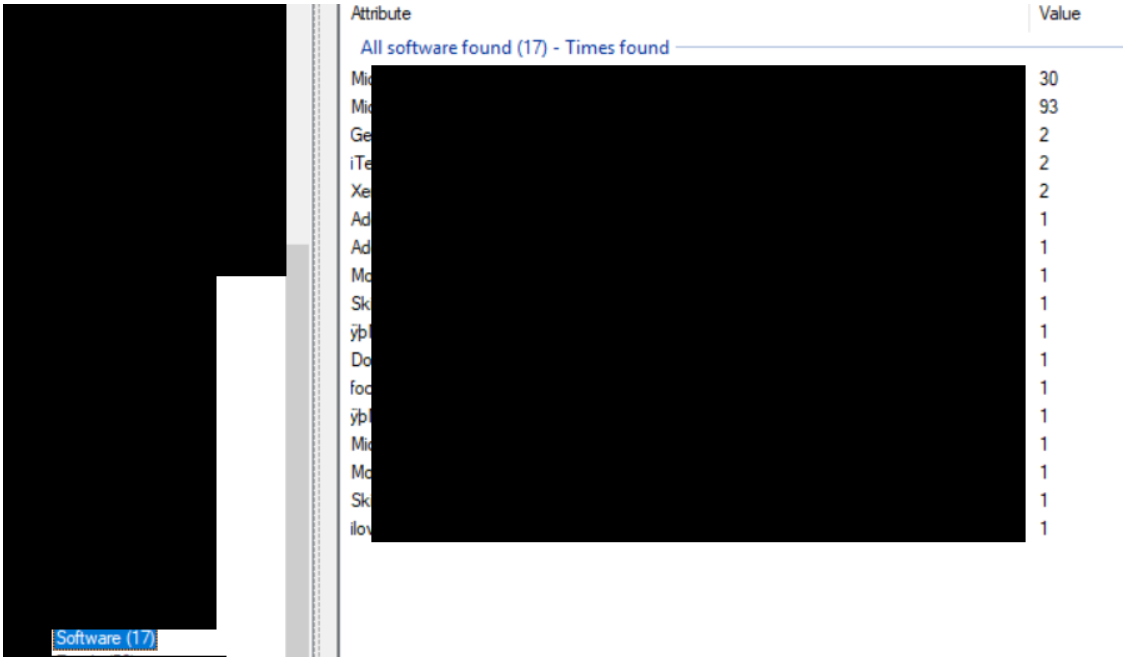


Figura 69. Software descubierto en FARMASOL.

Nombre	**Cantidad de Apariciones en Documentos**
Microsoft Office	93
Microsoft Office XP	1
Microsoft Office 2007	30
GeneXus PDF Report Generator	2

Doro PDF Writer (2.04)	1
iText 2.17 by 1T3XT	2
Adobe Photoshop CS2	1
Adobe Photoshop CS6	1
ilovepdf.com	1

Tabla 25. Datos de software descubierto en FARMASOL.

En la Figura 69. Tenemos los datos del software encontrado en FARMASOL, los mismos datos que se encuentran en la Tabla 25, la misma resume datos similares que se pueden apreciar en la Figura 69, pero con la diferencia que en esta tabla se presentan menos datos que en la Figura 69. El software indexa falsos positivos, y en esta tabla están solamente los datos del software eliminando estos falsos positivos.

Como podemos observar en la Tabla 25, en FARMASOL, logramos obtener los datos del software que se utilizada en FARMASOL. Tenemos que entender bien la indexación de estos datos, pues como podemos apreciar en cifrar se puede ver que existe una mayor cantidad de apariciones del Software Microsoft Office, y se podría pensar que la mayoría de documentos indexados a la página igualmente debería ser de extensión: docx, xlxs, y más extensión de Office, pero no es así.

El por qué es simple, estos documentos son creados con las herramientas de Microsoft Office, pero para mayor facilidad de distribución y lectura de los usuarios son transformados a PDF. Es por esto que la mayoría de documentos como podemos apreciar en la Figura 66 son PDF.

Una vez que se tiene la versión del software con el crean los documentos, cualquier pirata informático pudiera tomar esta información y conseguir el exploit para explotar esta vulnerabilidad.

Figura 70. Correos Electrónicos descubiertos en FARMASOL.

Como podemos observar en la Figura 70, en FARMASOL, logramos obtener los datos de 50 emails localizados en FARMASOL. Con esto podemos conocer información privilegiada de la empresa de manera externa.

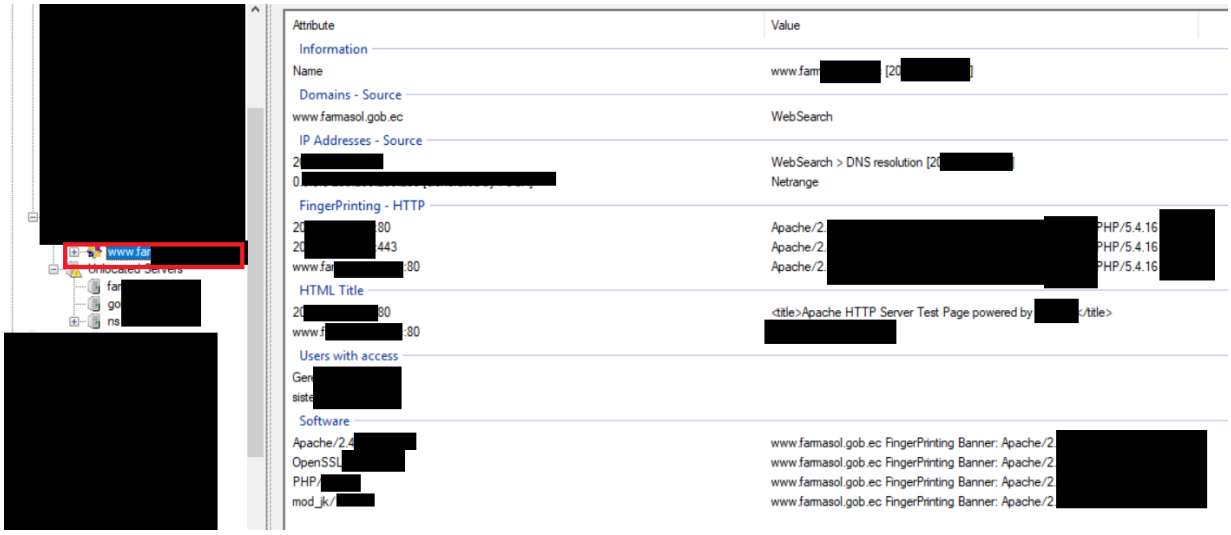


Figura 71. Detalle de información de un servidor descubierto en FARMASOL.

En la Figura 71. Podemos apreciar que se ha seleccionado un servidor de la toda la lista de servidores de FARMASOL, solamente por medios de investigación para conocer más a profundidad toda la información que se puede obtener de un usuario y su máquina.

Podemos conocer el nombre asignado a este servidor, y tenemos conocimiento de cuáles son los usuarios que tiene acceso al miso, pues se despliega una lista. Podemos conocer cuál es la versión de apache que corre sobre el servidor, la versión de Open SSL, la versión de PHP, y más datos importantes.

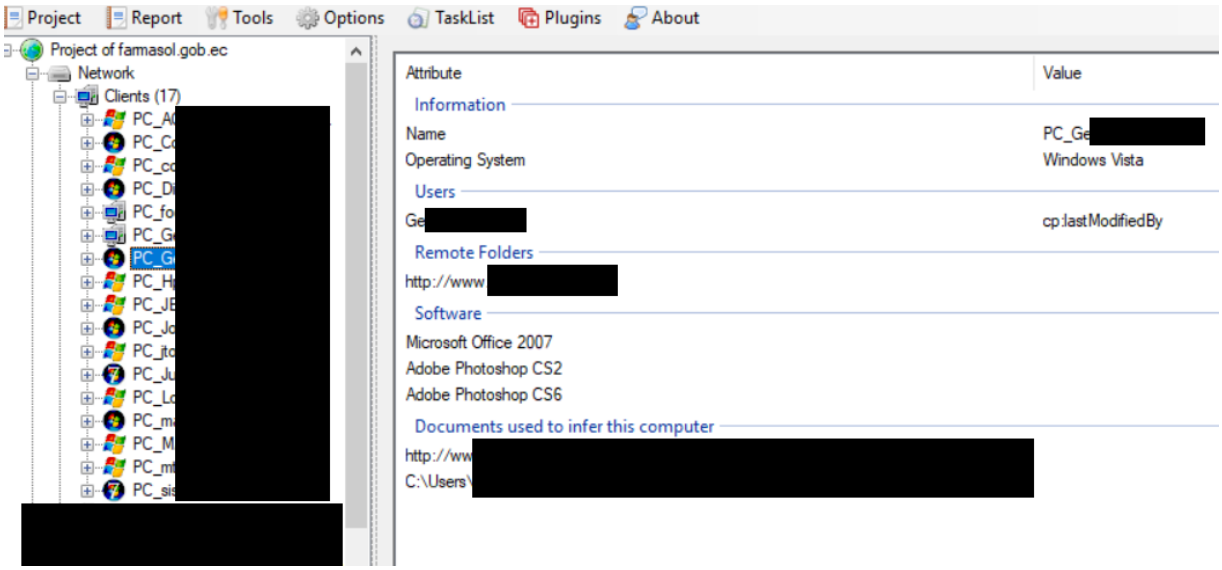


Figura 72. Detalle de información de un equipo descubierto en FARMASOL.

En la Figura 72. Podemos apreciar que se ha seleccionado un equipo de la toda la lista de equipos de FARMASOL, solamente por medios de investigación para conocer más a profundidad toda la información que se puede obtener de un usuario y su máquina.

Podemos conocer el nombre del usuario de esa máquina, por lo tanto, el nombre de la persona que trabaja en FARMASOL, en caso de ser más de uno, se podrá visualizar los usuarios pertenecientes a esa máquina. El sistema operativo que tiene esa máquina, en este caso Windows Vista. El software con el que se crea los documentos en este equipo, como son Microsoft Office 2007, Adobe Photoshop CS2, Adobe Photoshop CS6. Además de los documentos que han sido creados desde este equipo, este es un punto muy importante pues podemos ver de qué tipo son los archivos y por ejemplo si el enfoque de estos es netamente financiero podemos deducir que esta persona está en el área financiera

de FARMASOL. Finalmente, los archivos que se indexan desde el equipo almacena direcciones internas del equipo, como se puede ver en la Figura 67. Se cita la ruta de donde se sacan los archivos, por lo tanto, tenemos la ruta del equipo, lo cual nos aporta más información, obviamente hemos difuminado toda la ruta por medidas de seguridad.

3.4.6 ALCADÍA CUENCA

Figura 73. Equipos descubiertos en ALCADÍA CUENCA.

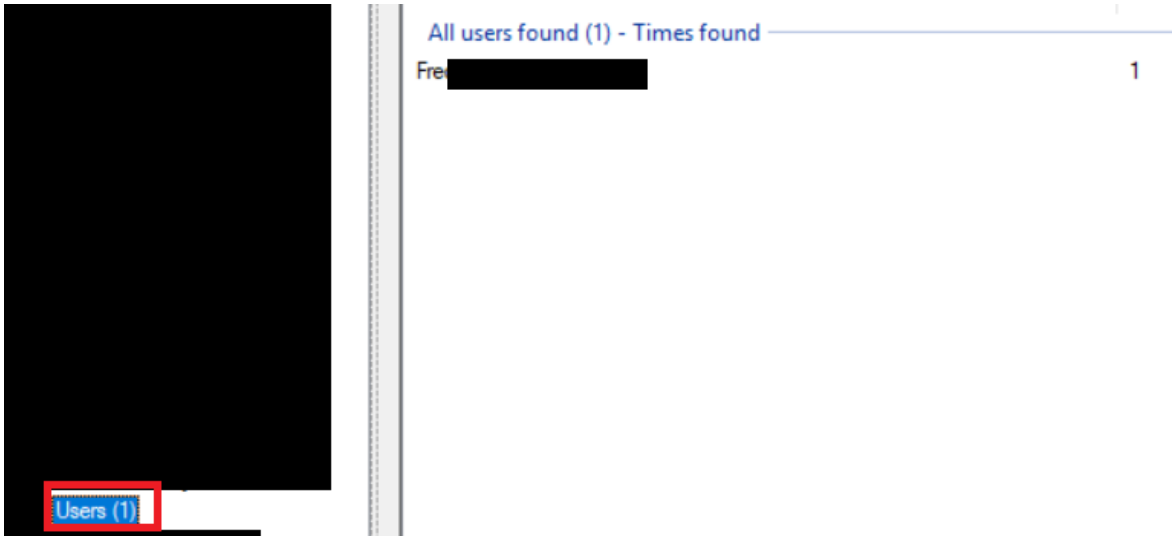


Figura 74. Usuarios descubiertos en ALCADÍA CUENCA.

Dispositivo	Cantidad	Sistema Operativo
Equipos	1	Windows
Usuarios	1	

Tabla 26. Datos de equipos descubiertos en ALCALDÍA CUENCA.

En la Figura 73 y Figura 74. Tenemos los datos de los equipos y los usuarios encontrados en la ALCADÍA CUENCA, datos similares a los que se encuentran en la Tabla 26, que es una tabla donde se resume los mismo que se puede apreciar en las 2 Figuras.

Como podemos observar en la Tabla 26, en la ALCALDÍA CUENCA, logramos obtener los datos de 1 equipo utilizado para crear sus documentos que fueron subidos a su sitio web, y tenemos la información de 1 usuario, El 100% de las maquinas utilizadas para subir archivos a su sitio web son Windows. Se puede deducir que no se obtuvo mucha información debido a la escasa cantidad de documentos encontrados en la página.

Figura 75. Servidores descubiertos en ALCADÍA CUENCA.

Dispositivo	Cantidad	Locación
Servidor	3	Dirección IP y No Asignado
	1	Servidores con Dirección IP
	2	Sin Dirección Asignada

Tabla 27. Datos de servidores descubiertos en ALCALDÍA CUENCA.

En la Figura 75. Tenemos los datos de los servidores encontrados en la ALCALDÍA CUENCA, los mismos datos que se encuentran en la Tabla 27, que es una tabla donde se resume datos similares que se pueden apreciar en la Figura 75.

Como podemos observar en la Tabla 27, en la ALCALDÍA CUENCA, logramos obtener los datos de 3 servidores conectados, tanto externos como internos. De los cuales 1 servidores logramos observar las direcciones ip. De los otros 2 servidores no se logra obtener la dirección ip, pero si el nombre y por supuesto se conoce que tiene conexión con las computadoras en la empresa, por lo que se puede asumir que son servidores internos de la empresa.

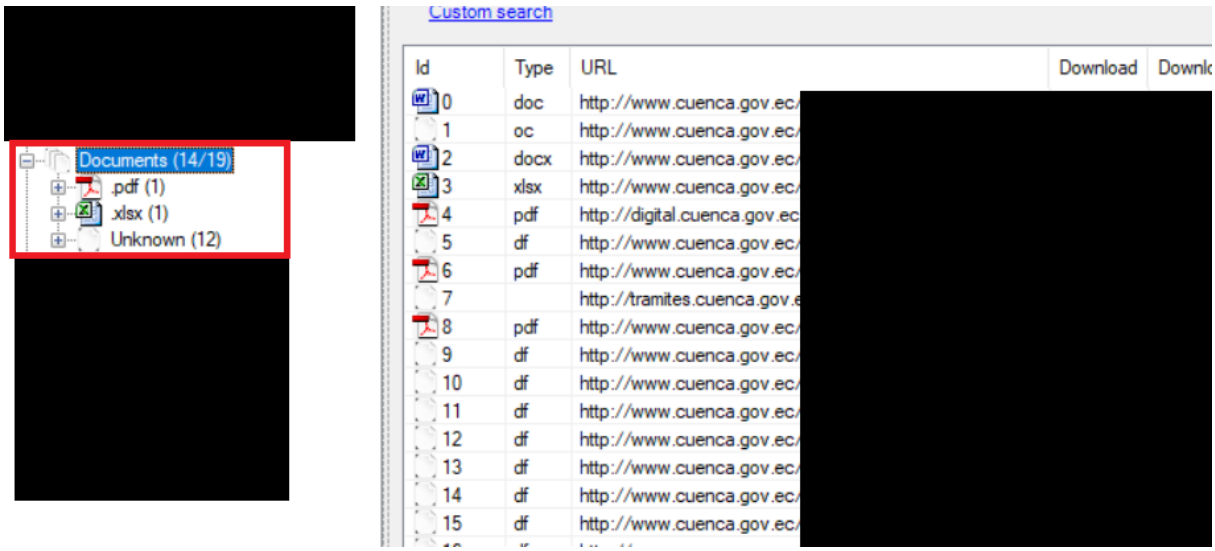


Figura 76. Documentos descubiertos en ALCADÍA CUENCA.

En la Figura 76. Tenemos los datos de los documentos encontrados en la ALCALDÍA CUENCA. Logramos obtener los datos de 19 documentos indexados a su sitio web. De los cuales: 1 es documento de Excel que representa el 5.26%, 1 es documento PDF que representa el 5.26% de los documentos, el resto son documentos de un formato desconocido. No se logra obtener mayor información debido a la poca cantidad de documentos indexados a su página web.

No se dispone información de directorios ni de impresoras indexadas a estos documentos.

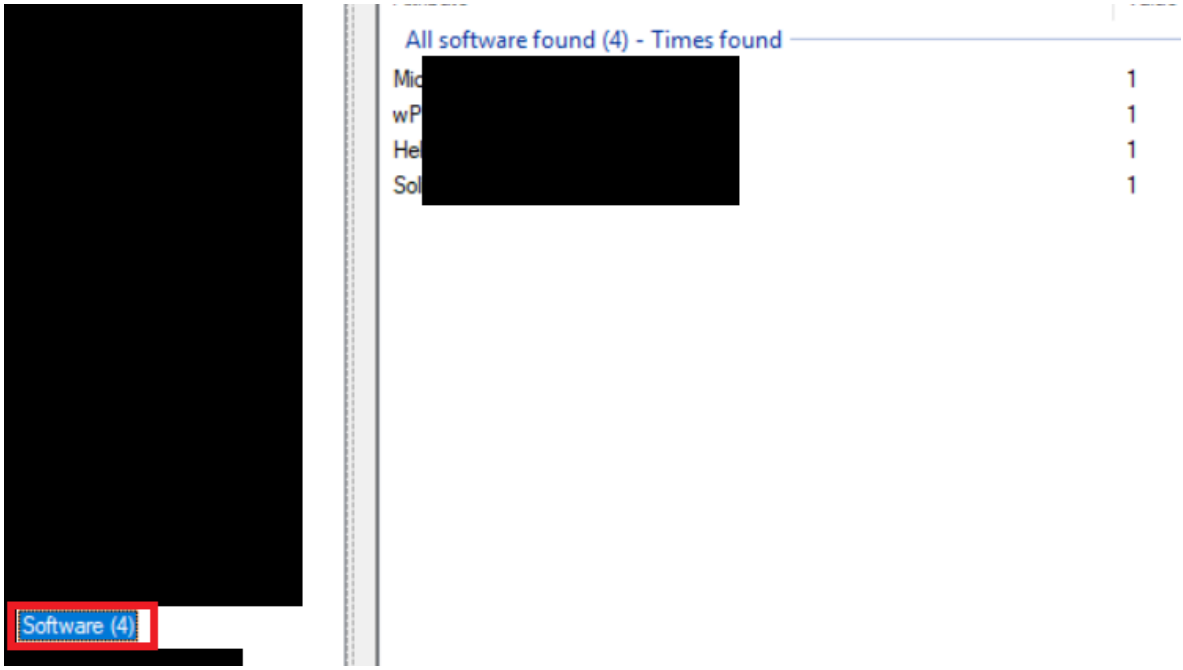


Figura 77. Software descubierto en ALCADÍA CUENCA.

Nombre	Cantidad de Apariciones en Documentos
Microsoft Office	1
wPDF3 by WPCubed GmbH	1
Solid PDF Tools (9.1.6079.1056)	1

Tabla 28. Datos de software descubierto en ALCALDÍA CUENCA.

En la Figura 77. Tenemos los datos del software encontrado en la ALCALDÍA CUENCA, los mismos datos que se encuentran en la Tabla 28, la misma resume datos similares que se pueden apreciar en la Figura 77, pero con la diferencia que en esta tabla se presentan menos datos que en la Figura 77. El software indexa falsos positivos, y en esta tabla están solamente los datos del software eliminando estos falsos positivos.

Como podemos observar en la Tabla 28, en la ALCADÍA CUENCA, logramos obtener los datos del software que se utilizada en la ALCADÍA CUENCA. Se tiene poca información como se ha dicho anteriormente por la poca cantidad de documentos que pueden se pueden examinar, como son apenas 2.

Una vez que se tiene la versión del software con el crean los documentos, cualquier pirata informático pudiera tomar esta información y conseguir el exploit para explotar esta vulnerabilidad.

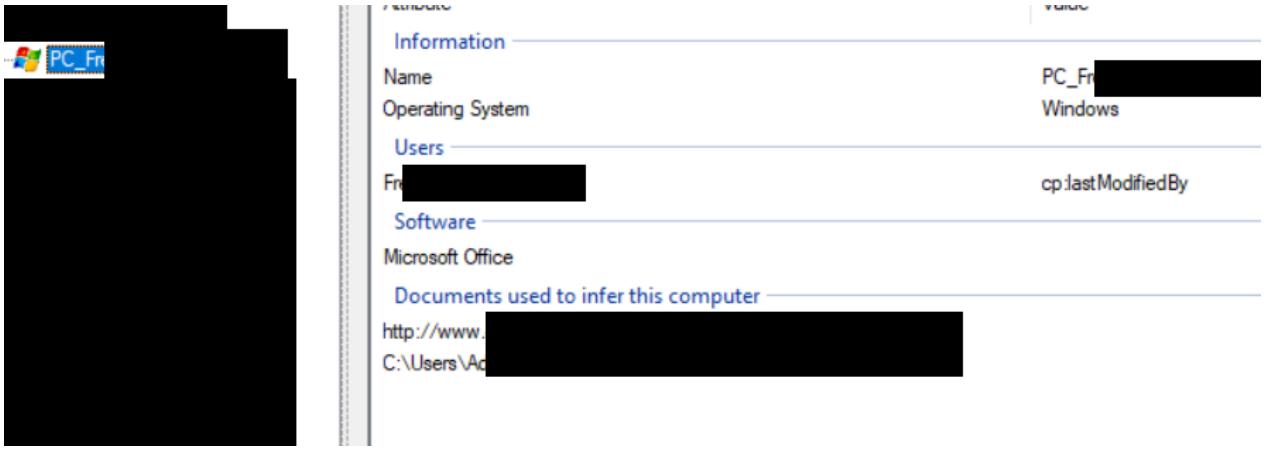


Figura 78. Usuarios descubiertos en ALCADÍA CUENCA.

En la Figura 78. Podemos apreciar que se ha seleccionado un equipo de la toda la lista de equipos de la ALCADÍA CUENCA, solamente por medios de investigación para conocer más a profundidad toda la información que se puede obtener de un usuario y su máquina.

Podemos conocer el nombre del usuario de esa máquina, por lo tanto, el nombre de la persona que trabaja en ALCADÍA CUENCA, en caso de ser más de uno, se podrá visualizar los usuarios pertenecientes a esa máquina. El sistema operativo que tiene esa máquina, en este caso Windows. El software con el que se crea los documentos en este

equipo, como son Microsoft Office. Además de los documentos que han sido creados desde este equipo, este es un punto muy importante pues podemos ver de qué tipo son los archivos y por ejemplo si el enfoque de estos es netamente financiero podemos deducir que esta persona está en el área financiera de la ALCALDÍA CUENCA. Se puede apreciar además que documentos ha creado este usuario.

Conclusiones

Como conclusión inicial del capítulo tenemos que el software de análisis de metadatos nos permite conocer cuáles son los metadatos que se indexan en los documentos informáticos, cual es la información que el usuario está dejando en cada documento que está creando.

Para el análisis de los documentos de las entidades estales seleccionadas, utilizamos LA FOCA, herramienta que nos permite con gran facilidad el análisis de los metadatos en documentos informáticos, y que además permite hacer un análisis de los metadatos para lograr relaciones entre los metadatos y aportarnos información de las entidades estatales seccionadas.

Conseguimos información crítica de los equipos y los usuarios de las entidades estatales, así podemos analizar qué sistema operativo usa qué persona, y generar un ataque dirigido hacia el sistema operativo seleccionado como vector de ataque. Además de obtener información de los servidores encontrados, tanto con direcciones ip o como servidores internos sin dirección ip, podemos conocer que personas tienen acceso a estos servidores, convirtiéndose explícitamente en vectores de ataque de los cibercriminales que pueden conocer las personas con mayores privilegios dentro de las empresas.

Con los documentos que se encontraron, podemos analizar cuáles son las herramientas y que tipos de documentos son los que mayormente se generan, pues puede ser que exista mayor cantidad de archivos creados de un tipo, pero convertidos a otro con distintos softwares que generan fallos de seguridad. Los directorios son otra información que se puede almacenar en los metadatos, nos indica los directorios sobre los que se manejan los trabajadores de las entidades estatales y los directorios personales almacenados por defecto al crear archivos PDF.

Las impresoras son más información que puede ser encontrada en estos documentos, pues cuando se genera una conexión con una impresora y se genera un archivo, automáticamente este archivo almacena los datos de la impresora conectada. Estos equipos tienen versión de sistema de control o incluso acceso por WIFI, lo que permite un vector de ataque para los cibercriminales que logren acceder a los equipos en red con las mismas. Emails, se pueden capturar y dejar por defecto en los metadatos de los archivos, esto generar una fuga de información privilegiada para que cualquier usuario que se descargue estos documentos tenga acceso.

Finalmente tenemos acceso a la información propia de los servidores, esto es muy importante pues podemos conocer cuáles son los usuarios que tiene accesos a estos servidores, y serían los vectores de ataque más importantes. Además, conocemos la información de la versión del software que corre sobre el ismo como es: Apache, Open SSL, PHP, etc. Este mismo proceso se puede realizar con los equipos descubiertos y podemos obtener la información del equipo, nombre del usuario, tipo del sistema operativo, versión del sistema operativo, carpetas, archivos que se han subido desde este equipo, software con el que se crean los documentos, versión de este software.

Toda esta información esta publica en las entidades estatales y es un proceso descrito ya en este capítulo como cualquier usuario puede acceder a esta información.

Un caso de ataque que se pueda dar cuando un equipo tiene cubierto su seguridad, pero dentro de su red existen otros usuarios que no sería el siguiente:

1ero, conoces la versión de la impresora y los posibles fallos de seguridad del mismo para explotarlos y 2do si se conoce que 3 o 4 personas ocupan una misma impresora, se puede deducir que ocupan un espacio físico compartido, por lo tanto se conoce que trabajan en áreas relacionadas dentro de la empresa, por lo que si se desea hacer un ataque dirigido, y el objetivo no es vulnerable pero sus compañeros de área si, se puede atacar a los compañeros y después acceder a la máquina del objetivo por la red interna.

CAPÍTULO 4
4. LA LEGALIDAD ECUATORIANA EN CUANTO A LA OBTENCIÓN DE INFORMACIÓN DE DOCUMENTOS PÚBLICOS

Introducción

La legislación ecuatoriana parte de una estructura jurídica que tiene por principio básico la pirámide kelseniana que ubica la categorización de las normas jurídicas de la siguiente manera: Constitución (Ley Suprema); los tratados y convenios internacionales; las leyes orgánicas; las leyes ordinarias; las normas regionales y las ordenanzas distritales; los decretos y reglamentos; las ordenanzas; los acuerdos y las resoluciones; y los demás actos y decisiones de los poderes públicos (Cevallos, 2017).

Ahora bien, por otro lado, creemos que es necesario resaltar que en esta etapa del desarrollo de la humanidad nos encontramos en una fase que los expertos han dado en llamar "LA SOCIEDAD DE LA INFORMACION Y EL CONOCIMIENTO", por cuanto el parámetro fundamental del desarrollo constituye LA INFORMACION.

Dentro de esta perspectiva, vemos precisamente que gracias al desarrollo de las Tecnologías de la Información y Comunicación, (TICs), la información se genera y almacena, ya no únicamente a través de medios físicos tradicionales, sino también a través de medios informáticos y digitales, que ha permitido hacer más ágiles estos procedimientos, no obstante también han aumentado en la misma proporción, los riesgos propios que conlleva este sistema por posibles ataques, alteraciones, manipulaciones que podrían afectar los principios básicos de los documentos digitales tales como: la integridad, la autenticidad y la disponibilidad de servicios.

La tendencia anterior se ve reforzada por un principio ecologista, sumado al criterio de ahorro de espacio físico; inclusive en ciertos países al igual que en el Ecuador, existen proyectos de oficinas públicas y privadas "CERO PAPELES" con respaldo de información en la NUBE.

Para irnos adentrando en el tema que nos interesa, debemos partir del concepto de DOCUMENTO PUBLICO. De manera general, se puede definir que el documento es un: "Objeto *susceptible de representar una manifestación del pensamiento con prescindencia de la forma en que esa representación se exterioriza*" (GOLDSTEIN, DICCIONARIO JURIDICO CONSULTOR MAGNO, 2014, pág. 231).

De lo anterior, se colige que el documento puede tener dos tipos de representación: física o digital. Al respecto la mayoría de las legislaciones, al igual que la nuestra, han establecido el principio universal de equivalencia funcional, es decir que da el mismo valor como medio de transmisión de información, y como medio de prueba para efectos legales (Cevallos, 2017).

Por otro lado, se conoce como documento público al "*Documento otorgado por un funcionario público o depositario de la fé pública dentro de los límites de su competencia y de acuerdo con las formalidades prescriptas (prescritas) por la ley*" (GOLDSTEIN, DICCIONARIO JURIDICO CONSULTOR MAGNO, 2014, pág. 232)

En el caso ecuatoriano, la legislación considera como sinónimos a la definición de DOCUMENTO e INSTRUMENTO PUBLICO; por tanto, puede tener esta característica un documento que es presentado como informe de actividades de un funcionario público o entidad pública, así como también una escritura realizada por personas particulares ante Notario Público, sin embargo, para el estudio del presente trabajo de investigación, se tomará en cuenta únicamente al documento referido en el primer caso (Cevallos, 2017).

4.1 Análisis de la ley penal ecuatoriana relacionado con la información de documentos públicos

En materia de derecho penal se parte de el aforismo latín, "NULLUM CRIMEN NULLA POENA SINE LEGE", esto significa que no existe crimen tampoco una pena sino existe una ley previa, es decir, que para que una conducta sea sancionada por la ley penal debe estar previamente establecida en el catálogo de delitos que en el caso del ecuador es el código orgánico integral penal, a más de tratados y convenios internacionales. En La legislación penal ecuatoriana no se encuentra prevista una conducta punible que sancione la obtención de metadatos, muy por el contrario, la ley orgánica de transparencia y acceso a la información pública es enfática en mencionar en su artículo 1ero, que el acceso a la información pública es un derecho de las personas que garantiza el estado (Vignolo, 2017)

La legislación penal ecuatoriana tiene como base al CODIGO ORGANICO INTEGRAL PENAL (COIP) que tiene la categoría de ley especial; fue publicada en el Suplemento del Registro Oficial número 180 de 10 de febrero del 2014 (Cevallos, 2017).

Su estructura, contiene una parte que define los diferentes tipos de delitos y las penas aplicables. Existe otro capítulo que se refiere al procedimiento, es decir la manera como debe determinarse la existencia del delito, la responsabilidad en los grados de autor, coautor, cómplice y encubridor; contiene además la forma de aplicar la pena y por último el sistema de rehabilitación social para los condenados (Cevallos, 2017).

Si vemos la estructura jurídica la ley penal ecuatoriana, al igual que la mayoría de las legislaciones en el mundo, debe sujetarse a principios básicos del ser humano como son; el respeto a la vida, la presunción de inocencia, el derecho a la defensa, el derecho a no auto incriminarse; el derecho a no ser juzgado dos veces por la misma causa, el derecho a un debido proceso, el derecho a la honra etc (Cevallos, 2017).

La propia Constitución de la República del Ecuador el año 2008, determina que es necesario transparentar la información de documentos públicos, como una forma de control y auditoria social, por esta razón, se dictó una ley llamada, "LEY ORGANICA DE TRANSPARENCIA Y ACCESO A LA INFORMACION PUBLICA" publicada en el Suplemento del Registro Oficial número 337 del 18 de mayo del 2004, que tiene como objetivo básico que toda la información generada por instituciones públicas o por entidades privadas que manejan información pública, deben ponerlos al alcance de la ciudadanía por medio de portales Web, y con facilidades para su acceso (Cevallos, 2017).

Esta tendencia ha sido reforzada a través de la expedición de otras leyes tales como la "LEY DEL SISTEMA NACIONAL DE REGISTRO DE DATOS PUBLICOS", publicada en el Suplemento del Registro Oficial número 162 del 31 de marzo del 2010, que determina a futuro en forma obligatoria conste en una sola base de datos, la información de entidades tales como: LA FUNCION JUDICIAL, EL MINISTERIO DE RELACIONES LABORALES, MIGRACION, REGISTRO CIVIL, I.E.S.S., S.R.I., REGISTROS DE LA PROPIEDAD Y MERCANTILES, entre otros (Cevallos, 2017).

Ahora bien, dentro de este proceso existe la tendencia de colocar la información a través de portales de acceso informáticos y digitales, inclusive la propia legislación ecuatoriana ha previsto, que el manejo de la información se realice a través de sistemas que garanticen: la autenticidad, la integridad y la disponibilidad del servicio, estableciendo penas agravantes por la acción u omisión que determine responsabilidades de los funcionarios públicos (Cevallos, 2017).

Lo anterior determina que pueda darse las siguientes circunstancias:

1.- Que el documento sea falsificado ya sea por el propio funcionario o por terceras personas.

2.- Que el documento sea alterado por el propio funcionario o por ataque de personas extrañas en el proceso de transmisión de datos.

3.- Que el documento o el sistema presente vulnerabilidades que hagan realidad la amenaza y el resultado final sea la denegación de servicios.

Para el análisis del tema propuesto, dentro de la estructura del Código Orgánico Integral Penal, (COIP), publicado en el Suplemento del Registro Oficial número 180 del 10 de febrero del 2014, se establece como elemento básico el principio de la intención, para determinar la responsabilidad en los diferentes grados como: autor, cómplice o encubridor; y por otro lado la existencia del delito o infracción que debe estar plenamente determinada con anterioridad a la pena es decir como acto antijurídico y punible que lesiona el bien jurídico protegido; por ejemplo en el caso de robo el bien jurídico protegido sería la propiedad o el patrimonio de una persona (Cevallos, 2017).

También existen delitos de acción y omisión; los primeros que son resultado de la actuar intelectual o material del responsable del delito; y los segundos que son resultado de la inacción o por no haber observado las reglas de procedimiento y seguridad por ejemplo en el manejo de la información (Cevallos, 2017).

Debido a la serie de amenazas, vulnerabilidades, ataques, incidentes que están presentes en los sistemas digitales, las empresas tanto públicas como privadas, han adoptado sistemas basados en las NORMAS ISO para aminorar esta situación, más aún cuando las empresas públicas manejan datos personales y sensibles que no pueden ser divulgadas sin el consentimiento de su titular, principio que se establece en la Constitución Ecuatoriana a través de HABEAS DATA y en otras leyes orgánicas conexas (Cevallos, 2017).

Si bien es cierto que nuestra legislación, ha tratado de adaptarse a los cambios que exige la actual "Sociedad de la Información", sin embargo el procedimiento para la elaboración de leyes no ha sido la más óptima, razón por la que generalmente se han copiado modelos adoptados por organismo internacionales tales como la ORGANIZACIÓN MUNDIAL DEL COMERCIO, en el caso de la LEY DE COMERCIO ELECTRONICO, FIRMAS Y MENSAJES DE DATOS, publicada en el Suplemento del Registro Oficial número 557 del 17 de abril del 2002, en donde se

estableció entre otros temas el capítulo de los DELITOS INFORMATICOS, que fue incorporado como un capítulo anexo al entonces Código Penal y luego manteniendo su estructura básica fue plasmada también al nuevo COIP, pero sin definir la esencia del bien jurídico protegido, que calificaría de mejor manera este tipo de delitos como el caso de la legislación colombiana en donde definen como bien jurídico protegido a "LA INFORMACION" (Cevallos, 2017).

Como habíamos dicho anteriormente dentro de la ley penal ecuatoriana el principio básico del delito es:

1.- Un acto antijurídico, es decir contrario a la ley

2.- Típico, que está previamente calificado como delito.

3.- Imputable: es decir que tiene un autor, cómplice y encubridor que actuó o dejo de actuar con conciencia y voluntad

4.- Punible, que es sancionada por la ley con la imposición de una pena.

Haciendo un análisis en el caso de estudio de la INFORMACION QUE CONTIENEN LOS DOCUMENTOS PÚBLICOS INFORMATICOS (dentro de ellos los METADATOS) en la legislación penal ecuatoriana, podemos ver que pueden presentarse las siguientes circunstancias:

A) RESPECTO DEL FUNCIONARIO PUBLICO

1.- El funcionario público, es responsable del manejo de la información (interna y externa) que contiene los documentos públicos.

2.- El funcionario público, debe sujetarse a los procedimientos y controles establecidos en las normas INEN, por lo tanto, debe filtrar los datos internos anexos al documento digital.

3.- El funcionario público, es responsable tanto por su acción como por su inacción tanto en el manejo de la información como en la disponibilidad del sistema.

B) USUARIO ETICO

1.- El usuario accede a la información (interna y externa) que contienen los documentos públicos con fines legales, administrativos e investigativos.

2.- El usuario, respeta los procedimientos legales, accede a sitios públicos sin forzar claves ni contraseñas.

3.- El usuario obtiene datos externos de la información y los utiliza con fines lícitos; también obtiene datos internos que no los divulga, solo utiliza con fines docentes, legales y administrativos

C) USUARIO ATACANTE

1.- El usuario accede a la información (interna y externa) que contienen los documentos públicos con fines ilícitos

2.- El usuario no respeta ningún tipo de regla ni norma, accede tanto a sitios públicos como a otros conexos, forzando claves y contraseñas.

3.- El usuario obtiene datos externos de la información y los utiliza como con fines ilícitos; también obtiene datos internos que los divulga, y utiliza para ataques, alteración de la información y denegación de servicio.

Para el análisis del caso en concreto acerca de la LEY PENAL ECUATORIANA RELACIONADA CON EL ACCESO A LA INFORMACION DE DOCUMENTOS PUBLICOS, nos remitiremos a lo determinado en el artículo 178 del CODIGO INTEGRAL PENAL que expresamente dice:

> *Violación a la intimidad. - La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años.* ***No son aplicables estas normas para la persona que divulgue grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley.*** **(El subrayado es nuestro)** (Asamblea Nacional, CODIGO ORGANICO INTEGRAL PENAL, 2017)

4.2 Análisis de la legalidad ecuatoriana en cuanto a documentos públicos

Todas las leyes que existen deben guardar concordancia con la constitución, de lo que se deduce que la constitución es una especie de ley madre, la misma establece que los ciudadanos tienen el derecho de acceder a la información pública, la misma se

entiende como la información que emana o se encuentra en poder de organismo o instituciones públicas, encontrándose la misma a total disposición de los ciudadanos. La limitante establecida legalmente hace referencia únicamente a la modificación de bases de datos, divulgación de información clasificada o reservada o que afecte a la intimidad personal o circule sin consentimiento de la persona, de lo que se expende que si un documento se encuentra publicado en cualquiera de los soportes informáticos estatales, tiene carácter de público, pudiendo cualquier persona acceder al mismo, analizarlo, estudiarlo, investigarlo siempre y cuando no se modifique su estructura y se circule el mismo modificado (Vignolo, 2017)

Antes de entrar al análisis de este capítulo tenemos que diferenciar entre lo que es legalidad y legislación. La legalidad como su nombre lo dice es todo acto, contrato, procedimiento, que está apegado a las normas determinadas por ley; en cambio la legislación es todo el conjunto de normas y leyes que conformar la estructura jurídica del Estado tales como: la Constitución, los Convenios y Tratados Internacionales, las leyes, los decretos, las ordenanzas etc. (Cevallos, 2017).

En base a lo anteriormente expuesto el objetivo de este capítulo es determinar si existen restricciones o impedimentos de acceso hacia la información interna (metadatos) de los documentos públicos digitales o informáticos.

4.2.1 CONSTITUCION DE LA REPUBLICA

En la sección tercera referida a la COMUNICACIÓN E INFORMACION específicamente el artículo **16** dice:

> *Todas las personas, en forma individual o colectiva, tienen derecho a: 1. Una comunicación libre, intercultural, incluyente, diversa y participativa, en todos los ámbitos de la interacción social, **por cualquier medio y forma**, en su propia lengua y con sus propios símbolos*. 2. *El acceso universal a las tecnologías de información y comunicación…* (Lo subrayado es nuestro). (Asamblea Nacional, CONSTITUCION DE LA REPUBLICA DEL ECUADOR, 2015)

A su vez el artículo **18** dice.

Todas las personas, en forma individual o colectiva, tienen derecho a: 1. Buscar, recibir, intercambiar, producir y difundir información veraz, verificada, oportuna, contextualizada, plural, sin censura previa acerca de los hechos, acontecimientos y procesos de interés general, y con responsabilidad ulterior. 2. ***Acceder libremente a la información generada en entidades públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas. No existirá reserva de información excepto en los casos expresamente establecidos en la ley. En caso de violación a los derechos humanos, ninguna entidad pública negará la información.*** (Lo subrayado es nuestro) (Asamblea Nacional, CONSTITUCION DE LA REPUBLICA DEL ECUADOR, 2015)

La constitución a previsto para los casos en los que se niega el acceso a la información pública, una herramienta conocida como acción de acceso a la información pública, la misma se encuentra contemplada en el artículo 91 de la constitución.

Art. 91*.- La acción de acceso a la información pública tendrá por objeto garantizar el acceso a ella cuando ha sido denegada expresa o tácitamente, o cuando la que se ha proporcionado no sea completa o fidedigna. Podrá ser interpuesta incluso si la negativa se sustenta en el carácter secreto, reservado, confidencial o cualquiera otra clasificación de la información. El carácter reservado de la información deberá ser declarado con anterioridad a la petición, por autoridad competente y de acuerdo con la ley.* (Asamblea Nacional, CONSTITUCION DE LA REPUBLICA DEL ECUADOR, 2015)

La garantía que todos los ciudadanos tienen sobre la obtención de documentos públicos por ley, con la limitante de no modificar y posteriormente divulgar esta modificada.

4.2.2 LEY DE COMERCIO ELECTRONICO, FIRMAS Y MENSAJES DE DATOS

El artículo **9** textualmente dice

Protección de datos. - Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros. La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y

confidencialidad garantizados por la Constitución Política de la República y esta ley, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente. ***No será preciso el consentimiento para recopilar datos personales de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de la administración pública, en el ámbito de su competencia, y cuando se refieran a personas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato****.* (El subrayado es nuestro) (Congreso Nacional, 2014)

4.2.3 ACUERDO MINISTERIAL SOBRE ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACION EGSI

Esta misma ley dentro de la sección de GLOSARIO DE TERMINOS refiriéndose a la DISPONIBILIDAD dice: "***Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran***." (Adminitración Pública Central, 2016)

4.2.4 LEY SISTEMA NACIONAL DE REGISTRO DE DATOS PUBLICOS

El artículo 28 dice:

Creación, finalidades y objetivos del Sistema Nacional de Registro de Datos Públicos. - Créase el Sistema Nacional de Registro de Datos Públicos con la finalidad de proteger los derechos constituidos, los que se constituyan, modifiquen, extingan y publiciten por efectos de la inscripción de los hechos, actos y/o contratos determinados por la presente Ley y las leyes y normas de registros; y con el objeto de coordinar el intercambio de información de los registros de datos públicos. En el caso de que entidades privadas posean información que por su naturaleza sea pública, serán incorporadas a este sistema. Con la finalidad de garantizar el ejercicio del derecho constitucional del acceso a la información, se crea la Ficha de Registro Único del Ciudadano, documento público electrónico y/o físico certificado, que contendrá los datos de registro público del ciudadano constantes en el Sistema Nacional de Registro de Datos Públicos. La Ficha de Registro Único del Ciudadano, no sustituye los documentos legalmente establecidos; pero se constituye en documento público de consulta del ciudadano y documento de

consulta y verificación obligatoria de las entidades y empresas públicas, para la prestación de servicios al ciudadano. (Asamblea Nacional, LEY DEL SISTEMA NACIONAL DE REGISTRO DE DATOS PUBLICOS, 2014)

4.2.5 LEY DE ACCESO A LA INFORMACION PUBLICA Y TRANSPARENCIA

Art. 1.- ***Principio de Publicidad de la Información Pública***. - *El acceso a la información pública es un derecho de las personas que garantiza el Estado. Toda la información que emane o que esté en poder de las instituciones, organismos y entidades, personas jurídicas de derecho público o privado que, para el tema materia de la información tengan participación del Estado o sean concesionarios de éste, en cualquiera de sus modalidades, conforme lo dispone la Ley Orgánica de la Contraloría General del Estado; las organizaciones de trabajadores y servidores de las instituciones del Estado, instituciones de educación superior que perciban rentas del Estado, las denominadas organizaciones no gubernamentales (ONGs), están sometidas al principio de publicidad; por lo tanto, toda información que posean es pública, salvo las excepciones establecidas en esta Ley*. (Lucio Gutiérrez, 2005)

Art. 4.- ***Principios de Aplicación de la Ley***.- *En el desarrollo del derecho de acceso a la información pública se observarán los siguientes principios:*
a) La información pública pertenece a los ciudadanos y ciudadanas. El Estado y las instituciones privada depositarias de archivos públicos, son sus administradores y están obligados a garantizar el acceso a la información … (Lucio Gutiérrez, 2005)

Art. 10.-***Custodia de la Información***.- *Es responsabilidad de las instituciones públicas, personas jurídicas de derecho público y demás entes señalados en el artículo 1 de la presente Ley, crear y mantener registros públicos de manera profesional, para que el derecho a la información se pueda ejercer a plenitud, por lo que, en ningún caso se justificará la ausencia de normas técnicas en el manejo y archivo de la información y documentación para impedir u obstaculizar el ejercicio de acceso a la información pública, peor aún su destrucción.*
Quienes administren, manejen, archiven o conserven información pública, serán personalmente responsables, solidariamente con la autoridad de la dependencia a

la que pertenece dicha información y/o documentación, por las consecuencias civiles, administrativas o penales a que pudiera haber lugar, por sus acciones u omisiones, en la ocultación, alteración, pérdida y/o desmembración de documentación e información pública. Los documentos originales deberán permanecer en las dependencias a las que pertenezcan, hasta que sean transferidas a los archivos generales o Archivo Nacional. (Lucio Gutiérrez, 2005)

Conclusiones

Como conclusión podríamos manifestar que el ACCESO A LA INFORMACIÓN DE DOCUMENTOS PÚBLICOS, es una garantía constitucional, que está igualmente plasmada en la legislación penal ecuatoriana, claro siempre y cuando cumpla con los preceptos legales, reglamentarios y de procedimiento para la obtención de la misma.

Además, que el ACCESO A LA INFORMACIÓN DE DOCUMENTOS PÚBLICOS ya sea físicos o digitales, es una garantía constitucional, a la que el ciudadano tiene libre acceso, principio que está reglamentado igualmente en las diferentes leyes tanto especiales como ordinarias, al igual que en los acuerdos, ordenanzas, reglamentos, decretos, pero siempre y cuando cumpla con los preceptos legales, reglamentarios y de procedimiento para la obtener dicha información.

Como se pudo conocer en este capítulo, el ACCESO A LA INFORMACIÓN DE DOCUMENTOS PÚBLICOS no se refiere solamente a documentos de entidades públicas, sino a todos los documentos que se generen con entidades privadas u ONGs que perciban dinero del estado, por lo tanto, la muestra de obtención de metadatos crece y no solo se refiere a entidades públicas. Con esto se puede conocer que más entidades públicas o privadas pueden ser víctimas de estas vulnerabilidades en documentos públicos.

CAPÍTULO 5
5. CONCLUSIONES

El Ecuador pocos años atrás, se cambia a la modernización y equipamiento de TICS, sobre todo del compromiso del gobierno al implementar el Plan Nacional de Telecomunicaciones y Tecnologías de Información del Ecuador 2016-2021. Con esto se puede comprender que el país cada vez se suma a la globalización y al cambio tecnológico, a esta actualización global que todo país requiere para ser parte de un mundo globalizado y esto implica que se tiene una mayor cantidad de vectores de posibles ataques a estos equipos y es obligación del gobierno, autoridades y la sociedad en general estar conscientes de los posibles problemas que se puedan presentar, prevenir estos problemas y planes de respuesta en caso de incidentes.

Azuay al encontrarse como cuarta provincia con mayor uso de TICS en el país, es un objetivo principal para cibercriminales que desean obtener acceso a información privilegiada de manera ilegítima, con esto poner en riesgo información de los ciudadanos. Existe entidades públicas que, por ley, manejan la información de los ciudadanos y esta puede llegar en algún punto, ser filtrada por cibercriminales.

Estas cifras nos demuestran la importancia que debemos tener como ciudadanos sobre los contras que se presentan en la globalización y que como ciudadanos debemos exigir a nuestras autoridades control sobre la documentación de todos los ciudadanos.

Proponemos una hipótesis que los documentos públicos de las entidades estatales si son vulnerables a fuga de información, Para comprensión se puede entender que los metadatos que son la base fundamental de la hipótesis. Los metadatos son datos de los datos, por lo tanto, aportan gran información para manejo de grandes cantidades de información, pero a su vez al ser públicos exponen estos datos para ser accedidos por cualquier usuario que lo dese, información que es intrínseca de un documento informático desde su creación.

Planteamos la eliminación de los metadatos como una medida de mitigación mediante la eliminación de los mismo, tanto en documentos office como en documentos PDF, que son los tipos de archivos públicos más utilizados de acuerdo con la investigación. Con este proceso manual se puede eliminar gran parte de los metadatos, sobre todo, los más importantes respecto a revelar información de las entidades públicas.

El software de análisis de metadatos nos permite conocer cuáles son los metadatos que se indexan en los documentos informáticos, cual es la información que el usuario está dejando en cada documento que está creando.

Para el análisis de los documentos de las entidades estales seleccionadas, utilizamos LA FOCA, herramienta que nos permite con gran facilidad el análisis de los metadatos en documentos informáticos, y que además permite hacer un análisis de los metadatos para lograr relaciones entre los metadatos y aportarnos información de las entidades estatales seccionadas.

Conseguimos información crítica de los equipos y los usuarios de las entidades estatales, así podemos analizar qué sistema operativo usan qué persona, y generar un ataque dirigido hacia el sistema operativo seleccionado como vector de ataque. Además de obtener información de los servidores encontrados, tanto con direcciones ip o como servidores internos sin dirección ip, podemos conocer que personas tienen acceso a estos servidores, convirtiéndose explícitamente en vectores de ataque de los cibercriminales que pueden conocer las personas con mayores privilegios dentro de las empresas.

Con los documentos que se encontraron, podemos analizar cuáles son las herramientas y que tipos de documentos son los que mayormente se generan, pues puede ser que exista mayor cantidad de archivos creados de un tipo, pero convertidos a otro con distintos softwares que generan fallos de seguridad. Los directorios son otra información que se puede almacenar en los metadatos, nos indica los directorios sobre los que se manejan los trabajadores de las entidades estatales y los directorios personales almacenados por defecto al crear archivos PDF.

Las impresoras son más información que puede ser encontrada en estos documentos, pues cuando se genera una conexión con una impresora y se genera un archivo, automáticamente este archivo almacena los datos de la impresora conectada. Estos equipos tienen versión de sistema de control o incluso acceso por WIFI, lo que permite un vector de ataque para los cibercriminales que logren acceder a los equipos en red con las mismas. Emails, se pueden capturar y dejar por defecto en los metadatos de los archivos, esto generar una fuga de información privilegiada para que cualquier usuario que se descargue estos documentos tenga acceso.

Tenemos acceso a la información propia de los servidores, esto es muy importante pues podemos conocer cuáles son los usuarios que tiene accesos a estos servidores, y serían los vectores de ataque más importantes. Además, conocemos la información de la versión del software que corre sobre el ismo como es: Apache, Open SSL, PHP, etc. Este mismo proceso se puede realizar con los equipos descubiertos y podemos obtener la información del equipo, nombre del usuario, tipo del sistema operativo, versión del sistema operativo, carpetas, archivos que se han subido desde este equipo, software con el que se crean los documentos, versión de este software.

Como conclusión de la parte legal podríamos manifestar que el ACCESO A LA INFORMACIÓN DE DOCUMENTOS PÚBLICOS, es una garantía constitucional, que está igualmente plasmada en la legislación penal ecuatoriana, claro siempre y cuando cumpla con los preceptos legales, reglamentarios y de procedimiento para la obtención de la misma.

Además, que el ACCESO A LA INFORMACIÓN DE DOCUMENTOS PÚBLICOS ya sea físicos o digitales, es una garantía constitucional, a la que el ciudadano tiene libre acceso, principio que está reglamentado igualmente en las diferentes leyes tanto especiales como ordinarias, al igual que en los acuerdos, ordenanzas, reglamentos, decretos, pero siempre y cuando cumpla con los preceptos legales, reglamentarios y de procedimiento para la obtener dicha información.

Como se pudo conocer en este capítulo, el ACCESO A LA INFORMACIÓN DE DOCUMENTOS PÚBLICOS no se refiere solamente a documentos de entidades públicas, sino a todos los documentos que se generen con entidades privadas u ONGs que perciban dinero del estado, por lo tanto, la muestra de obtención de metadatos crece y no solo se refiere a entidades públicas. Con esto se puede conocer que más entidades públicas o privadas pueden ser víctimas de estas vulnerabilidades en documentos públicos.

Además, como conclusión podemos conocer que el acceso a los metadatos de DOCUMENTOS PUBLICOS no es un delito tipificado en el Código Integral Penal, por lo tanto, la práctica de la extracción de metadatos no está penada por la ley.

CAPÍTULO 6
6. BIBLIOGRAFIA

Adminitración Pública Central. (2016). *ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACION EGSI.* Quito.

Adobe. (15 de 11 de 2017). *Adobe Support.* Obtenido de Adobe Support: https://help.adobe.com/es_ES/acrobat/pro/using/WS58a04a822e3e50102bd615109794195ff-7c63.w.html

Alonso, C., González, P., Palop, I., Rando, E., Alonso, R., Moreno, J., & Fernández, M. (2013). *Pentesting con FOCA.* Móstoles: 0xWord.

Asamblea Nacional. (2014). *LEY DEL SISTEMA NACIONAL DE REGISTRO DE DATOS PUBLICOS.* Quito.

Asamblea Nacional. (2015). *CONSTITUCION DE LA REPUBLICA DEL ECUADOR.* Quito.

Asamblea Nacional. (2017). *CODIGO ORGANICO INTEGRAL PENAL.* Quito.

Baca, M. (2016). *Introduction to Metadata.* Los Angeles, California: Getty Publications.

Censos, I. N. (2016). *Tecnologías de la Información y Comunicaciones (TIC's) 2016.* Obtenido de http://www.ecuadorencifras.gob.ec: http://www.ecuadorencifras.gob.ec/documentos/web-inec/Estadisticas_Sociales/TIC/2016/170125.Presentacion_Tics_2016.pdf

Cevallos, E. (19 de 11 de 2017). Doctor. (C. Flores, Entrevistador)

Congreso Nacional. (2014). *LEY DE COMERCIO ELECTRONICO, FIRMAS Y MENSAJES DE DATOS.* Quito.

Gartner, R. (2016). *Metadata, Shaping Knowledge from Antiquity to the Semantic Web.* Londres: Springer International.

GOLDSTEIN, M. (2014). DICCIONARIO JURIDICO CONSULTOR MAGNO. En M. GOLDSTEIN, *DICCIONARIO JURIDICO CONSULTOR MAGNO* (pág. 232). CIRCULO LATINO AUSTRAL.

GOLDSTEIN, M. (2014). DICCIONARIO JURIDICO CONSULTOR MAGNO. En M. GOLDSTEIN, *DICCIONARIO JURIDICO CONSULTOR MAGNO* (pág. 231). CIRCULO LATINO AUSTRAL.

Google. (15 de 11 de 2017). *Google Inside.* Obtenido de Google Inside: https://www.google.com/intl/es/insidesearch/howsearchworks/crawling-indexing.html

Información, M. d. (14 de 07 de 2017). *Ministerio de Telecomunicaciones y de la Sociedad de la Información* . Obtenido de Plan nacional de telecomunicaciones y tecnologías de información del Ecuador 2016-2-21: https://www.telecomunicaciones.gob.ec/wp-content/uploads/2016/08/Plan-de-Telecomunicaciones-y-TI..pdf

Lucio Gutiérrez. (2005). *REGLAMENTO A LEY DE TRANSPARENCIA Y ACCESO A INFORMACION PUBLICA.* Quito.

Meeuwisse, R. (2017). *Cybersecurity for Beginners.* Kent,UK: Cybersimplicity.

Navarro, M. (1 de 11 de 2017). *e-Library and Information Science.* Obtenido de e-Library and Information Science: http://eprints.rclis.org/19449/1/Esteban.pdf

ObservatorioTIC. (14 de 7 de 2017). *Ministerio de Telecomunicaciones y de la Sociedad de la Información*. Obtenido de Observatorio TIC: https://observatoriotic.mintel.gob.ec/estadistica/

Pomerantz, J. (2015). *Metadata, The MIT Press Essential Knowledge Series.* Cambridge, Massachusetts: MIT Press.

Rodríguez Bravo, B. (1 de 11 de 2017). *Universidad de Murcia.* Obtenido de Universidad de Murcia: http://revistas.um.es/analesdoc/article/view/1251/1301

Serra Serra, J. (1 de 11 de 2017). *Universidad de Barcelona.* Obtenido de Universidad de Barcelona: http://diposit.ub.edu/dspace/handle/2445/24347

Telefonica. (1 de 12 de 2017). *Telefonica Digital Espana.* Obtenido de Elevenpaths: https://www.elevenpaths.com/es/labstools/foca-2/index.html

Vignolo, G. (13 de 11 de 2017). Abogado Penalista. (C. Flores, Entrevistador)

Doctora Jenny Ríos Coello, Secretaria de la Facultad de Ciencias de la Administración de la Universidad del Azuay

C E R T I F I C A:

Que, el Consejo de Facultad en sesión del 29 de mayo de 2017, conoció la petición del estudiante **CHRISTIAN PAUL FLORES TERREROS** con código **62850**, que presenta el diseño de su trabajo de titulación denominado: ***"DIAGNÓSTICO DE VULNERABILIDADES DE INFORMACIÓN EN DOCUMENTOS PÚBLICOS DE ENTIDADES DEL SECTOR PÚBLICO DE LA CIUDAD DE CUENCA"***, presentado previa a la obtención del título de Ingeniero de Sistemas y Telemática.- El Consejo de Facultad acogió el informe de la Junta Académica de Ingeniería de Sistemas y Telemática y resolvió aprobar el diseño. Designa como **Director al ingeniero Pablo Pintado Zumba** y como miembros del Tribunal Examinador a los ingenieros Francisco Salgado Arteaga, Ph.D. y Esteban Crespo Martínez.- En esta misma sesión el Consejo de Facultad fija como plazo para la entrega del trabajo de titulación, seis meses contados desde la fecha de su aprobación, esto es hasta el **29 de noviembre de 2017,** debiendo el Director presentar a la Junta Académica, dos informes bimensuales del desarrollo del trabajo de titulación.

Cuenca, mayo 30 de 2017

Dra. Jenny Ríos Coello
Secretaria de la Facultad de
Ciencias de la Administración

Decano de la Facultad de Ciencias de la Administración, Cuenca, 24 de noviembre de 2017.- Con autorización amplia y suficiente concedida por el Consejo de Facultad en sesión del 25 de febrero de 2016, conoció la petición del estudiante **CHRISTIAN PAUL FLORES TERREROS** con código 62850, quien solicita prórroga para la presentación del trabajo de titulación denominado: "***DIAGNOSTICO DE VULNERABILIDADES DE INFORMACIÓN EN DOCUMENTOS PUBLICOS DE ENTIDADES DEL SECTOR PUBLICO DE LA CIUDAD DE CUENCA***", previo a la obtención del título de Ingeniero de Sistemas y Telemática, cuyo plazo de presentación vence el 29 de noviembre de 2017, en apego al Reglamento de Régimen Académico y la normativa Institucional, *resuelve aprobar la solicitud y conceder una prórroga de seis meses, esto es* ***hasta el 29 de mayo de 2018.***

Ing. Oswaldo Merchán Manzano
Decano de la Facultad de
Ciencias de la Administración

rcr.-

CONVOCATORIA

Por disposición de la Junta Académica de **Ingeniería de Sistemas y Telemática**, se convoca a los Miembros del Tribunal Examinador, a la sustentación del Protocolo del Trabajo de Titulación: **"DIAGNÓSTICO DE VULNERABILIDADES DE INFORMACIÓN EN DOCUMENTOS PÚBLICOS DE ENTIDADES DEL SECTOR PÚBLICO DE LA CIUDAD DE CUENCA"**, presentado por el estudiante **Christian Paul Flores Terreros**, previa a la obtención del grado de **Ingeniero en Sistemas y Telemática**, para el día **LUNES 15 DE MAYO DE 2017 A LAS 07h00.** La sustentación se realizará en el **laboratorio del IERSE.**

Cuenca, 10 de mayo de 2017

Dra. Jenny Ríos Coello
Secretaria de la Facultad

Ing. Pablo Pintado Zumba .....

Ing. Esteban Crespo Martínez .....

Dr. Francisco Salgado Arteaga Francisco Salgado .....

mjmr/

Comunicado 19-05-2017

Oficio Nro. 059-2017-DIST-UDA

Cuenca, 12 de mayo de 2017

Señor Ingeniero
Oswaldo Merchán Manzano
DECANO DE LA FACULTAD DE CIENCIAS DE LA ADMINISTRACIÓN
Presente.-

De nuestras consideraciones:

La Junta Académica de la Escuela de Ingeniería de Sistemas y Telemática, reunida el día 12 de mayo del 2017, recibió el proyecto de tesis titulado "Diagnóstico de vulnerabilidades de información en documentos públicos de entidades del sector público de la ciudad de Cuenca", presentado por Christian Paul Flores Terreros estudiante de la Escuela de Ingeniería de Sistemas y Telemática, y revisado por el Ing. Pablo Pintado, previo a la obtención del título de Ingeniero de Sistemas y Telemática.

Por lo expuesto, y de conformidad con el Reglamento de Graduación de la Facultad, recomendamos como director y responsable de aplicar cualquier modificación al diseño del trabajo de graduación posterior al Ing. Pablo Pintado y como miembros del Tribunal a Francisco Salgado Ph.D. e Ing. Esteban Crespo.

Atentamente,

Ing. Marcos Orellana Cordero
Cordinador Escuela de Ingeniería de Sistemas y Telemática
Universidad del Azuay

ACTA

SUSTENTACIÓN DE PROTOCOLO/DENUNCIA DEL TRABAJO DE TITULACIÓN

1.1 **Nombre del estudiante: Christian Paul Flores Terreros**
1.2 **Director sugerido**: Ing. Pablo Pintado Zumba
1.3 **Codirector (opcional)**: _____
1.4 **Tribunal:** Ing. Esteban Crespo Martínez/ Dr. Francisco Salgado Arteaga
1.5 **Título propuesto: "DIAGNÓSTICO DE VULNERABILIDADES DE INFORMACIÓN EN DOCUMENTOS PÚBLICOS DE ENTIDADES DEL SECTOR PÚBLICO DE LA CIUDAD DE CUENCA"**
1.6 **Resolución:**

1.6.1 Aceptado sin modificaciones ✓

1.6.2 Aceptado con las siguientes modificaciones:

_____

_____

_____

1.6.3 Responsable de dar seguimiento a las modificaciones: Ing. Pablo Pintado Zumba
1.6.4 No aceptado
- Justificación:

_____
_____
_____

Tribunal

.....	.....	.....
Ing. Pablo Pintado Zumba	Ing. Esteban Crespo Martínez	Dr. Francisco Salgado Arteaga

.....
Sr. Christian Paul Flores Terreros

Dra. Jenny Ríos Coello
Secretario de Facultad

Fecha de sustentación: día **LUNES 15 DE MAYO DE 2017 A LAS 07h00**

UNIVERSIDAD DEL AZUAY

RÚBRICA PARA LA EVALUACIÓN DEL PROTOCOLO DE TRABAJO DE TITULACIÓN

1.1 Nombre del estudiante: Christian Paul Flores Terreros
1.2 Director sugerido: Ing. Pablo Pintado Zumba
1.3 Codirector (opcional):
1.4 Título propuesto: "DIAGNÓSTICO DE VULNERABILIDADES DE INFORMACIÓN EN DOCUMENTOS PÚBLICOS DE ENTIDADES DEL SECTOR PÚBLICO DE LA CIUDAD DE CUENCA"
1.5 Revisores (tribunal): Ing. Esteban Crespo Martínez/ Dr. Francisco Salgado Arteaga

1.6 Recomendaciones generales de la revisión:

	Cumple totalmente	Cumple parcialmente	No cumple	Observaciones (*)
Línea de investigación				
1. ¿El contenido se enmarca en la línea de investigación seleccionada?	✓			
Título Propuesto				
2. ¿Es informativo?				
3. ¿Es conciso?	✓			
Estado del arte				
4. ¿Identifica claramente el contexto histórico, científico, global y regional del tema del trabajo?	✓			
5. ¿Describe la teoría en la que se enmarca el trabajo	✓			
6. ¿Describe los trabajos relacionados más relevantes?	✓			
7. ¿Utiliza citas bibliográficas?	✓			
Problemática y/o pregunta de investigación				
8. ¿Presenta una descripción precisa y clara?	✓			
9. ¿Tiene relevancia profesional y social?	✓			
Hipótesis (opcional)				
10.¿Se expresa de forma clara?	✓			
11.¿Es factible de verificación?	✓			
Objetivo general				
12.¿Concuerda con el problema formulado?	✓			
13.¿Se encuentra redactado en tiempo verbal infinitivo?	✓			

Objetivos específicos				
14.¿Concuerdan con el objetivo general?	✓			
15.¿Son comprobables cualitativa o cuantitativamente?	✓			
Metodología				
16.¿Se encuentran disponibles los datos y materiales mencionados?	✓			
17.¿Las actividades se presentan siguiendo una secuencia lógica?	✓			
18.¿Las actividades permitirán la consecución de los objetivos específicos planteados?	✓			
19.¿Los datos, materiales y actividades mencionadas son adecuados para resolver el problema formulado?	✓			
Resultados esperados				
20.¿Son relevantes para resolver o contribuir con el problema formulado?	✓			
21.¿Concuerdan con los objetivos específicos?	✓			
22.¿Se detalla la forma de presentación de los resultados?	✓			
23.¿Los resultados esperados son consecuencia, en todos los casos, de las actividades mencionadas?	✓			
Supuestos y riesgos				
24.¿Se mencionan los supuestos y riesgos más relevantes?	✓			
25.¿Es conveniente llevar a cabo el trabajo dado los supuestos y riesgos mencionados?	✓			
Presupuesto				N/A
26.¿El presupuesto es razonable?				
27.¿Se consideran los rubros más relevantes?				
Cronograma				
28.¿Los plazos para las actividades son realistas?	✓			
Referencias				
29.¿Se siguen las recomendaciones de normas internacionales para citar?	✓			
Expresión escrita				
30.¿La redacción es clara y fácilmente comprensible?	✓			
31.¿El texto se encuentra libre de faltas ortográficas?		✓		

(*) Breve justificación, explicación o recomendación.

- Opcional cuando cumple totalmente,
- Obligatorio cuando cumple parcialmente y NO cumple.

.....

.....

.....

Ing. Pablo Pintado Zumba Ing. Esteban Crespo Martínez Dr. Francisco Salgado Arteaga

Lugar de Almacenamiento	Retención	Disposición Final
F: Archivo Secretaría de la Facultad	5 años	Almacenar en archivo pasivo de la Facultad

Cuenca, 12 de mayo de 2017

Ingeniero,
Oswaldo Merchán Manzano
DECANO DE LA FACULTAD DE CIENCIAS DE LA ADMINISTRACIÓN
UNIVERSIDAD DEL AZUAY

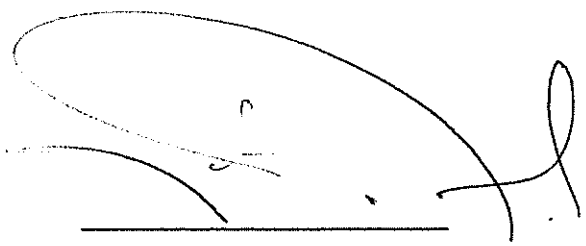
De mi consideración,

Yo, **Pablo Fernando Pintado Zumba** informo que he revisado el protocolo de trabajo de titulación previo a la obtención del título de Ingeniero en Sistemas y Telemática, denominado **"DIAGNOSTICO DE VULNERABILIDADES DE INFORMACION EN DOCUMENTOS PUBLICOS DE ENTIDADES DEL SECTOR PUBLICO DE LA CIUDAD DE CUENCA"**, realizado por el estudiante **Christian Paul Flores Terreros** con código estudiantil 62850, protocolo que a mi criterio, cumple con los lineamientos y requerimientos establecidos por la carrera.

Por lo expuesto, me permito sugerir que sea considerado para la revisión y sustentación del mismo,

Sin otro particular, suscribo.

Atentamente



Ing. Pablo Pintado

UNIVERSIDAD DEL AZUAY

Escuela Sistemas y Telemática	**Oficio Estudiante: Solicitud aprobación de Protocolo de Trabajo de Titulación**	IST-RE-EST-02 Versión 01 04/04/2017 Página 1 de 1

Lugar de Almacenamiento	Retención	Disposición Final
F: Archivo Secretaría de la Facultad	5 años	Almacenar en archivo pasivo de la Facultad

Cuenca, 12 de mayo de 2017

Ingeniero,
Oswaldo Merchán Manzano
DECANO DE LA FACULTAD DE CIENCIAS DE LA ADMINISTRACIÓN
UNIVERSIDAD DEL AZUAY

De mi/ nuestra consideración,

Estimado Señor Decano, yo **Christian Paul Flores Terreros** con C.I. **0105500227**, código estudiantil 62850; estudiante de la Carrera de Sistemas y Telemática, solicito muy comedidamente a usted y por su intermedio al Consejo de Facultad, la aprobación del protocolo de trabajo de titulación con el tema **"DIAGNOSTICO DE VULNERABILIDADES DE INFORMACION EN DOCUMENTOS PUBLICOS DE ENTIDADES DEL SECTOR PUBLICO DE LA CIUDAD DE CUENCA"** previo a la obtención del título de Ingeniero en Sistemas y Telemática para lo cual adjunto la documentación respectiva.

Por la favorable acogida que brinde a la presente, anticipo mi agradecimiento.

Atentamente:

Christian Flores

Estudiante de la Carrera de Sistemas y Telemática

Edición autorizada de 10.000 ejemplares
Del 788.501 al 798.500 N° 0796057

UNIVERSIDAD DEL AZUAY

DOCTORA JENNY RIOS COELLO, SECRETARIA DE LA FACULTAD DE CIENCIAS DE LA ADMINISTRACION DE LA UNIVERSIDAD DEL AZUAY

C E R T I F I C A:

Que, el señor **FLORES TERREROS CHRISTIAN PAUL,** con código **62850,** alumno de la escuela de **INGENIERIA DE SISTEMAS Y TELEMATICA,** tiene aprobado más del 80% de los créditos de su malla de estudios.

Que, al señor **FLORES TERREROS CHRISTIAN PAUL,** le falta aprobar las siguientes asignaturas para finalizar sus estudios:

PRODUCCIÓN II

SISTEMAS DE INFORMACIÓN GERENCIAL

PROYECTOS TELEMÁTICOS

CALIDAD DE SOFTWARE

INGENIERÍA DE SOFTWARE II

METODOLOGIA DE LA INVESTIGACION

Cuenca, 11 de mayo de 2017

Derecho No. **001-001-000156978**

Edición autorizada de 10.000 ejemplares
Del 788.501 al 798.500 Nº 0796052

UNIVERSIDAD DEL AZUAY

1. DATOS GENERALES

1.1 Nombre del estudiante: Christian Paul Flores Terreros

1.1.1 Código: 62850

1.1.2 Contacto:

Teléfono convencional: 4102343

Celular: 0992523733

Correo electrónico: chris.ft1993@hotmail.com

1.2 Director sugerido: Ing. Pablo Fernando Pintado Zumba.

1.2.1 Contacto:

Teléfono convencional:

Celular: 0997031452

Correo electrónico: pablopintado@hotmail.com

1.3 Co-director sugerido:

1.3.1 Contacto:

Correo electrónico: francisco.salgado@fulbrightmail.org

1.4 Asesor metodológico: (opcional).

1.5 Tribunal designado:

1.6 Aprobación: Junta Académica:

Consejo de Facultad:

1.7 Línea de Investigación de la carrera:

1.7.1 Código UNESCO: 1203 Ciencia de los Ordenadores.

1203.99 Sistemas de Seguridad de la Información.

1.7.2 Tipo de trabajo: Tesis en el campo formativo.

UNIVERSIDAD DEL AZUAY

1.8 Área de estudio: Casos prácticos de seguridad de información aplicado a entidades públicas.

1.9 Título propuesto:

Diagnóstico de vulnerabilidades de información en documentos públicos de entidades del sector público de la ciudad de Cuenca.

1.10 Subtítulo: Obtención, análisis y recomendaciones de información privilegiada a partir de documentos públicos que se encuentran en páginas web estatales dentro de la ciudad de Cuenca, así como la legalidad, y repercusión jurídica de captar esta información.

1.11 Estado del proyecto: Se trata de una investigación para comprobar la hipótesis de que existe información privilegiada de entidades, que puede ser sustraída de manera legal mediante el uso de un programa software, se analizará mediante pruebas el alcance que se puede llegar a tener de comprobar que la hipostasis es verdadera y como maneja el ámbito jurídico ecuatoriano este tipo de casos.

2. CONTENIDO

2.1 Motivación de la investigación:

Los puntos a tratar de esas tesis son la preocupación de la seguridad informática en documentos públicos que se generan en entidades públicas en Ecuador, específicamente en la ciudad de Cuenca, con el fin de prevenir ataques a estas entidades, ya que las mismas disponen información de todos los ciudadanos.

2.2 Problemática:

Los piratas informáticos día a día encuentran nuevas técnicas para vulnerar la seguridad tanto de personas como de empresas, y la seguridad informática es la encargada de contrarrestar estos problemas. Los documentos públicos son vector de ataque que los piratas informáticos pueden utilizar para acceder a información privilegia de las empresas. Es trabajo de los encargados de la seguridad informática de las empresas combatir esa problemática.

UNIVERSIDAD DEL AZUAY

2.3 Pregunta de Investigación

¿Los documentos públicos de las entidades públicas están libres de metadatos que generen vulnerabilidades de acceso?

2.4 Resumen

Los documentos públicos son una parte importante de las empresas públicas en la ciudad, pues aportan información de importancia para los ciudadanos o información que las empresas piensen que son pertinentes para los ciudadanos.

El problema con estos documentos es que son publicados en Internet sin ningún tipo de análisis o protección sobre sus metadatos, estos al ser manipulados pueden entregar información importante sobre las empresas y convertir esta en un vector de ataque para cualquier pirata informático que tenga acceso a esa información.

2.5 Indagación previa

Las políticas de seguridad son generalmente un documento de especificación o reglas que se deben conocer por parte del equipo de seguridad de la información, generalmente estas políticas cubren una sola área específica. La documentación de seguridad de la información forma parte importante dentro de la empresa. Además está demostrado que varias de las brechas de seguridad se generan en las empresas, no por el hecho de no disponer de políticas de seguridad, sino que los empleados no las conozcan o las comprendan, pues como se conoce, siempre el factor humano será el eslabón más débil en la cadena de la seguridad informática. (Alotaibi, Furnell, & Clarke, IEEE Explorer)

En la implementación de las Tecnologías de la Información y Comunicación (TICs), la implementación de la seguridad de la información es muy importante, considerando que el rendimiento de las TICs se puede ver interrumpido por el riesgo seguridad de la información. Dentro del gobierno de TICs la seguridad es de vital importancia pues comprende los dominios de confidencialidad, integridad y disponibilidad. (Budi Setiawan, Syamsudin, & Sasongko Sastrosubroto)

La Sociedad Española de Documentación e Información Científica (SEDIC), ha definido el termino metadato como "toda aquella información descriptiva sobre el contexto, calidad, condición, o características de un recurso u objeto de información que tiene la finalidad de facilitar su recuperación, autentificación, evaluación, preservación y/o interoperabilidad", por

cual para el caso que se utilizara, serán los documentos ofimáticos, puesto que los metadatos de estos archivos pueden almacenar información sobren quien creó estos documentos, quien los modificó, quien fue el último en modificarlo, el tiempo que tomó realizar el documento, dispositivo, sistema operativo o software con el que fue realizado, etc, datos que nos permiten tener un conocimiento de las personas y el ambiente en el que desarrolla el documento. (Pública)

2.6 Objetivo General:

Diagnosticar la vulnerabilidad de la información en documentación pública de entidades del sector público de la ciudad de Cuenca.

2.7 Objetivos Específicos:

- Analizar la problemática de la vulnerabilidad de la información en documentación pública de entidades del sector público de la ciudad de Cuenca.
- Estudiar las buenas prácticas de seguridad de la información.
- Aplicar un diagnóstico de la vulnerabilidad de la información en documentación pública de entidades del sector público de la ciudad de Cuenca.
- Analizar la legalidad ecuatoriana en cuanto a la obtención de información de documentos públicos.

2.8 Metodología

La metodología de desarrollo de la tesis es investigativa en los primeros pasos del desarrollo de la misma, se generará una indagación previa del tema de manera general en el ámbito de la seguridad informática, posteriormente una investigación profunda del tema de los metadatos de los documentos ofimáticos. Finalmente, se hará correlación entre seguridad informática y la seguridad en metadatos para conceptualizar los primeros capítulos de la tesis.

Posteriormente, con la investigación generada anteriormente, se tomará una muestra de 5 empresas de la ciudad para generar las pruebas con los conceptos obtenidos de seguridad en metadatos. Se pondrá en práctica el análisis y se genera un reporte final después del análisis.

Edición autorizada de 10.000 ejemplares
Del 778.501 al 788.500
N° 0785959

Una vez obtenida toda la información privilegiada de las empresas, se procede a aplicar los conceptos de seguridad que se han obtenido para generar un manual de buenas prácticas con respecto a los metadatos.

Para finalizar con la tesis, se propone un capítulo sobre la legalidad de realizar estas prácticas dentro de la legislación ecuatoriana. Este capítulo será realizado junto con el acompañamiento de un abogado con maestría en seguridad informática, por lo que tendrá un buen asesoramiento.

2.9 Alcances y resultados esperados

Al finalizar este proyecto se espera generar un documento que tanto teórico como práctico muestre a la comunidad el real alcance de no tomar en cuenta los metadatos en las empresas, un procedimiento para detectarlo y medidas para la mitigación del problema. Además de un aporte en el ámbito legal que puede repercutir en las leyes ecuatorianas de llegar a tener la repercusión mediática necesaria pues con estas técnicas se puede obtener mucha información privilegiada de las empresas.

UNIVERSIDAD DEL AZUAY

2.10 Supuestos y riesgos

Riesgos	Probabilidad	Alternativas de solución
Falta de cumplimiento de las tareas en los tiempos asignados.	media	Destinar mayor cantidad de tiempo al proyecto
El director de tesis demore demasiado tiempo en revisar los avances propuestos	baja	Cronograma de revisiones con fecha de clases para facilitar el tiempo del profesor
Retraso de tiempo en las reuniones con el abogado externo en las reuniones	media	Generar un cronograma de reuniones para facilitar el tiempo del abogado externo
El tema práctico de la tesis tome más tiempo del esperado	baja	Destinar más tiempo del programado a la parte práctica

2.11 Cronograma

Objetivos	Actividades	Duración (Semanas) 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17
Analizar la problemática de la vulnerabilidad de la información en documentación pública de entidades del sector público de la ciudad de Cuenca	Generar una indagación previa y marco teorico sobre los problemas que presentan los metadatos en documentos públicos	
Estudiar las buenas prácticas de seguridad de la información	Revisión de documentos, libros y estandares sobre seguridad informatica.	
	Elaborar un conjunto de buenas prácticas sobre el tratamiento	
Aplicar un diagnóstico de la vulnerabilidad de la información en documentación pública de entidades del sector público de la ciudad de Cuenca	Buscar información privilegiada en documentos públicos mediante el análisis de metadatos de los mismos	
Analizar la legalidad ecuatoriana en cuanto a la obtención de información de documentos públicos	Conjuntamente con un abogado master en seguridad informática, analizar la legalidad ecuatoriana en cuanto al tema de metatados en documentos públicos	
	Generar un capítulo de tesis con este tema	

Edición autorizada de 10.000 ejemplares
Del 778.501 al 788.500
Nº 0785961

UNIVERSIDAD DEL AZUAY

2.12 Bibliografía

Alonso, C. (2013). *Pentesting con Foca.* 0xWorld.

Alotaibi, M., Furnell, S., & Clarke, N. (2016). Information Security Policies: A Review of Challenges and Influencing Factors. *11th International Conference for Internet Technology and Secured Transactions (ICITST)*, 352-358.

Alotaibi, M., Furnell, S., & Clarke, N. (s.f.). *IEEE Explorer.* Obtenido de IEEE Explorer.

Budi Setiawan, A., Syamsudin, A., & Sasongko Sastrosubroto, A. (s.f.). *IEEE Explorer.* Obtenido de IEEE Explorer.

Chatvichienchai, S. (2011). Automatic Metadata Extraction and Classification of Spreadsheet Documents Based on Layout Similarity. *Dept. of Information and Media Studies, University of Nagasaki*, 38-43.

Choudhruy, S. R., Mitra, P., Kirk, A., Szep, S., Pellegrino, D., Jones, S., & Giles, C. (2013). Figure Metadata Extraction From Digital Documents. *12th International Conference on Document Analysis and Recognition*, 135-139.

Nessah, D., & Okba, K. (2012). Document Analysis to Provide Semantic Metadata based Ontologies. *International Conference on Multimedia Computing and Systems*, 1-7.

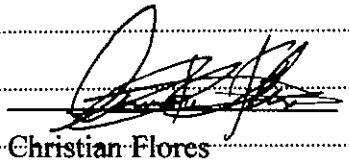
Pomerantz, J. (2015). *Metadata (The MIT Press Essential Knowledge series).* MIT Press.

Portia Buthelezi, M., Van der Poll, J. A., & Oketch Ochola, E. (2016). Ambiguity as a Barrier to Information Security Policy Compliance: A Content Analysis. *International Conference on Computational Science and Computational Intelligence*, 8.

Pública, M. d. (s.f.). *Gobierno de España.*

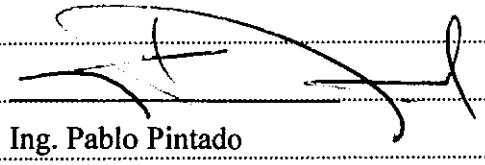
UNIVERSIDAD DEL AZUAY

2.13 Firma de responsabilidad (estudiantes)



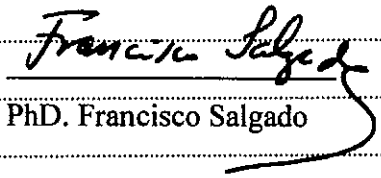
Christian Flores

2.14 Firma de responsabilidad (director sugerido)



Ing. Pablo Pintado

2.15 Firma de responsabilidad (asesor metodológico)



PhD. Francisco Salgado

2.16 Fecha de entrega: 10/05/2017

Edición autorizada de 10.000 ejemplares
Del 778.501 al 788.500
Nº 0785963