RESUMEN

En la actualidad, los sistemas virtuales han tomado un papel indispensable para una institución, organización o empresa. Sin embargo, el tener un adecuado control sobre lo que posee la entidad, conocer sus falencias y estar actualizados con las nuevas amenazas informáticas. Es fundamental, por esta resulta importante poseer un sistema de gestión de seguridad de la información (SGSI).

El presente proyecto de grado es la representación de la investigación realizada cuyo objeto de estudio fue el sistema virtual de la Universidad de Cundinamarca, la cual busca comprender y simplificar el entorno ciberespacial de dicho sistema por medio de distintos métodos y técnicas interdisciplinares que además de identificar los elementos, considera algunos factores de riesgo. Generando así un análisis de riesgos y vulnerabilidades, que lleve a la creación del MAPA TOPOLÓGICO de este sistema.

Es muy importante comprender como está conformado el espacio de interacción diaria de este gremio, por esta razón este proyecto busca que su resultado final (Mapa topológico) sirva para la toma de decisiones estratégicas por parte de los estamentos de la universidad.

De esta manera estimular la cartografía como una herramienta importante para la toma de decisiones y en el proceso de auditoria informática.

PALABRAS CLAVE

Sistema de Gestión de Seguridad de la Información, Entorno ciberespacial, Auditoria Informática.

ABSTRACT

Currently, virtual systems have taken an indispensable role for an institution, organization or company. However, have adequate control over what the entity has, know the anomalies and be updated with the new computer threats. It is a vital objective, for this reason, it is very important to have an information security management system (ISMS).

The present degree project is the representation of the University of Cundinamarca, which seeks to understand and simplify the cyberspace environment of said system by means of several interdisciplinary methods and techniques that in addition to identifying the elements, considers some risk factors. Generating an analysis of risks and vulnerabilities, which leads to the creation of the TOPOLOGICAL MAP of this system.

It is very important to understand how the daily interaction space of this union is made up, for this reason this project seeks that its final result (topological map) be used for strategic decision making by the university.

In this way, stimulate cartography as a very useful tool in decision making and in the process of computer audit.

KEY WORDS

Information security management system, Virtual environment, computer audit.

INTRODUCCIÓN

TEMA GENERAL

Es importante pensar porque nace la cartografía y es que no simplemente es el hecho de entender y simplificar un territorio. Tiene un trasfondo social muy amplio; LA PROPIEDAD PRIVADA es uno de tantos, el hombre tiene esa necesidad de definir lo que cree que es de él. Ese es el papel que ha jugado la cartografía en la historia, lo que realmente les importa a los gobernantes de una zona. Pero no solo para la delimitación de zonas específicas, dado a que su uso se extendió hasta transmutarse en un arma intelectual de apoyo a numerosas guerras, que al final se convertirán en más propiedades y por lo tanto más riquezas; el conocer el espacio donde se han de enfrentar los ejércitos genera una ventaja. Pero el mundo ha cambiado, después de mucha violencia las guerras son distintas, la química y la física pasaron a ser un potencial peligro después de la primera bomba nuclear o cuando los ejércitos nazis experimentaban con la genética, pero sin darse cuenta llego un tercer factor que nos recuerda la guerra fría este factor es la tecnología “la información es poder” (Francis Bacon,1582).

Ojala solo fuera eso una guerra de espionaje, los ataques cibernéticos han llegado a un punto descontrolado, casos como el de STUXNET ”Imagen No. 1” donde una central nuclear de Irán, explotó a causa del ya mencionado malware echando a perder la investigación de meses o robos financieros e intelectuales que destruyen compañías y personas, manipulación de información, malversar fondos bancarios hasta casos tan simples como el uso de botnets para llenar los correos de una población con spam de determinado producto o servicio. Sin olvidarnos de la mayor preocupación de los expertos en seguridad, que los cibercriminales comiencen a trabajar con bandas de crimen organizado, cosa que a la fecha ya sucede a gran escala en “La web oscura”.

¿Si todo eso ocurre en un espacio digital es posible hacer cartografía de dicho espacio para brindarle una ventaja a nuestro ejército en el dado caso que nos veamos enfrentados a un ciber-ataque?

Las empresas reconocen la importancia de la tecnología dado que esta no solo permite el manejo de datos e información, sino que también permite organizar a nuestro equipo con objetivos comunes. El tratamiento de la información abarca aspectos que van desde el manejo de documentos en medio físico como el proceso de almacenaje y recuperación conocido también como proceso de gestión documental, hasta los sistemas de información que tenga la organización o sistemas externos a los que esté obligada a reportar información. Pasando por aspectos tan importantes como la forma de almacenamiento de datos digitales, modelos de respaldo de información y planes de contingencia o continuidad del

negocio, si existen, claro está. Incluyendo además los sistemas físicos de protección y accesibilidad a sitios o áreas restringidas.

No debe caerse en el error de asumir, que estos ataques cibernéticos solo afectan a las empresas grandes o países, por que se quiera o no; la comunidad académica de la Universidad de Cundinamarca (UDEC), se encuentra inmersa en este mundo tecnológico. Dado que cada estudiante, profesor, administrativo y el resto de personal de apoyo, cuenta con acceso a tecnologías como lo son computadores, celulares, entre otros. Que en muchos casos no son solo utilizados en el plantel educativo. Por lo cual se puede definir que cada uno de estos es una potencial amenaza para la institución UDEC. Tampoco se puede creer, como si fuera un axioma, que la seguridad informática es imposible de lograr. Con esfuerzo, dedicación y el apoyo de los directivos se puede alcanzar un nivel de seguridad razonable, que satisfaga las necesidades de una entidad en crecimiento como lo es la UDEC, implementando políticas de seguridad preventiva para anticiparse a posibles sucesos tomando medidas oportunas.

Al trabajar de una forma interdisciplinar con cartografía, se puede aportar información de la estructura virtual, que permitirá al personal especializado de la universidad, tomar decisiones coherentes. Para lo cual, la cartografía tiene la OBLIGACIÓN de adaptarse a los nuevos espacios.

TEMA ESPECÍFICO

Este proyecto de investigación, busca minimizar los posibles riesgos informáticos a los que se encuentra expuesta la Universidad de Cundinamarca. Por tal motivo, se plantea realizar un mapa topológico con los principales vectores de ataque, que pueden afectar los activos de software de esta entidad. Por esta razón, se genera un análisis de riesgos y amenazas sobre el sistema de información de la universidad, lo que requiere conocer los espacios de contenido por analizar.

Apoyados en conocimientos técnicos, se seleccionan las mejores opciones para llevar a cabo el levantamiento de información relevante. Primeramente, las metodologías de una prueba de penetración (Pentesting) y las recomendaciones de la norma técnica colombiana NTC 5254 del año 2004. De las cuales se tomaron los métodos que se encontraban acorde al proyecto y aquellos que se encontraban más cerca de los objetivos planteados. De esta manera, se decidió realizar una serie de fases de reconocimiento y exploración del sistema, por parte de lo que serían las metodologías de pentesting y por la parte de la NTC 5254/2004, se desarrollaron estas prácticas orientadas a poseer una mejor identificación de los riesgos y amenazas, que permita una forma acertada de tomar decisiones y generar planificación estratégica.
La importancia de este proyecto, radica en el rol que se asume para realizar la investigación, dado que fue planteada “como si, se tratara de un usuario externo a

la Universidad de Cundinamarca". Se trabajó sin tener datos oficiales y por medio de distintas herramientas, se logró reconocer los espacios de contenido de la institución educativa e identificar las posibles vulnerabilidades a las que se encuentra sometida la universidad.

Como un segundo factor, se encuentra el trabajo interdisciplinar de Cartografía e Ingeniera de Sistemas. Demostrando la importancia de la Cartografía en otras disciplinas científicas, al lograr representar elementos cualitativos y cuantitativos en una forma gráfica, permitiendo así una fácil comprensión del espacio a trabajar.

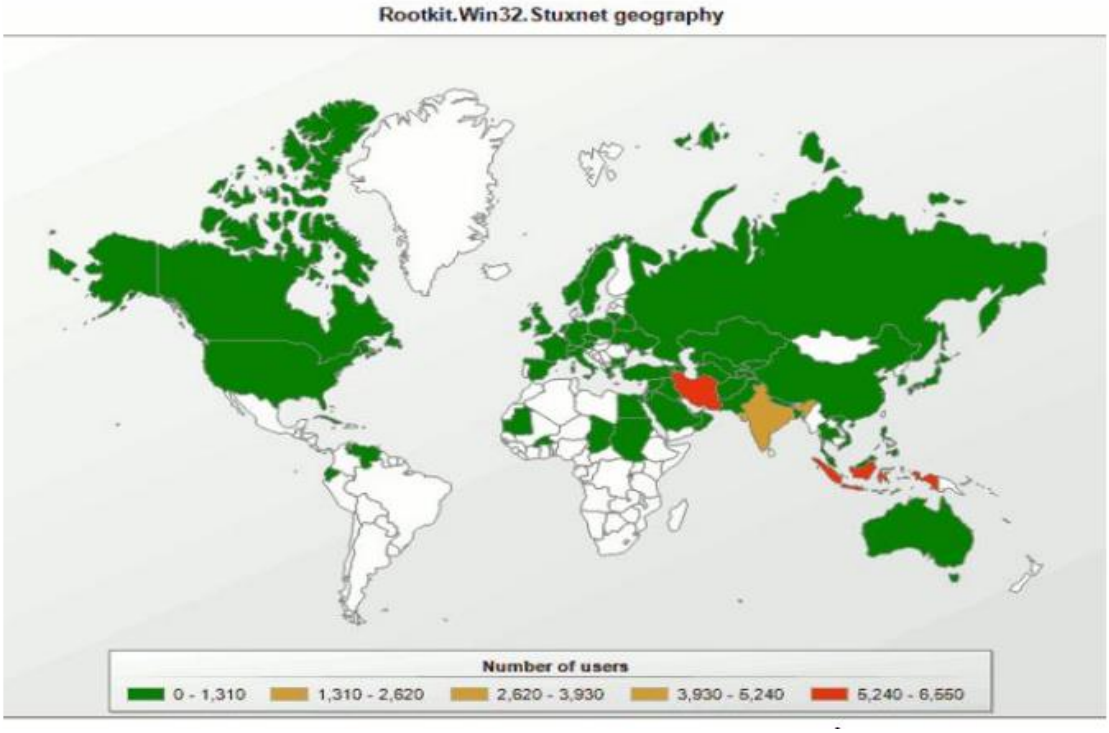


Imagen No. 1: Mapa de usuarios infectados por stuxnet, Iroel Sánchez,16 enero 2011

1. ESTADO DEL ARTE

1.1 ANTECEDENTES

La informática, se ha ganado un lugar en la vida de todas las personas, llegándose a convertir incluso en algunos casos en una necesidad básica, debido a la dependencia que tiene la sociedad actual con esta ciencia. Por eso se hace necesario el debate sobre la seguridad informática. Ya que la mayoría de estos sistemas se diseñaron para ser eficaces y funcionales, pero no seguros. Se debe comprender que, así como estos servicios permiten una gran cantidad de beneficios para todos, también permiten efectuar operaciones ilícitas. Y ese desempeño, en las tecnologías de la información a gran escala, genera que el lado negativo e inseguro de las redes de información, vaya aumentando a un ritmo descontrolado. Por tal razón, las instituciones han comenzado a adoptar la seguridad informática dentro de su organización y no es de extrañar, que una de las principales inquietudes, se encuentre en el campo de los activos que estas mismas posen. Dado que el crecimiento sobretodo del internet, ha hecho que las empresas y organizaciones ofrezcan a la red, una gran cantidad de contenido. Pero esta lucrativa actividad para algunas empresas se ha vuelto en su contra, por no gestionar su seguridad de una manera efectiva.

Día a día, la dependencia a la informática va creciendo. Esto ha generado una serie de modelos, que explican las bases para generar un programa de seguridad. La clave es la protección de los activos más importantes para la organización. "*Estos activos pueden ser identificados mediante los análisis de riesgos, además de la identificación de las vulnerabilidades y amenazas que puedan tener una materialización."* (Gutiérrez David & Zuccardi Giovanni, 2006). Una vez se realizan estos procesos, se puede tener claro el presupuesto de inversión, contemplando objetos materiales, implementación de políticas, educación del personal, desarrollo de guías, estándares, etc.

Es importante invertir en estos aspectos, dado que el buen funcionamiento de la organización y su desarrollo depende de concientizar a cada uno de sus miembros. Y en cuanto a seguridad, una de las mejores herramientas es educar a aquellos, en las políticas y procedimientos. Estas deben considerarse como reglas a cumplir, las cuales surgen para evitar problemas y dan soporte a los mecanismos de seguridad, si se implementan correctamente en los sistemas y redes de comunicación. Buscando cumplir el principal objetivo de la seguridad informática, el cual es evitar que personas externas a la organización, logren tener acceso a los recursos.

Para ello, es fundamental preparar una serie de medidas protectoras de los equipos informáticos, contra un acceso o escucha no permitido. Debido a que las empresas y organizaciones hoy en día, manejan su recurso más importante por medio de SOFTWARE; es necesario que todas estas implanten, una evaluación de riesgos para la información, con el propósito de proteger la integridad de ésta y cumplir con los controles de políticas de seguridad.

Es de vital importancia, entender la diferencia entre seguridad informática y seguridad de la información. Así que, recordando el nacimiento de esta rama de la informática, existía una gran expectativa de una metodología para la protección de la información, en medio de este afán aparece la seguridad informática. La cual se define como: "*Un conjunto de métodos que utilizan herramientas que permiten proteger la información ante cualquier amenaza" (Yánez Ericka,2015).* Aunque es común encontrarla como un *"Conjunto de medidas de prevención, detección y corrección orientadas a proteger la confidencialidad, integridad y disponibilidad de los recursos informáticos." (Iglesias Javier,2016).*

Mientras la seguridad de la información, consiste en preservar sus tres principios básicos confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento. Tal como se menciona es "*La protección de los sistemas de información y de información contra el acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados a fin de proporcionar confidencialidad, integridad y disponibilidad." (*Deluque Coko,2008). Hay que tener cuidado, no solo centrarse en lo anteriormente mencionado, ya que la seguridad de la información, no es simplemente una cuestión técnica, sino una responsabilidad de alta gerencia.

Las personas que gestionan los datos sensibles, estrategias de negocio y otro tipo de información, en su mayoría son personas anónimas. Dejando a los demás empleados y clientes alejados de sistema de seguridad. Ahí es cuando, un caso de espionaje industrial causaría un daño fatal, dado que uno de los mayores vectores de ataque es la misma red. Fundamentalmente porque la gente se siente "protegida" por estas personas anónimas, por lo tanto, tienden a bajar la guardia en la red interna, desconociendo lo que pasa y dando por sentado sus propias especulaciones de la seguridad. Además de sentirse cómodos, lo cual hace que muchos realicen diversas acciones en la red interna, las cuales no se harían en un cibercafé. Desconocen lo que sucede, pero confían en que los administradores, hacen todo lo posible para dotarlos de un sistema seguro,

asumiendo que, en su propia red empresarial, no hay “enemigos” o delincuentes informáticos.

Cuando se genera una política para la seguridad en la red, es de suma importancia hacer comprender al equipo, la razón de crear esa política. Es decir, que los esfuerzos dedicados a la seguridad, produzcan los beneficios esperados. Tanto en costos como en eficacia. Para ello se debe conocer cuáles son los recursos que vale la pena proteger, cuales son más importantes que otros y en cuales se encuentran o pueden encontrar posibles amenazas. A pesar de toda la publicidad generada por los medios, acerca de los intrusos que irrumpen en una red, la mayoría de estudios demuestran que, en las organizaciones, las pérdidas causadas por los usuarios internos son mayores.

Los análisis de riesgos, sirven para identificar las amenazas y vulnerabilidades, sobre la plataforma tecnológica de la organización objeto de estudio. De esta manera, se podrá generar un plan de implementación de los controles y políticas que prodiguen un ambiente seguro y controlado; basado en los criterios de disponibilidad, confidencialidad e integridad.

Para efectuar un análisis de riesgos se debe decidir si éste, será tratado bajo una metodología cualitativa y/o cuantitativa. Aunque en el análisis de riesgo cualitativo, no se puede llevar a un estado de perfección, dado que es bastante complejo cuantificar elementos cualitativos. Es de gran importancia, realizarlo para poseer otra perspectiva de los riesgos que pueden afectar la información, que se maneja en la organización. Para esto, los riesgos deben clasificarse por su nivel de importancia en la entidad y la gravedad que implicaría su perdida. De esta manera, no terminar en una situación en la cual, se gaste más protegiendo algún recurso que tenga un menor valor para la organización.

Es decir, el análisis de riesgos es guiado por los principales procesos, activos y prioridades del negocio. Alineado con la estrategia corporativa y guiando a su vez, a los otros dominios de análisis de riesgos. En el nivel corporativo alto, los cambios son menos frecuentes y más lentos, mientras en los niveles inferiores se debe tener mayor detalle en políticas específicas, procedimientos técnicos y operativos.

Siendo simultáneamente, necesaria de manera anticipada, la comprensión del termino topología y cómo esta se ve involucrada en la cartografía. Aproximadamente en los años ochenta, existió una gran expansión del uso de los SIG (Sistemas de Información Geográfica), permitiendo se expandieran de forma acelerada un gran número de herramientas especializadas en el dibujo y diseño asistido por computador. Además de la

generalización del uso de ordenadores portátiles, estaciones de trabajo y la consolidación de las bases de datos relacionales, junto a las primeras modelizaciones de las relaciones espaciales o topología. La aparición de la orientación a objetos en los SIG, permite una nueva concepción de los sistemas de información geográfica, dado que se integra todo el contenido conocido de una entidad (simbología, geometría, topología y atributos)

En informática, la topología es una vista interactiva de la red, donde cada host se encuentra ubicado en circunferencias concéntricas, que indican el número de saltos desde el nodo de inicio hasta el nodo central.

Una de sus definiciones más claras es: La topología geoespacial estudia las relaciones espaciales entre los diferentes elementos gráficos (topología de nodo/punto, topología de red/arco/línea, topología de polígono) que representan las características geográficas y su posición en el mapa (*cerca de*, *entre*, *adyacente a*, etc.). Estas relaciones, que para el ser humano pueden ser obvias a simple vista, el programa informático las debe establecer mediante un lenguaje y unas reglas de geometría matemática. Es la capacidad de crear topología, lo que diferencia a un Sistema de Información Geográfica (SIG) de otros sistemas de gestión de la información.

Se sabe que un objeto posee al menos dos componentes, uno gráfico y otro no gráfico. A un objeto grafico se le atribuye por medio del software un numero clave de identificación, de la misma manera el componente alfanumérico se define con el mismo identificador. De tal forma que el software establece una relación entre estos dos componentes. Además de esta relación se encuentra la relación topológica que dice sencillamente la relación del elemento con otros elementos de su entorno geográfico próximo.

1.2 PLANTEAMIENTO DEL PROBLEMA

¿Cómo puede la Cartografía apoyar el campo de la seguridad informática de la Universidad de Cundinamarca?

En un estudio de previo, de la situación actual en la Universidad de Cundinamarca, se dio a conocer que no tienen estandarizados los suficientes controles y políticas que lleven a minimizar los posibles delitos informáticos, a los que están expuestos los datos, comprometiendo la integridad, confidencialidad y disponibilidad de la información. Además de poseer falencias en la normatividad vigente del país.

Por esta razón y apoyándose, en que actualmente la seguridad informática es un punto clave de análisis, dado que las condiciones van cambiando a lo largo del tiempo y se día a día surgen nuevas amenazas informáticas. Gestionar los riesgos de una manera eficiente, evitara ser víctimas de delitos informáticos, que obstaculicen el normal funcionamiento de la institución educativa, como lo pueden ser intrusiones, modificación y/o robo de información, denegación de servicios, malware en su amplia categoría, entre otros.

La cartografía por otra parte, tiene la obligación de adaptarse al ciberespacio y las nuevas tecnologías de interacción humana, que nacen día a día. Y donde se pueden observar los problemas sociales, de reunir a una gran parte de la población mundial en un solo lugar. Donde el comportamiento individual, depende de la ética de cada actor. Así como, un día lo hizo con la cámara fotográfica o la carrera espacial. Hoy es necesario mostrar la importancia de esta ciencia en este campo, porque de lo contrario serán profesionales de otras áreas los que terminen supliendo la necesidad de comprensión del ciberpunk.

1.3 OBJETIVOS

1.3.1 OBJETIVO GENERAL

- Concebir, diseñar y estructurar el mapa topológico del espacio virtual, a partir del análisis de riesgos de los activos de software de la Universidad de Cundinamarca.

1.3.2 OBJETIVOS ESPECÍFICOS

• Identificar y clasificar los principales activos de software, en la Universidad De Cundinamarca.

• Analizar los espacios de contenido de información que puedan verse comprometidos en un ataque informático.

• Representar la información adquirida de los activos de software de la Universidad de Cundinamarca en un mapa topológico.

1.4 JUSTIFICACIÓN

Cuando se comete algún delito informático, existe una rama de la informática que se dedica a entender, como esto es posible y quien lo hizo posible, esta rama se conoce como informática forense. Y una de sus mejores herramientas es la creación de mapas, con información que se va recopilando del atacante. Este proyecto plantea apoyar a la universidad, con una política novedosa de seguridad informática. Brindándole un mapa topológico, de la información que puede llegar a ser utilizada por un atacante en su estructura intangible, para que esta pueda intentar anticiparse y tomar las medidas preventivas oportunas.

El no estar preparados para un ciber-ataque, puede exponer a la institución a las situaciones como: la modificación del malware o virus Petya, en el mes de junio de 2017, donde se han visto afectadas numerosas empresas, bancos y compañías, de Europa, Asia y Estados Unidos, además de un importante puerto indio y varias empresas chinas.

A otros casos como; la modificación de notas por parte de los estudiantes. Donde la Universidad de Cundinamarca, como muchas otras ya fue testigo una vez, los peligros de no cumplir con las leyes de protección de datos o incluso ataques de denegación de servicio (DOS) como los realizados por el colectivo de Anonymous al Ministerio de Defensa de Colombia, la Policía Nacional entre otros organismos gubernamentales del mismo país y del mundo.

La institución debe asumir metodologías actuales. Entendiendo, que no son ajenos a estas situaciones. Para ello, es necesario empezar con la ejecución del análisis de riesgos y amenazas del sistema información de la Universidad de Cundinamarca, y la creación de un modelo gráfico de este sistema, es un primer paso para aplicar POLÍTICAS INNOVADORAS de seguridad informática.

1.5 MARCO REFERENCIAL

1.5.1 MARCO TEÓRICO

Más que una serie de elementos en un espacio, existen una gran cantidad de “fenómenos” que están presentes, apoyando la subsistencia de estos elementos, algunos otros creados por una interacción mutua o con su espacio. He incluso existen externos, a este espacio que los pueden mejorar o destruir. Así nace la ciencia, como la manera de explicar los diferentes “fenómenos”, que se encuentran presentes en un sistema y la relación que tienen entre sí y con los demás elementos del sistema. Cuando un científico logra describir esto, se dice que ha creado una teoría. Pero como se ha descrito anteriormente, dicha teoría aplica dentro de los límites de este sistema. Dado que, al enfrentarse a un sistema diferente, que contiene elementos diferentes, el “fenómeno” se comportara de una manera distinta. Esto incluye también las modificaciones sustanciales al mismo sistema. Por ejemplo, en los tiempos que la teoría de la tierra plana predominaba, el fenómeno de estudio era: ¿Cómo es el lugar dónde estamos?, los elementos eran una serie de individuos y geografía presente. Pero en el momento, en que se modifica drásticamente el sistema con nuevas herramientas que permiten mejorar su análisis, es necesario generar nuevas teorías.

El entorno espacial, es fundamental para comprender cualquier dificultad y así mismo generar las posibles soluciones. Pero también, se deben tener en cuenta los elementos presentes en dicho entorno y las herramientas que existen para estudiarlos. Haciendo énfasis en las herramientas, el ser humano crea una muy especial que es la misma ciencia, pero lastimosamente esta magnífica herramienta, se ha ido deteriorando a través de los años, hasta un punto donde se fragmentó en una gran cantidad de disciplinas, con el fin de apoyar intereses económicos de ciertos individuos, además de muchas otras maneras en las que contaminaron esta herramienta. Es así como nos encontramos hoy, en una sociedad donde el conocimiento es un negocio y no algo universal, pero aun así es necesario volver a sus orígenes, reuniendo los fragmentos de conocimientos como lo son cartografía, matemáticas, ingeniería de sistemas, ingeniería en informática, inglés, etc. Para poder generar teorías aplicables y útiles para la misma sociedad.

Muchos sistemas son un conjunto de subsistemas que trabajan en una forma coordinada y precisa, estos subsistemas pueden ser tomados como elementos o como bien se dice un subsistema, con sus propias reglas. La cartografía, brinda tal apoyo que ha llegado a generar mapas que permiten

conocer nuestro cuerpo, los circuitos electrónicos de una máquina, que permiten la navegación marítima y la aérea. Así como mapas de subsistemas como el mapa genético de nuestra especie y muchos más.

1.5.1.1 *Cartografía y su función en el Ciberespacio.*

Pero la cartografía no deja de ser una ciencia, que debe seguir un método científico, con unos pasos definidos previamente tales como tener claro el objeto o sistema a trabajar, recolectar los datos relevantes de este, organizar los datos, analizar la información recolectada, generar modelos y con base en estos llegar a una serie de conclusiones o teorías.

Además, de que la tecnología ha transformado nuestras vidas, desde el principio de los tiempos y la seguirá transformando día a día. Alterando el sistema conocido, este cambio también afecta el sistema académico. Las profesiones se van actualizando, esa es una de las principales funciones de la cartografía. Ya que la grandeza del concepto, fue minimizada al tener carencia de un término que realmente describiera su actividad, dado a que es mucho más que de lo que señala su propia etimología: (Charta= Papel y Grafia = Escritura).

El poder adaptarse a nuevos espacios para lograr interpretar sus dinámicas de una forma apropiada y útil. Es una de las maneras en la que los profesionales de esta ciencia, muestran su verdadera función con la sociedad y académicos. Ya que, en vista de la necesidad de un mapa, los profesionales de otras disciplinas, han sido obligados realizar este oficio en la actualidad.

Hoy en día se puede notar el aumento de los productos cartográficos y de los sistemas de información geográfica (SIG), en aplicaciones móviles y servicios web. En otras palabras, el internet y el mundo le abrió las puertas a la cartografía y esta, proporciono todo el conocimiento que poseía, ahora le toca complementar ese conocimiento con el nuevo espacio. Brindando sus saberes y formulando teorías, para la interpretación del ciberespacio y sus fenómenos.

1.5.1.2 *Ciberespacio.*

Un nuevo dominio entre los dominios existentes (terrestre, marítimo, aéreo, espacial) es la definición, de uno de los principales marcos de referencia de las fuerzas armadas, el dominio global. *El Ciberespacio es un entorno*

*virtual sin límites geográficos, en él se desarrollan actividades vitales para la sociedad, pero este fue diseñado principalmente para que funcionase de manera rápida y eficaz pero no para ser seguro. (*Tcol. Baselga M*)*

Este ciberespacio es tan grande como lo es la mente, puesto que día a día se producen cantidades exorbitantes de datos, servicios, conocimiento, productos, etc. Y aunque, se suele confundir el internet con el ciberespacio este tiene un significado mucho más amplio. Algo de recalcar, es que el ciberespacio se ve como un mundo paralelo al nuestro, pero todo esto está cambiando con el internet de las cosas, apuntándole a que estos dos mundos estén interconectados. Por lo cada vez es más importante que los cartógrafos puedan apoyar a las instituciones que buscan, el bien común en este entorno. Protegiendo, cosas de mucho valor, que se encuentran en un sitio inseguro. Ya que, las actividades criminales, que se desarrollan en el mundo real, tienen su réplica en el ciberespacio.

1.5.1.3 *Topología.*

La mejor herramienta que ofrecen las matemáticas, para poder comprender el ciberespacio es la topología. Esta ciencia estudia los objetos, viéndolos estos de una forma variante. Permitiendo que estos sufran deformaciones, para llegar a otros objetos con propiedades similares, estas deformaciones deben cumplir dos reglas bastante estrictas, al menos en la topología clásica los objetos no se pueden cortar, ni romper.

Esta rama de la matemática, era conocida anteriormente como geometría de caucho, donde la idea predominante es la continuidad. La topología nace en 1736 gracias a *Leonard Euler,* al solucionar el problema de los siete puentes. Analizando las conexiones y las distintas partes de la ciudad, Euler advirtió que las distancias eran irrelevantes. De cierta manera es una geometría no métrica. Esta trabaja con vértices y aristas, para generar un esquema que permita estudiar las propiedades del sistema. Y al contrario de la geometría euclidiana, que se ve afectada por las cantidades, en esta no importa, que tan lejos estén los puntos o si las líneas son largas o cortas.

Aunque el primero en utilizar el término topología fue *Johan Benedict L.* quien, en 1847, publica un artículo como estudiante proponiendo que era mejor utilizar el término *topología* a *geometría citus* que se venía utilizando. Johan Benedict, estudio las propiedades de la cinta o banda de Moebius, la cual se encuentra, en lo que matemáticamente se conoce como una **SUPERFICIE NO ORIENTADA**, dado que no existe ni arriba, ni abajo, ni

adelante, ni atrás. Porque todo se encuentra en un mismo plano. Esta versión de la geometría no tenía sentido en el siglo XVIII, debido a que, estudiaba las propiedades de unas figuras variables, fijándose en las cualidades. Se decía que venía de la geometría de posición utilizada por Euler.

Solo hasta el siglo XX, se comprendió que tras las propiedades de los objetos se reúnen las ideas y surgen unos nuevos conceptos. Los cuales son denominados topológicos, estos conceptos se adentran en un nuevo espacio.

La topología estudiara los diferentes tipos de espacios, ejemplos de esto es. La teoría de grafos: que permite generar el trayecto óptimo para el reparto de mercancías. La teoría de nudos: que hace corresponder el anudamiento del ADN, con una cuerda con nudos. La teoría de las superficies: que trata de clasificar todas las superficies compactas, etc.

1.5.1.4 Mapeado Topológico o Bump Mapping.

Se ha logrado definir, el sistema a trabajar y las propiedades teóricas que la cartografía, puede utilizar para llegar a representarlo. En cuanto a las herramientas, una bastante utilizada es el mapeado topológico. Que consiste en trabajar, con un conjunto de entidades (punto, línea o polígono) que comparten una o más geometrías coincidentes entre sí. Incluso el software ArcGIS, ha implementado la herramienta BUMP MAP MODEL. Que permite generar mapas topológicos como el sistema hidráulico, eléctrico o vial de una ciudad. En internet se encuentran bastantes formas de utilizarlo, como en el artículo publicado por (Gómez, Fernández Emilio:2012, Alter geosistemas) donde explica, la metodología usada por Jeffery Nighbert en el 2003 para implementarlo en un SIG.

En el ámbito de la computación, representan gráficamente el arreglo físico o lógico de sistema de información. Y generalmente, es bastante útil para comprender los nodos, rutas de envió de paquetes e incluso problemas en red.

1.5.1.5 Seguridad De La Información.

Entre los elementos del ciberespacio a tener en cuenta, es la seguridad. Un fenómeno, que amenaza la eficacia de los procesos realizados, en la interacción diaria. El conocer, con que cuenta una organización, es decir sus activos. Es el primer paso para poder aplicar seguridad, por tal razón la cartografía de estos activos, se vuelve el primer paso, para poder ser seguros y tener claridad del sistema, en caso de circunstancias imprevistas que lo puedan perjudicar.

La seguridad en las organizaciones, ya no se limita a la protección de dinero, bienes o personas. La realidad actual exige, que las organizaciones protejan un recurso esencial, **la información**. Ya que las entidades dependen de la información y de la tecnología que la soporta, pero hay que tener claridad *"La información adopta diversas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en video o hablada"* (Rodríguez M, 2015)

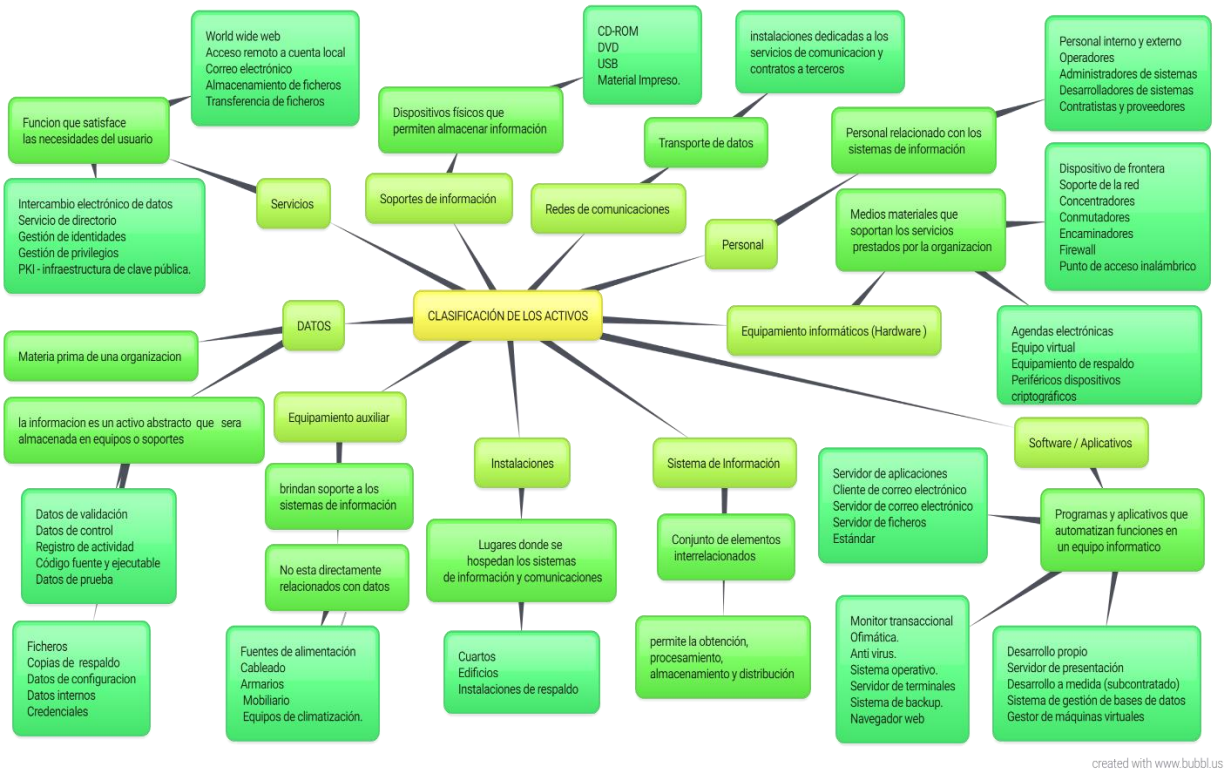
1.5.1.6 CLASIFICACIÓN DE LOS ACTIVOS

Los elementos, que componen el sistema de una organización, se conocen como activos. A continuación, se muestra una taba y un mapa conceptual, explicando cada uno de estos elementos detalladamente, aunque para efectos de este proyecto se trabajaran los activos de software.

TIPO	DESCRIPCIÓN
[D] Datos / Información	Los datos son el combustible con el que opera una organización. La información es un activo abstracto que será almacenado en equipos o soportes de información y que puede ser transferido de un lugar a otro por los medios de transmisión de datos. Pertenecen a este grupo: ficheros, copias de respaldo, datos de configuración , datos de gestión interna, credenciales, datos de validación de credenciales, datos de control de acceso, registro de actividad, código fuente, código ejecutable y datos de prueba
[S] Servicios	Función que satisface una necesidad de

	los usuarios, como: world wide web, acceso remoto a cuenta local , correo electrónico , almacenamiento de ficheros, transferencia de ficheros, intercambio electrónico de datos, servicio de directorio, gestión de identidades , gestión de privilegios , PKI - infraestructura de clave pública.
[SW] Software / Aplicativos	Programas, aplicativos, desarrollos, que han sido automatizadas para su desempeño por un equipo informático, entre ellos están: desarrollo propio , desarrollo a medida (subcontratado), estándar, navegador web, servidor de presentación, servidor de aplicaciones, cliente de correo electrónico, servidor de correo electrónico, servidor de ficheros , sistema de gestión de bases de datos, monitor transaccional, ofimática, anti virus, sistema operativo, gestor de máquinas virtuales, servidor de terminales, sistema de backup.
[HW] Equipamiento informáticos (Hardware)	Medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, entre ellos podemos identificar: agendas electrónicas , equipo virtual, equipamiento de respaldo, periféricos dispositivos criptográficos, dispositivo de frontera, soporte de la red, concentradores, conmutadores, encaminadores, firewall, punto de acceso inalámbrico, etc.
[COM] Redes de comunicaciones	Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros. Medios de comunicación que tiene por objetivo transportar datos de un sitio a otro.
[Media] Soportes de información	Dispositivos físicos que permiten almacenar información de forma permanente o por largos periodos de tiempo. Ejemplo: CD-ROM, DVD, USB, Material Impreso.
[AUX] Equipamiento auxiliar	Equipos que sirven de soporte a los sistemas de información, sin estar

	directamente relacionados con datos; como: fuentes de alimentación, cableado, armarios, mobiliario, equipos de climatización.
[L] Instalaciones	Lugares donde se hospedan los sistemas de información y comunicaciones. Ejemplo: cuartos, edificios, instalaciones de respaldo.
[P] Personal	Personal relacionado con los sistemas de información; como: personal interno y externo, operadores, administradores de sistemas, desarrolladores de sistemas, contratistas y proveedores.
[SI] Sistema de Información	Conjunto de elementos interrelacionados que permiten la obtención, procesamiento, almacenamiento y distribución de la información para apoyar la toma de decisiones y el control en una organización.



Mapa conceptual No. 1, clasificación de activos de software, Daniel Rodriguez;2018

1.1.1.1 GLOSARIO

INSTITUCIÓN:

Un sistema conjunto, conocido como organización o asociación, que trabaja con el fin desempeñar una función cultural, política, científica o social. Puede desarrollar sus funciones en el ámbito privado o público.

ORGANIZACIÓN:

Complemento de estructuras administrativas y sistemas administrativos, que comparten objetivos y metas, apoyados por un talento humano y otro tipo de recursos. Compuesta, por un conjunto de subsistemas interrelacionados que cumplen funciones especializadas.

ACTIVIDAD:

Una meta, compuesta por una o más tareas, para las cuales es necesario alguien las realice.

CIBERESPACIO:

Según la OTAN, 2016: el ciberespacio es un dominio global formado por los sistemas de TIC y otros sistemas electrónicos. Los cuales procesan información, la almacenan y la transmiten. En una institución, se comprende cómo los flujos de la comunicación existente, en una plataforma de TIC además de agregar la interacción del ser humano con estos elementos.

CIBERDELINCUENTES:

Persona o personas que realizan acciones delictivas, premeditadamente con el fin de robar información profesional y personal, malversar fondos, dañar los equipos informáticos entre muchas otras acciones delictivas por medio de las TIC. En el caso Rodríguez, ciberdelincuencia 2015; Convenio de Budapest dice que es toda acción antijurídica, típica y culpable. Que se realiza el objetivo de destruir y dañar computadoras y redes por vías informáticas. Además de mencionar la importancia, de tener una legislación actualizada, dado que muchos de los eventos, que suceden en este ámbito, no son consideradas delitos.

ACTIVOS:

Son todos los recursos, con los que cuenta una organización. Para que esta se mantenga en el mercado. Estos recursos, son tanto físicos como intangibles, comprendiendo también las metodologías, para realizar la labor en la que se especialice.

HARDWARE:

Conjunto de elementos físicos, que constituyen una computadora o un sistema informático, permitiendo el almacenamiento, procesamiento y transmisión de datos.

SOFTWARE:

Son las instrucciones para que el hardware funcione correctamente. Estos conjuntos de programas y funciones, permiten que se realicen determinadas tareas específicas con el hardware.

SISTEMAS DE INFORMACIÓN:

Conjunto de elementos, que interactúan entre sí. Procesando, almacenando, analizando y transmitiendo información para cumplir un objetivo específico. Los sistemas de información pueden automatizar procesos, además de apoyar la toma decisiones.

HOST:

Un host o anfitrión, es un ordenador que funciona, como el punto de inicio y final de las transferencias de datos. Recibiendo a los clientes, generar las peticiones de los mismos y cumplir estas peticiones permitiéndole consultar o descargar.

DOMINIO:

En internet, es un nombre único que se asocia a un sitio web, este y el sistema de nombres de dominio (DNS), permiten identificar rápidamente los activos, de determinada red. Además, sin ayuda de este, para acceder a un sitio web, tocaría por medio de la dirección IP, lo cual dificultaría las búsquedas.

ANCHO DE BANDA:

Es la capacidad, de una onda electromagnética medida en Hz, que posee un medio para propagar información.

CERTIFICADO DIGITAL:

Documento electrónico, vinculado a la llave de encriptación de un individuo o entidad pública. Este contiene, atributos del portador de la llave, según las especificaciones de la autoridad certificadora.

FILTRADO DE CONTENIDO:

Se refiere, al bloqueo de información indeseable de internet. Generalmente, las empresas por medio de un software, pueden bloquear el contenido, que se permite mostrar. Con base en el tipo de tráfico.

FIREWALL:

Sistema o combinación de sistemas, que refuerzan los límites entre dos o más redes. Un firewall, regula el acceso entre las redes de acuerdo a una política de seguridad específica.

COOKIE:

Un mensaje, suministrado a un navegador web, por un servidor web. Que puede contener información específica sobre el usuario final. El navegador, almacena el mensaje en un archivo de texto y lo envía de nuevo al servidor, cada vez que el navegador solicita una página del servidor. La información almacenada, contiene los hábitos de navegación del usuario, sus preferencias o información demográfica. Esta tecnología, se utiliza para identificar a los usuarios y personalizar las páginas web. Las cookies, también pueden utilizarse para rastrear actividad del usuario dentro de un sitio Web.

CORREO INSTITUCIONAL:

Es un servicio, que permite a usuarios específicos enviar y recibir mensajes, por medio de una red de comunicación electrónica. Además, de permitir el acceso a otros servicios de la comunidad.

SISTEMAS OPERATIVOS:

Es un software, donde operan otros software's. Haciendo que, este sea el software principal, para la operación de un aparato tecnológico. Para esto, es necesario que posea un conjunto de programas y órdenes que permitan controlar los procesos básicos y el funcionamiento.

WINDOWS:

Es el sistema operativo, más utilizado a nivel hogar, este sistema operativo, es solo para computadoras con excepción de unos pocos teléfonos móviles. Es una plataforma, que trabaja de la mano de otras entidades reguladoras de contenido de los usuarios. Y su código fuente fue liberado recientemente, aunque aún su licencia es paga.

LINUX:

Es el sistema operativo más utilizado a nivel empresarial, este sistema operativo desde sus inicios, permito que los usuarios de Unix experimentaran con el código fuente. Esto género, que existan una gran variedad de distribuciones Linux y que este sea aplicado a otros aparatos electrónicos. Los sistemas Linux pueden ser multiplataforma, multiusuario y multitarea. Una particularidad, es que Linux respeta más la privacidad del usuario, al almacenar menos registros de este.

AUDITORIA:

Inspección o verificación a una entidad o empresa, donde se verifica que esta esté cumpliendo, con los requerimientos a los que está obligada.

LEVANTAMIENTO DE INFORMACIÓN:

El levantamiento de información, se ha transformado con el transcurso de los años, en la actualidad se pueden recopilar datos de manera masiva e información sobre las opiniones, conductas, actitudes o estado y características de un elemento (animado o inanimado) especifico.

RECONOCIMIENTO:

Es una de las fases del levantamiento de información, donde se intenta recopilar, la mayor cantidad de datos del objetivo. Esta se divide a su vez en dos ramas, el reconocimiento activo y el reconocimiento pasivo.

EXPLORACIÓN:

La segunda fase del levantamiento de información, en la que se comprenden, las dinámicas que poseen y los elementos. Que permiten que el sistema se mantenga en pie, además de garantizar la eficacia del mismo sistema.

RIESGOS Y AMENAZAS:

Son dos conceptos, que están relacionados entre sí. Dado que ambos tienen sus bases en matemáticas, el riesgo se define como la probabilidad, de que ocurra evento o fenómeno negativo y la amenaza es intensidad y frecuencia que puede tener este evento o fenómeno.

PRUEBAS DE PENETRACION:

Se realizan distintos tipos de tareas, para lograr identificar una infraestructura objetivo, las vulnerabilidades que pueden explotarse y los daños podría causar un atacante.

VULNERABILIDAD:

Es una debilidad, que es propensa a causar un daño. Y está estrechamente relacionada, con el nivel de amenazas que puede recibir un sistema.

MALWARE:

Cualquier programa, que tiene como objetivo alterar el funcionamiento normal de un programa, computadora o un sistema, sin el conocimiento o autorización del usuario.

CONTROL:

Los procedimientos, practicas o elementos. Que se emplean, para minimizar o eliminar un riesgo. Es toda acción, orientada a minimizar la frecuencia de ocurrencia de las causas del riesgo o valor de las pérdidas ocasionadas por ellas. Los controles, sirven para asegurar la consecución de los objetivos de la organización o asegurar el éxito de un sistema y para reducir la exposición de los riesgos, a niveles razonables. Los objetivos básicos de los controles son: Prevenir las causas del riesgo, detectar la ocurrencia del riesgo y retroalimentar el sistema de control interno con medios correctivos.

CONTROL DE ACCESO:

Es un control, que provee los medios para administrar el comportamiento, uso y contenido de un sistema. Permite al administrador, especificar que usuarios pueden acceder al sistema, que recursos pueden usar o ver, y que acciones pueden realizar.

GESTIÓN DEL RIESGO:

Cultura, procesos y estructuras. Que van dirigidas, a obtener oportunidades potenciales, mientras se administran los efectos adversos.

PROCESOS DE GESTIÓN DEL RIESGO:

Aplicación sistemática de políticas, procedimientos y prácticas de gestión a las labores de comunicar, establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y revisar el riesgo.

ISO 27000:

Estándares de seguridad, con los que debe cumplir una organización, trabajando desde conceptos teóricos, mejores prácticas, guías, etc.

1.5.2 MARCO LEGAL

Acto Jurídico	Numero	Fecha	Nombre	Descripción
LEY	594	2000	Ley General de Archivos y se dictan otras disposiciones	Establece las reglas y principios generales que regulan la función archivística del Estado.
NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA	27000	2016	NTC ISO/IEC 27000	Requisitos del sistema de gestión de seguridad de la información
NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA	27001	2006	UNE/ISO 27001	Define los requisitos para la implementación de un SGSI (Sistema de Gestión de la Seguridad de la Información)
NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA	27001	2013	ISO/IEC 27002	Es una guía de buenas prácticas, describe los controles a seguir dentro del marco de la seguridad de la información
NORMA TÉCNICA DE CALIDAD EN LA GESTIÓN PÚBLICA	1000	2009	NTCGP 1000:2009	Calidad en la gestión pública.

NORMA TÉCNICA COLOMBIANA	9001	2015	NTC-ISO 900, Sistemas De Gestión De La Calidad.	Norma que se centra en todos los elementos de la gestión de la calidad con los que una empresa debe contar para tener un sistema efectivo que le permita administrar y mejorar la calidad de sus productos o servicios
Ley	1273	2009	Modificación el Código Penal	Se crea un nuevo bien jurídico "la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones
Norma técnica colombiana	5254	2004	Gestión del Riesgo	Busca contribuir eficientemente en la identificación, análisis, tratamiento, comunicación y monitoreo de los riesgos del negocio.

1.6 METODOLOGÍA

1.6.1 TIPO DE ESTUDIO

La investigación realizada, fue descriptiva y correlacional, sin llevar a cabo ningún tipo de desarrollo o implementación.

1.6.2 POBLACIÓN, UNIVERSO Y MUESTRA:

La población universitaria, es la directa beneficiada con este proyecto entendiendo esta como sus estudiantes, docentes, estamentos, contratistas, etc. Además del público en general, que desee comenzar a ser parte, de la comunidad académica de la UdeC.

Este proyecto de grado, se desarrolla en el amplio universo del ciberespacio, tomando como muestra específica, el lugar asignado a la

universidad de Cundinamarca. Planteado de otra manera, se desarrolla el análisis de la red interna de la institución educativa, la cual se trata de una red, contenida en la gran red de redes (internet).

1.6.3 MÉTODOS:

Se realiza una investigación descriptiva y correlacional, donde se maneja un enfoque mixto. Debido a que, el primer resultado *el inventario de los activos de información* y segundo resultado que es *la clasificación de los activos de información* son entregas cuantitativas. El tercer y cuarto resultado, *la matriz de valoración de riesgos* basándose en los conceptos del *consejo nacional de rectores* y *la elaboración del mapa topológico de los activos de software de la Universidad de Cundinamarca,* son productos cualitativos y cuantitativos.

Los métodos utilizados en este proyecto, son una mezcla entre la norma NTC 5254 del 2004, que propone una manera eficaz de gestionar el riesgo en un negocio u organización, seguido de métodos de Ethical hacking y Pentesting que nos proveen la materia prima (los datos). Para desarrollar, las propuestas de una gestión de riesgos eficientemente.

1.6.4 TÉCNICAS:

Siguiendo las especificaciones, de la NTC 5254 del 2004. Para una gestión del riesgo eficaz, es necesario aplicar una serie de técnicas de comunicación y consulta. Buscando una mejora, en la identificación de oportunidades y amenazas, tener una base rigurosa para la toma de decisiones y planificación, generando una gestión proactiva, que permita mejorar la conformidad con la legislación pertinente, además de mejorar la gestión de incidentes, la reducción de pérdidas y el costo del riesgo.

En el caso concreto, se aplicarán técnicas de escaneo y recolección de datos, técnicas de escaneo y penetración de vulnerabilidades y una última de documentación de las dos anteriores, siguiendo los estándares de una auditoria informática. Por medio, de instrumentos tecnológicos, como los son ordenadores, sistemas operativos en los que encontramos algunas distribuciones de Linux (Wifislax, Kali Linux y Parrot Security) y el tradicional Windows, la gran red de redes (Internet) y por supuesto el sistema de información de la organización.

1.6.5 DISEÑO METODOLÓGICO:

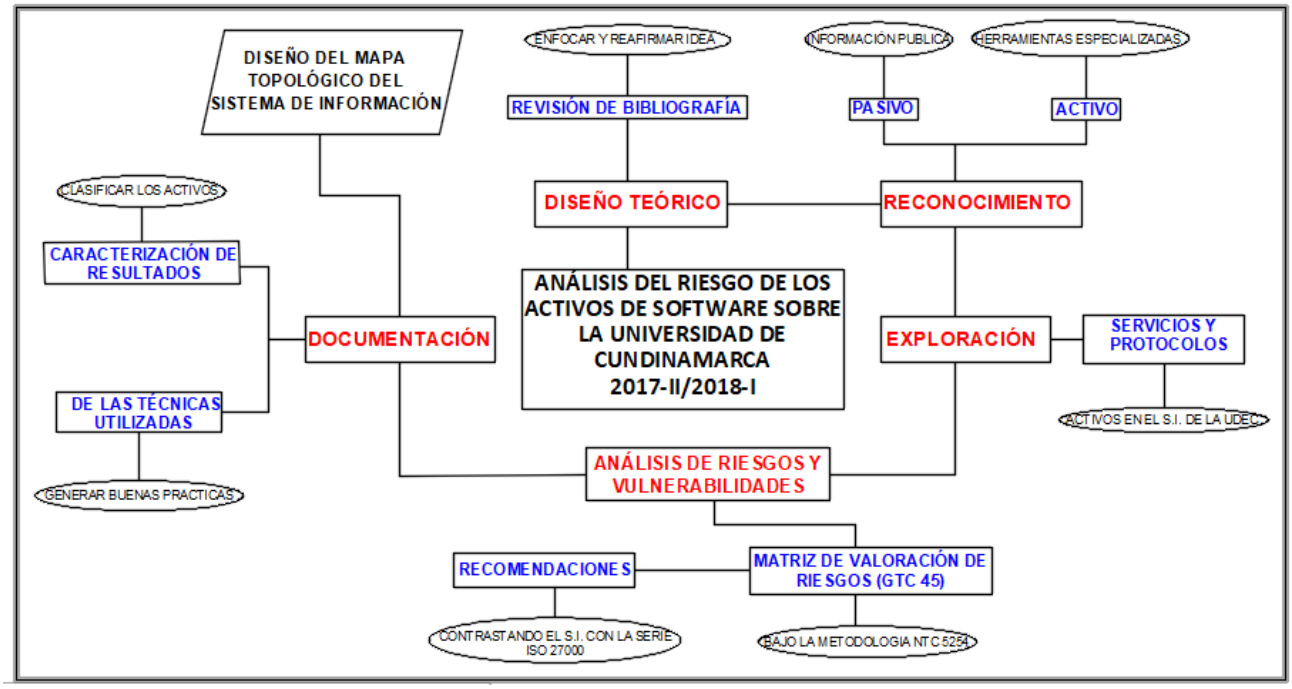


Imagen No. 2. Metodología aplicada al desarrollo del mapa topológico del sistema de virtual de la Universidad de Cundinamarca, Daniel Rodríguez, 2018.

Para generar, el mapa topológico del sistema virtual de la Universidad de Cundinamarca, se debe realizar una serie de procesos sistemáticos, iniciando con un estado del arte, que muestre con claridad los conceptos claves y estudios preliminares, que constituirán la revisión bibliográfica y por lo mismo los pilares de esta investigación. Es importante, ser cuidadosos a la hora de seleccionar, la información que es útil para este proyecto. Una vez se posee claridad, en la idea se pasa a la segunda fase el reconocimiento, enfocado de dos maneras: Pasivo: Comprendido como la información pública, que la institución no puede ocultar y Activo: El cual, conlleva el uso de herramientas especializadas, para la obtención de la información. Posteriormente, se inicia la fase de exploración, donde se analizan los servicios y protocolos, que la institución educativa tiene activos, en su sistema de información. Una vez se obtienen estos datos, se realiza el análisis de riesgos, el cual tiene por objetivo identificar cuáles son los principales vectores de ataque, una vez concluidas estas tareas, que son las que proveen los insumos básicos para la generación del mapa topológico, se abren las puertas a la última parte y una de las más importantes, la documentación de los procesos realizados, que son los productos finales de esta investigación.

Hay que plantear, la continuidad a los procesos realizados, para ello se generan las propuestas de mejora y estándares de gestión de riesgo. Como los que pone a disposición la NTC 5254.

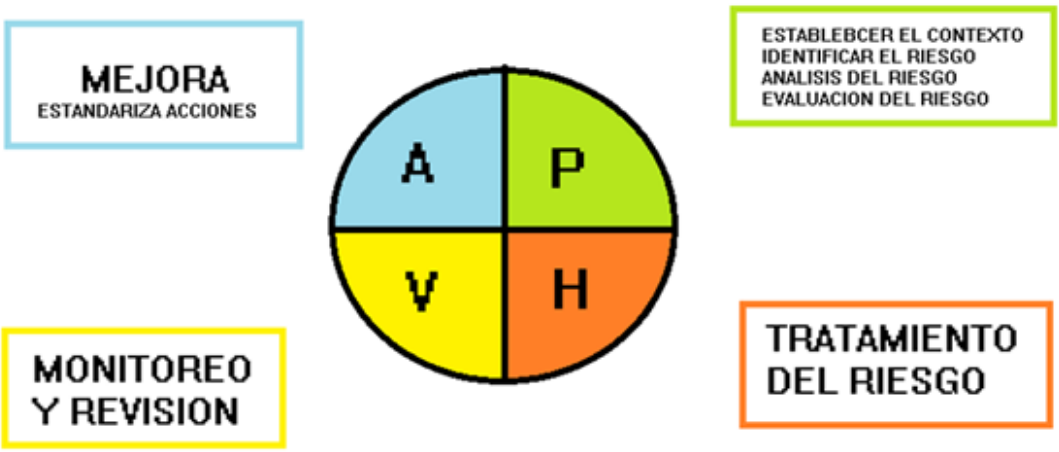


Imagen No.3: Metodología planteada para el desarrollo general del especifico, NTC 5254(2004).

Esto requiere seguir cinco fases fundamentales.

1. Tener conciencia y cultura del riesgo.
2. poseer un pensamiento visionario
3. tomar responsabilidad en la toma de decisiones.
4. Crear una comunicación eficiente
5. Generar una relación costo-beneficio.

Gestionar el riesgo cuidadosamente, no solo genera una planificación estratégica, sino que también se evitaran circunstancias inesperadas. Debido a que se está previniendo que ocurra algo no deseable, como resultado un conocimiento más amplio y una integración de la exposición a riesgos claves, permitirá reducir costos, además de generar una transparencia en la toma de decisiones y procesos de gestión en curso.

2. DESARROLLO DE LA INVESTIGACIÓN

2.1 CONCEPTOS TEÓRICOS

2.1.1 ACRÓNIMOS

ABI Application binary interface

A.P. Amenaza Persistente

ASCII código de caracteres

COMSEC Communications Security

DB Data Base (Base de datos)

DOS Denial of Service (Denegación de servicio)

EFI Extensible Firmware Interface

S.I. Sistema de información

S.G.S.I Sistema de gestión de seguridad de la información

SSL Secure Sockets Layer

IP Internet Protocol (Protocolo de internet)

IPS Intrusion prevention systems (Sistema de prevención de intrusos)

FHS Filesystem Hierarchy Standard

MSF Metasploit Framework

OS Sistema Operativo

GNU General Public License

GRUB Grand Unified Bootloader

URL Uniform Resource Locator

TLS Transport Layer Security

VPN Virtual Private Networks

2.1.2 CONCEPTOS FUNDAMENTALES DE LA INVESTIGACIÓN

En esta investigación, busca generar el diseño del mapa topológico, enfocado al análisis de riesgos y vulnerabilidades realizado a los activos de software, para generar así un MAPA TOPOLÓGICO DE LA INSTITUCIÓN CON LOS PRINCIPALES VECTORES DE ATAQUE que se puedan extraer.

Por esta razón y por la importancia que este proyecto tiene para la población beneficiada, se hace énfasis en la revisión de literatura (La cual es puesta a disposición en el capítulo 1, concretamente en los antecedentes) en dos temas importantes la *seguridad informática* y la *seguridad de la información*.

Así, una vez es mencionada, la importancia de estos temas en el estudio, se debe plantear la pregunta: ¿La seguridad informática **es igual, mas importante** o **menos importante** que la seguridad de la información?

La verdad, es que cuando se habla de sistema de gestión de seguridad de la información (SGSI) concretamente la ISO 27001 del 2013, dispone las buenas prácticas en entornos corporativos, enfocados en su mayoría al área de seguridad, pero se deja por debajo la seguridad informática. Acá es donde se debe pensar, si los procesos de la seguridad de la información van a garantizar que la institución (UdeC) se encuentre en un entorno seguro. Entonces se estaría priorizando, la usabilidad por la seguridad. Por lo tanto, es pertinente recomendar que los modelos y políticas no se queden en una talanquera teórica y burocrática, si no que al contrario se apliquen esos documentos.

Ciertamente la ISO 27001, no se equivoca totalmente en la forma de abordar el tema, dado que la seguridad informática realmente es menos importante que la seguridad de la información, por que al momento de dejar de lado los procesos y no documentar las técnicas de seguridad que se están aplicando, se puede llegar a fallas en los sistemas, dado a que no se conoce que se está aplicando. Por esta razón, las buenas prácticas en entornos corporativos, deben ir ligadas a unas buenas prácticas de ejecución.

Para esta investigación, se tratan herramientas y procesos de seguridad informática, documentando las practicas realizadas en el sistema de información (SI), las que a su vez formaran la auditoria informática. Esta es de vital importancia, dado a que aparte de ser el sustento teórico-práctico del análisis de riesgos y amenazas, es el que provee la materia prima para el diseño del mapa topológico de la institución.

Como se evidencia, en la metodología esta se manejará de una forma pasiva y activa, y continuando con la metodología de pentest se aplica *Gray Box.* En la cual, se trabajará con todos los protocolos de seguridad activos y en la cual la institución educativa no brinda al investigador ningún tipo de información.

Hacking ético Externo: Este acceso, se realiza desde fuera de la red de la compañía, es decir, el ataque está dirigido a los equipos que están expuestos a Internet como: SERVIDORES WEB, CORTAFUEGOS, SERVIDOR DE CORREO, DNS, ENTRE OTROS.

2.2 DOCUMENTACIÓN DE LA PRACTICA

2.2.1 RECONOCIMIENTO

2.2.1.1 RECONOCIMIENTO PASIVO

El reconocimiento pasivo, es comprendido como toda la información, que se pueda obtener de la entidad, de manera pública. Ósea que, esta no se puede ocultar. Así que, se empieza con la descripción general de la institución educativa, la Universidad de Cundinamarca UDEC cuenta un dominio público que es www.ucundinamarca.edu.co

Figura No. 4, Dominio actual de la página principal de la UDEC, 2018-Autor

Anteriormente, se llamaba www.unicundi.edu.co. Aunque, este no ha desaparecido. Dado a que, si lo buscamos, este aún está presente en la web y lo que realiza es una redirección, a el primer enlace aparentemente.

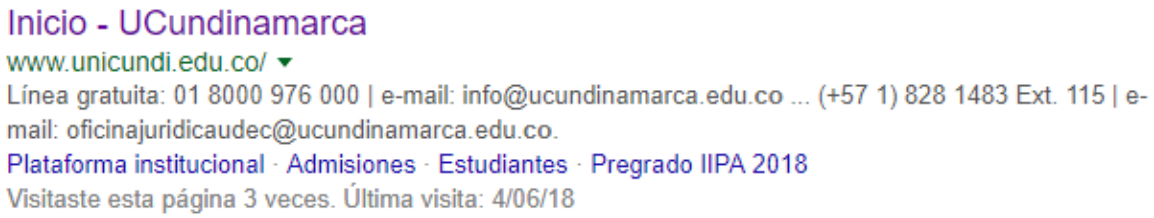


Figura No. 5, Dominio anterior de la página principal de la UDEC;2018-Autor

Este dominio, a su vez cuenta con servicios que enriquecen la comunidad académica. Estos son ofrecidos en su portal principal, como se puede observar en la imagen No. 6.

Figura No. 6, Servicios prestados por la UDEC; 2018-Autor

Aunque algunos de estos, son enlaces dentro del mismo sitio web otros utilizan subdominios, estos últimos son: Aulas virtuales, la plataforma institucional, la biblioteca y las revistas.

Figura No. 7, Link del servicio de aula virtual UDEC; 2018-Autor

Figura No. 8, Link del servicio de plataforma institucional UDEC; 2018-Autor

Figura No. 9, Link del servicio de biblioteca UDEC; 2018-Autor

Figura No. 10, Link del servicio de investigaciones UDEC; 2018-Autor

Figura No. 11, Link del servicio de revistas virtuales UDEC; 2018-Autor

Sin olvidarnos de la intranet, donde reposan algunas actas y resoluciones de la institución.

Figura No. 12, Link de la intranet UDEC; 2018-Autor

Una vez, se tiene una identificación básica del sitio web a analizar. Se procede a saber la dirección IP que este posee, para lo que se trabaja el comando ping, pasándole como argumento el DNS del portal universitario.

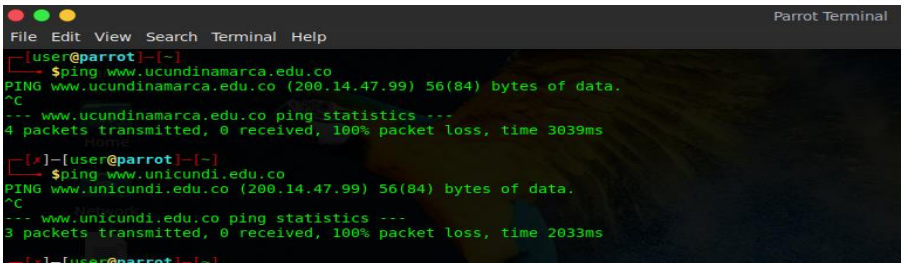


Figura No. 13, Uso de comando ping; 2018-Autor

Al conocer, cuál es la dirección IP del servicio principal de la UDEC hay un segundo paso que es importante y es saber cuáles datos se proporcionaron a la hora de obtener este dominio, para esto se utilizara la herramienta de Whois. En ambos dominios.

Nombre del Dominio	ucundinamarca.edu.co
ID del dominio del registro	D78801390-CO
Fecha actualizada	2017-02-09T22:53:56Z
Fecha de creación	2016-03-30T19:08:32Z
Fecha de caducidad del registro	2021-03-29T23:59:59Z
Registrador	.CO Internet S.A.S.
Registrador IANA ID	111111
URL del Registrador	www.cointernet.com.co
Registrar WHOIS servidor	
Correo electrónico de contacto de abuso de Registrador	soporte@cointernet.com.co
Teléfono de contacto de abuso de Registrador	+57.16169961
Estado del dominio	ok https://icann.org/epp#ok
ID del Registrador del Registro	
Nombre del Registrante	
Organización de Registrantes	UNIVERSIDAD DE CUNDINAMARCA
Calle Registrante	
Calle Registrante	
Calle Registrante	
Ciudad Registrante	
Registrante Estado / Provincia	Cundinamarca
Código Postal del Registrante	
País Registrante	CO
Nombre del servidor	ns1.merca.net.co
Nombre del servidor	ns2.merca.net.co
DNSSEC	unsigned

>> Last update of WHOIS database:2018-06-10T17:27:44Z <<<

Figura No. 14, Whois dominio actual ucundinamarca.edu.co; 2018-Autor

Nombre del Dominio	unicundi.edu.co
ID del dominio del registro	D614419-CO
Fecha actualizada	2015-11-23T15:09:51Z
Fecha de creación	2004-02-10T00:00:00Z
Fecha de caducidad del registro	2020-02-18T23:59:59Z
Registrador	.CO Internet S.A.S.
Registrador IANA ID	111111
URL del Registrador	www.cointernet.com.co
Registrar WHOIS servidor	
Correo electrónico de contacto de abuso de Registrador	soporte@cointernet.com.co
Teléfono de contacto de abuso de Registrador	+57.16169961
Estado del dominio	ok https://icann.org/epp#ok
ID del Registrador del Registro	
Nombre del Registrante	
Organización de Registrantes	Universidad de cundinamarca
Calle Registrante	
Calle Registrante	
Calle Registrante	
Ciudad Registrante	
Registrante Estado / Provincia	Cundinamarca
Código Postal del Registrante	
País Registrante	CO
Nombre del servidor	ns4.merca.net.co
Nombre del servidor	ns2.merca.net.co
DNSSEC	unsigned

>> Last update of WHOIS database:2018-06-10T17:29:36Z <<<

Figura No. 15, Whois dominio antiguo www.unicundi.edu.co; 2018-Autor

Al realizar, el whois aparte de conocer las fechas de creación, actualización y registro, se obtienen nombres de los servidores, donde puede que estén almacenados los ficheros de éstos dominios.

Los datos recolectados fueron:

ID	NOMBRE DEL ACTIVO	DESCRIPCIÓN	IP
01	www.ucundinamarca.edu.co	Dominio	200.14.47.99
02	www.unicundi.edu.co	Dominio	200.14.47.99
03	Virtual.ucundinamarca.edu.co	Sub-Dominio	200.14.47.114
04	Plataforma.ucundinamarca.edu.co	Sub-Dominio	200.14.47.115
05	Biblioteca.ucundinamarca.edu.co	Sub-Dominio	200.14.47.111
06	Revistas_electronicas.unicundi.edu.co	Sub-Dominio	200.14.47.112
07	Investigaciones.unicundi.edu.co	Sub-Dominio	200.14.47.116
08	Intranet.unicundi.edu.co	Sub-Dominio	200.14.47.107
09	Ns1.merca.net.co	Servidor	200.14.41.8
10	Ns2.merca.net.co	Servidor	200.14.41.8
11	Ns3.merca.net.co	Servidor	200.14.41.8
12	Ns4.merca.net.co	Servidor	200.14.41.8

2.2.1.2 RECONOCIMIENTO ACTIVO

Lo primero que se realiza, después del reconocimiento pasivo de la institución es comenzar a recolectar datos técnicos de esta, con el objetivo de identificar y cuantificar los activos del sistema de información de la UDEC, para esto se usan herramientas especializadas de distintos sistemas operativos.

Algo que es de recalcar, desde la parte cartográfica, es que, si un usuario se encuentra fuera de Colombia, no puede ingresar a la página de la universidad. Tal y como se muestra en la figura 13 y 14. En la que por medio de una VPN, se intenta acceder a la página de la institución educativa y esta generara el error de locación.

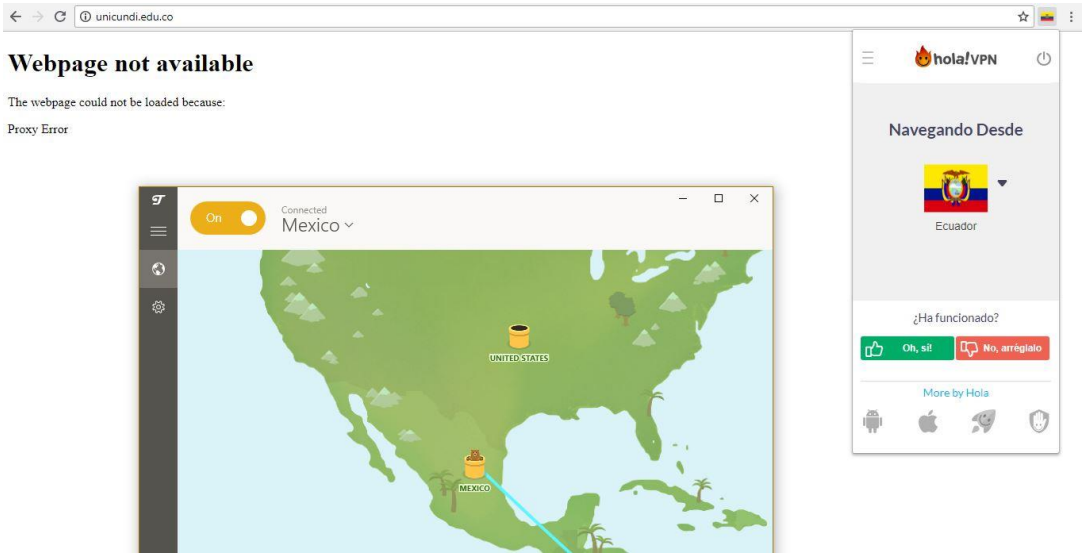


Figura No. 16,Uso de tunnelBear & HolaVPN fallo desde Ecuador; 2018-Autor

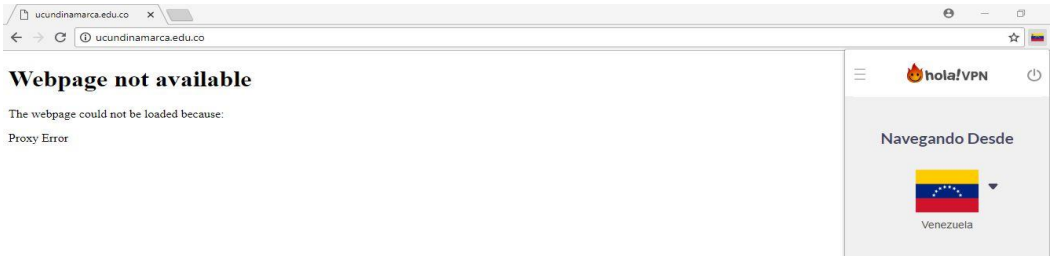


Figura No. 17, Uso de HolaVPN fallo desde Venezuela; 2018-Autor

Conociendo, desde que proxys se puede acceder a este portal web, se utiliza otra herramienta THEHARVESTER, la cual realiza una búsqueda de información, en el caso específico se utilizó el buscador google, pero esta herramienta, también permite generar búsquedas en otros buscadores, como Bing, he incluso hasta en redes sociales como Twitter y registros de usos de aplicaciones, Además de buscar los hosts activos de dicha dirección, tal como se ve en la imagen 18 en el dominio actual y en la 19 del dominio antiguo.

Figura No. 18, Uso de la herramienta theHarvester en www.ucundinamarca.edu.co; 2018-Autor

Figura No. 19, Uso de la herramienta theHarvester en www.unicundi.edu.co; 2018-Autor

Utilizando la herramienta Zenmap, desde Parrot security OS. Se pudo recolectar bastante información relevante. En la imagen No.20. Se evidencia que en la dirección IP, correspondiente a la UdeC (200.14.47.99) y se encuentran 4 (cuatro) puertos activos. Aunque solo logra identificar dos de ellos: El puerto 80 y el puerto 443. Además de, encontrar el servidor donde residen los ficheros de este dominio merca.net.co.

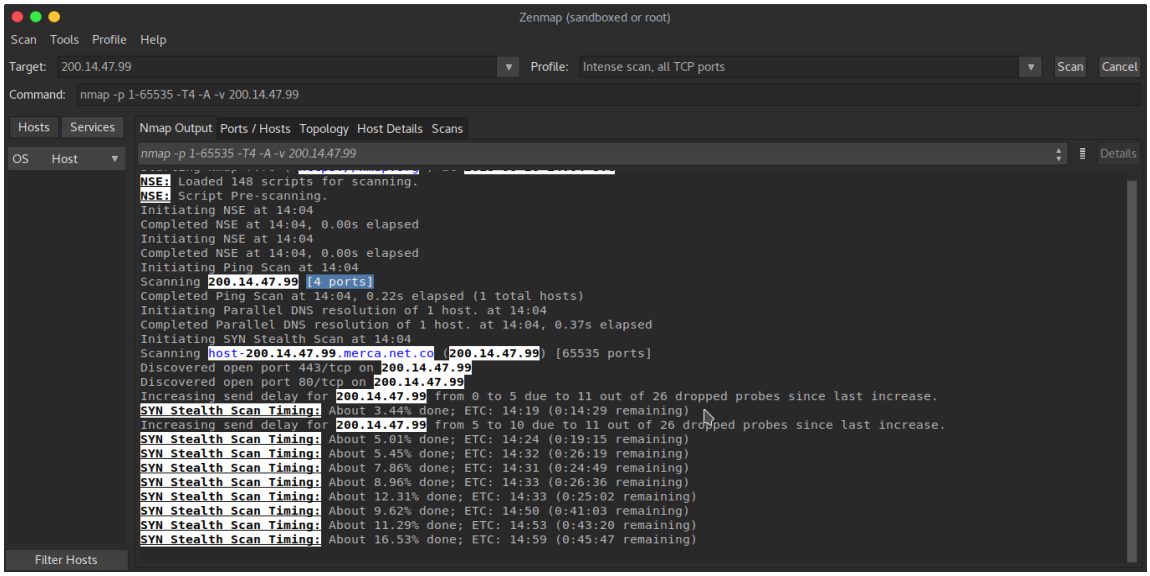


Figura No. 20, Uso de la herramienta Zenmap en www.ucundinamarca.edu.co; 2018-Autor

Continuando, con el escaneo del dominio, se encuentra un tercer puerto activo, que como se puede observar en la imagen número 21. El puerto 15000 se encuentra activo y se encuentra que este DNS tiene 7 hosts en servicio.

Figura No. 21, Uso de la herramienta Zenmap en www.ucundinamarca.edu.co; 2018-Autor

Además, de datos como el país de ubicación, que es Colombia. El servidor de este portal web MERCANET LTDA. CO y aunque existe un password, se pueden extraer datos, como que, en el firewalk, el protocolo TCP bloquea los puertos 9,20 y el UDP bloquea el 2-3,7,9,13,17,19-22. Por último, se vuelve a dar información de los puertos, que este dominio tiene activos, sin embargo, se nota que el puerto 15000 tiene un 10% de pérdidas en los datos enviados. Tal como se evidencia en la imagen No. 22.

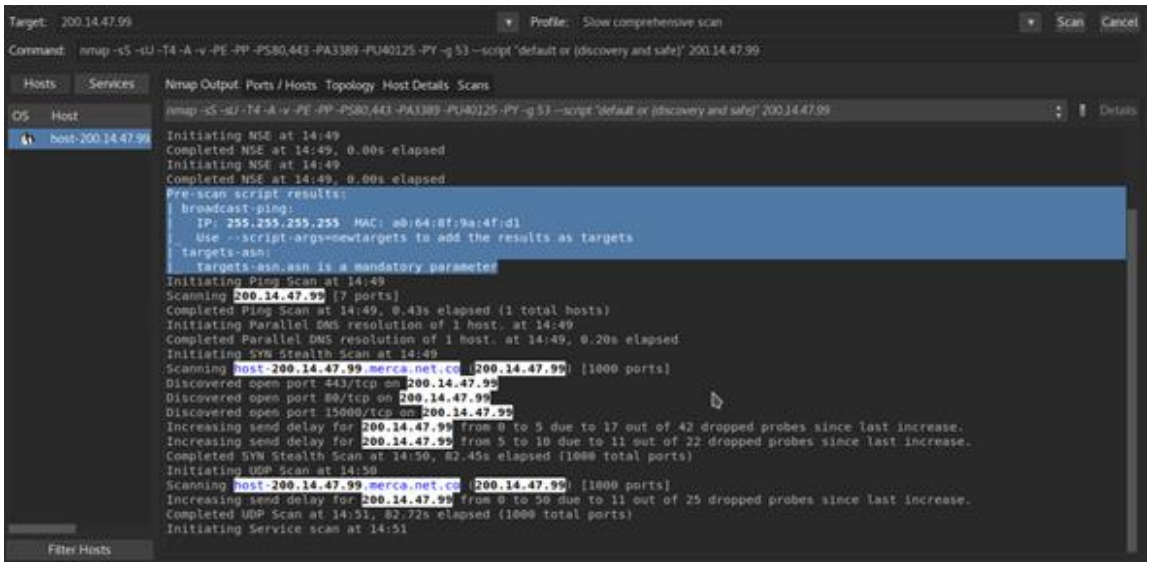


Figura No. 22, Uso de la herramienta Zenmap en www.ucundinamarca.edu.co; 2018-Autor

Una de las cosas más interesantes, que plantea la herramienta Zenmap es que en el escáner logra identificar la máscara de red, que posee la entidad y una dirección física MAC de uno de sus servidores de almacenamiento, como se observa en la imagen No. 23

Figura No. 23, Uso de la herramienta Zenmap en www.ucundinamarca.edu.co; 2018-Autor

En la figura No. 24 se puede ver como la herramienta, indica que el portal universitario NO posee vulnerabilidades de XSS y muestra información importante del sistema operativo utilizado por él administrador, el cual aparentemente es una distribución Linux.

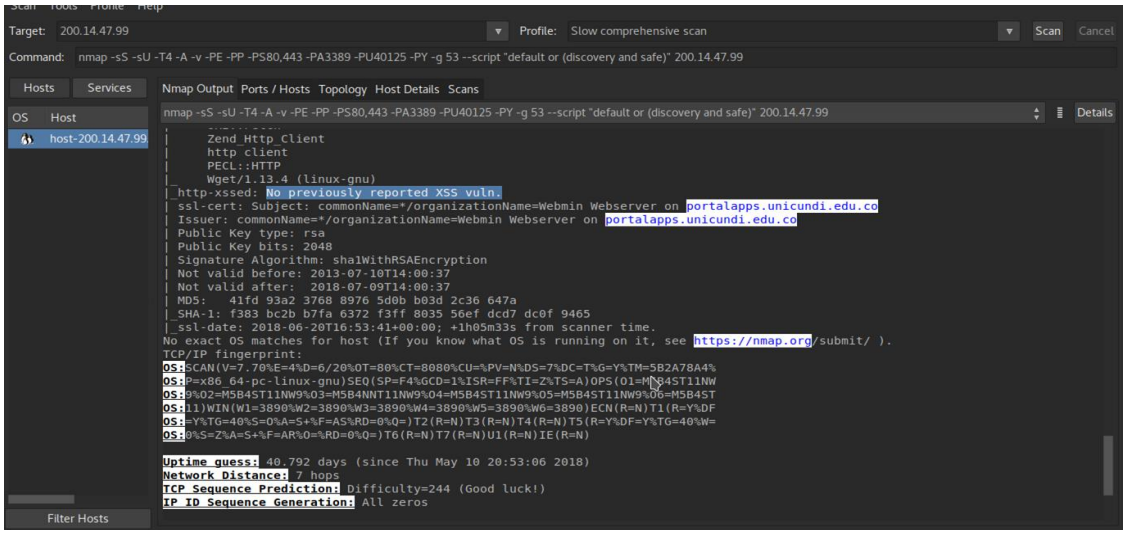


Figura No. 24, Uso de la herramienta Zenmap en www.ucundinamarca.edu.co; 2018-Autor

La herramienta, genera un escaneo por el puerto 80 y el 8080 el cual da como resultado la geolocalización de los servidores principales de MERCANET. Brindando además la dirección IP de cada uno de ellos. Provee datos además del responsable de este servidor los cuales son: Nombre del responsable, correo electrónico del responsable. Figura No.25.

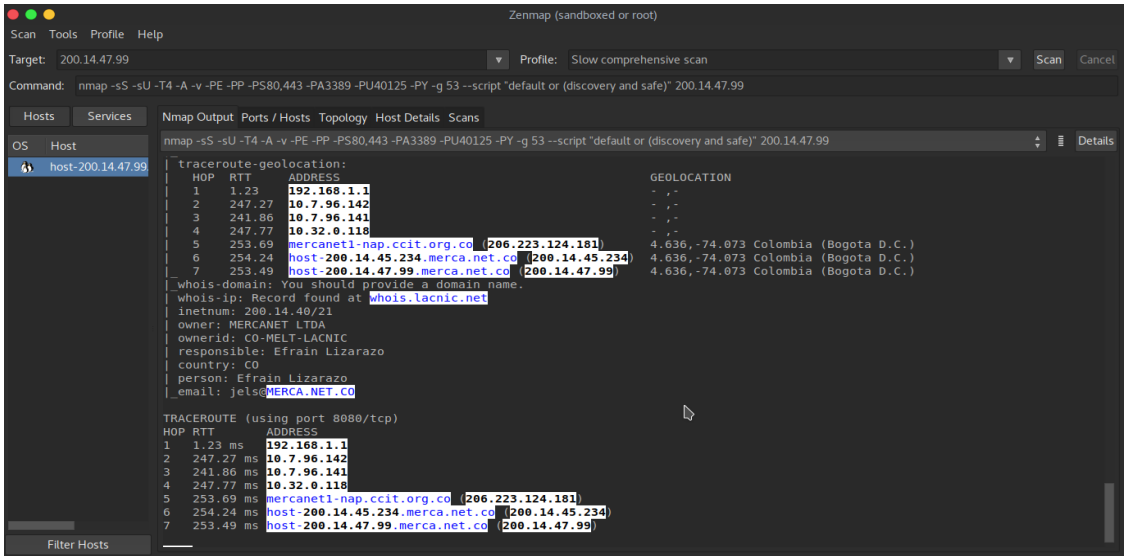


Figura No. 25, Uso de la herramienta Zenmap en www.ucundinamarca.edu.co; 2018-Autor

Una vez se termina el escaneo, se procede a observar los resultados obtenidos, tal como se evidencia en la imagen No. 25. La institución educativa UDEC se encuentra con: el puerto 80 activo el cual maneja un protocolo de TCP, en un servidor Apache manejado por Linux, que además utiliza programación en PERL y PHP. De una manera similar opera el puerto 443, en el momento de hacer el escaneo el puerto 8080 se encontraba cerrado y por último el puerto 15000 que se encuentra abierto y transfiere información a una entidad externa. Como se observa en la figura No.26.

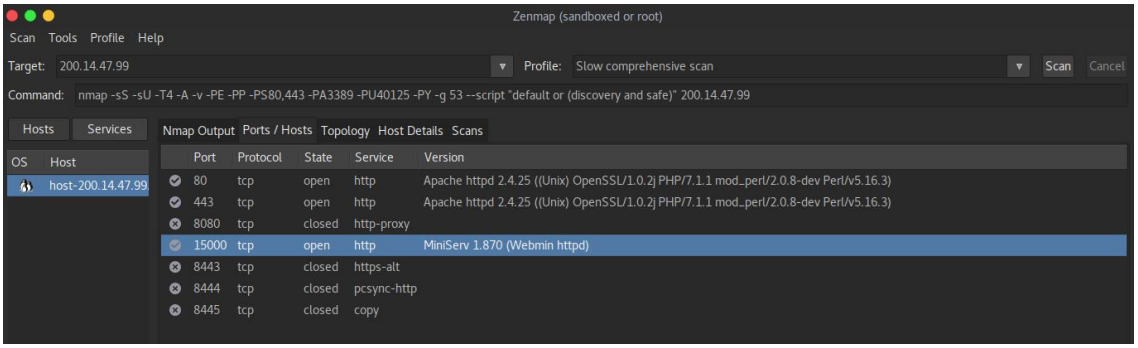


Figura No. 26, Uso de la herramienta Zenmap en www.ucundinamarca.edu.co; 2018-Autor

En los detalles del host, se encuentra que este cuenta con 3 puertos abiertos y 4 cerrados, la dirección IP del servidor MERCA.NET.CO y el sistema operativo utilizado por el administrador o administradores del sistema.

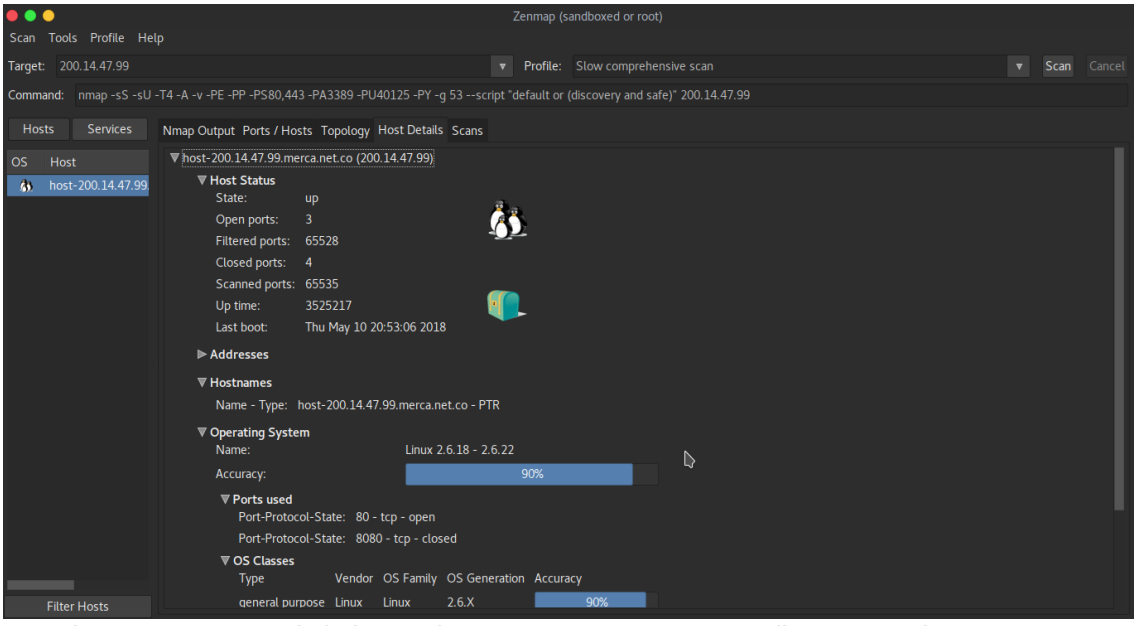


Figura No. 27, Uso de la herramienta Zenmap en www.ucundinamarca.edu.co; 2018-Autor

Esta herramienta provee además un servicio de topología, que una vez termina los distintos tipos de escaneos que posee el software, grafica automáticamente la información recolectada en Zenmap. Figura No. 28

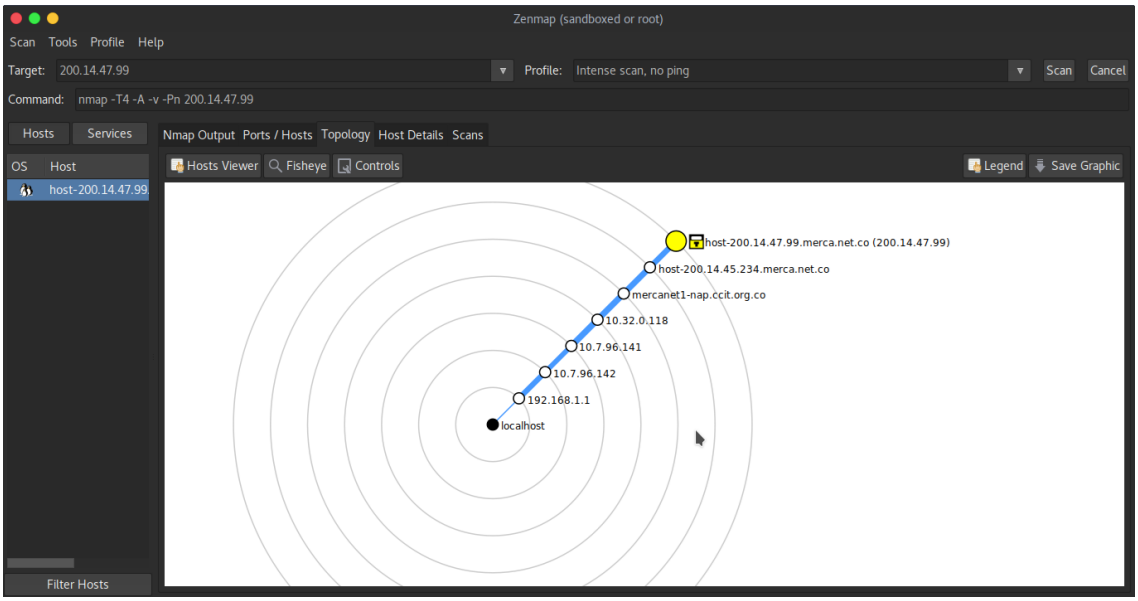


Figura No. 28, Uso de la herramienta Zenmap en www.ucundinamarca.edu.co; 2018-Autor

La siguiente herramienta utilizada, fue DMITRY la cual se aplicó a los dos dominios existentes en la institución educativa, tal como muestra la documentación oficial de Kali Linux es: "*Una de las herramientas que se pueden utilizar en la fase de obtención de información, ya que **Dmitry** se puede utilizar para el escaneo de puertos, dominios o direcciones IP, etc*."

En la figura No. 29, 30 y 31. Se trabaja con el dominio www.ucundinamarca.edu.co, donde se identifica la dirección IP, que corresponde al DNS de la UDEC. Además de una nomenclatura urbana, del lugar en el que se encuentran los servidores de MERCA.NET, el cual se ubica en la Cra. 69 #25-8, Bogotá en la oficina 809. Y datos significativos del dominio, que ya eran conocidos gracias a herramientas anteriores como lo son las fechas de creación y actualización, localización, etc.

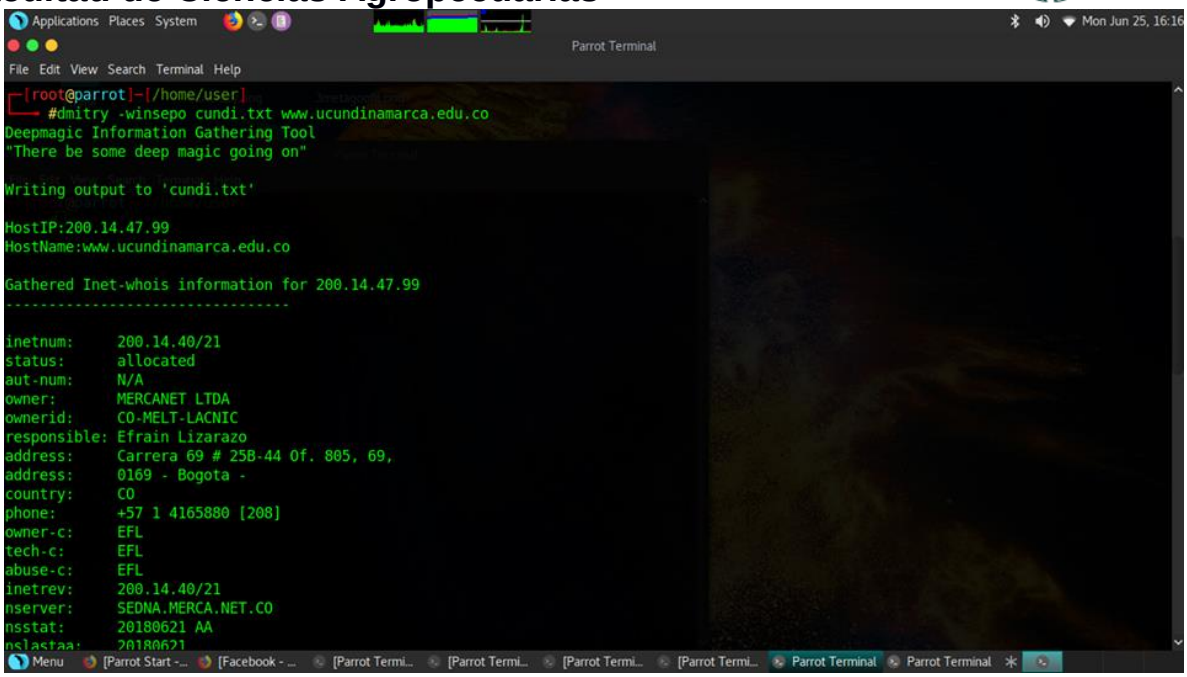


Figura No. 29, Uso de la herramienta Dmitry en www.ucundinamarca.edu.co; 2018-Autor

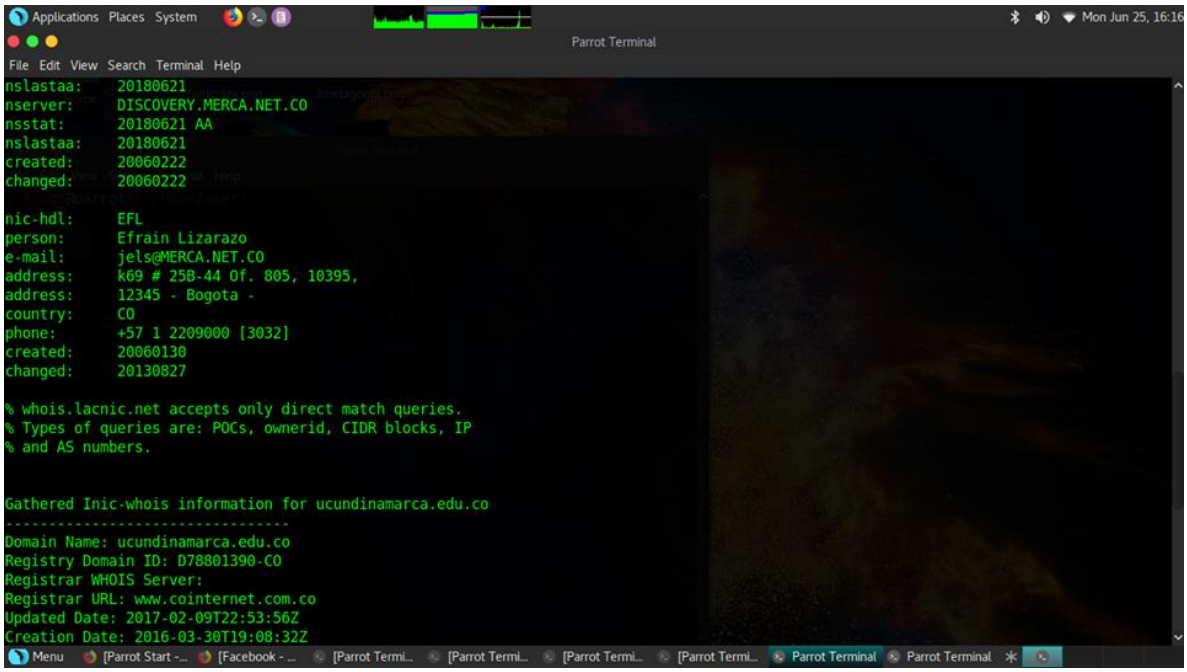


Figura No. 30, Uso de la herramienta Dmitry en www.ucundinamarca.edu.co; 2018-Autor

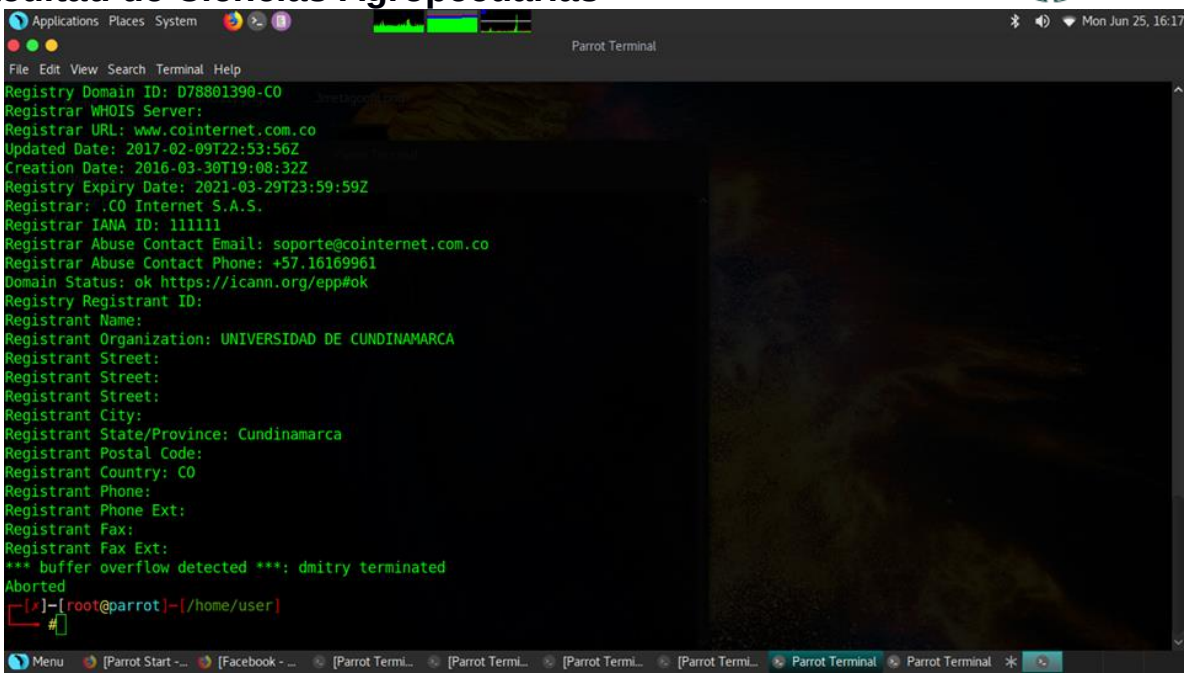


Figura No. 31, Uso de la herramienta Dmitry en www.ucundinamarca.edu.co; 2018-Autor

Bajo los aspectos de la herramienta ENUM4LINUX, se logran conocer algunos usuarios y esta misma intenta autenticarse en el servidor, aprovechando vulnerabilidades de SQLi, que como se observa en la imagen No. 32. No tiene un resultado positivo.

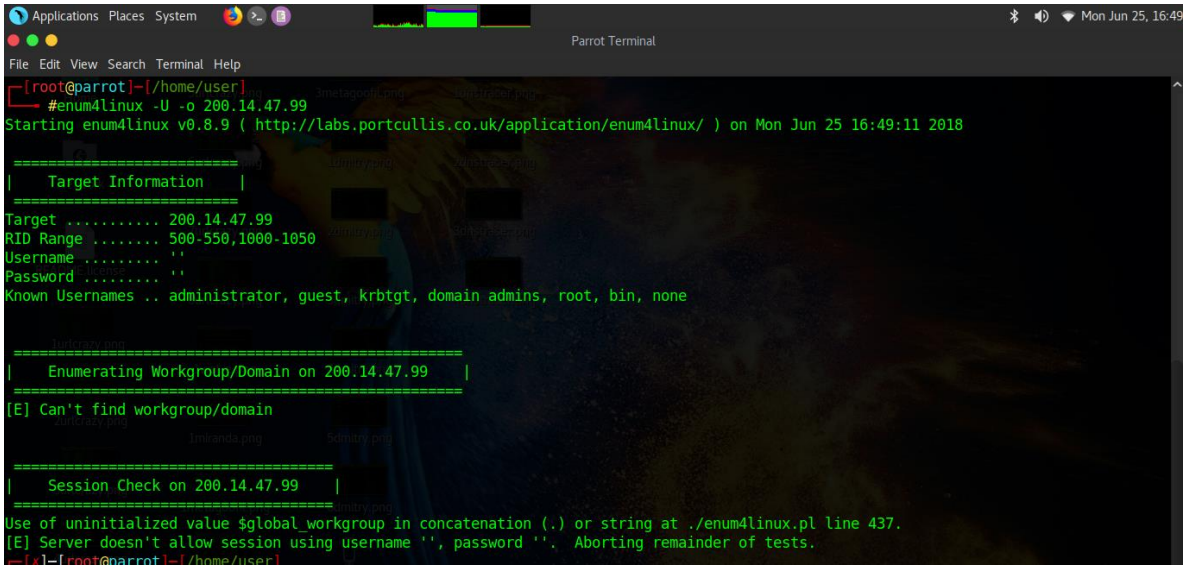


Figura No. 32, Uso de la herramienta Enum4linux en ucundinamarca.edu.co; 2018-Autor

Una de las herramientas, más conocidas y utilizadas en el mundo de la seguridad informática es nmap, este software permite hacer escaneos de redes para detectar fallas o intrusos, utilizando la menor cantidad de recursos, para no entorpecer las actividades de los usuarios de la red. También permite generar rastreo de puertos. En la imagen No. 33. Se realiza el este último proceso, el resultado cautivo al arrojar que solo se encuentran 3 puertos abiertos.

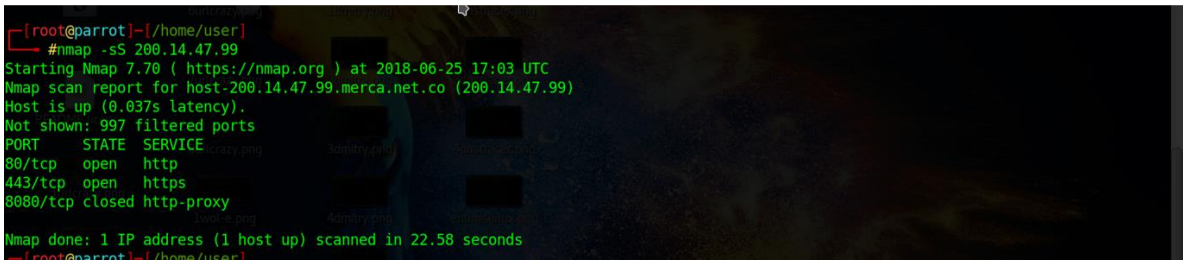


Figura No. 33, Rastreo de puertos con Nmap en 200.14.47.99 ; 2018-Autor

En la distribución de Kali Linux, encontramos un proyecto escrito en Python, el cual se enfoca a realizar auditorías automáticas, Este se llama GOLISMERO y uno de sus comandos más importantes, es el de scan que realiza un escáner a un sitio web. Tal como, se puede ver en la imagen No. 34. Se aplica esta herramienta, en el dominio de www.unicundi.edu.co y esta comienza utilizando a theharvester, identificando el host por medio de diferentes buscadores.

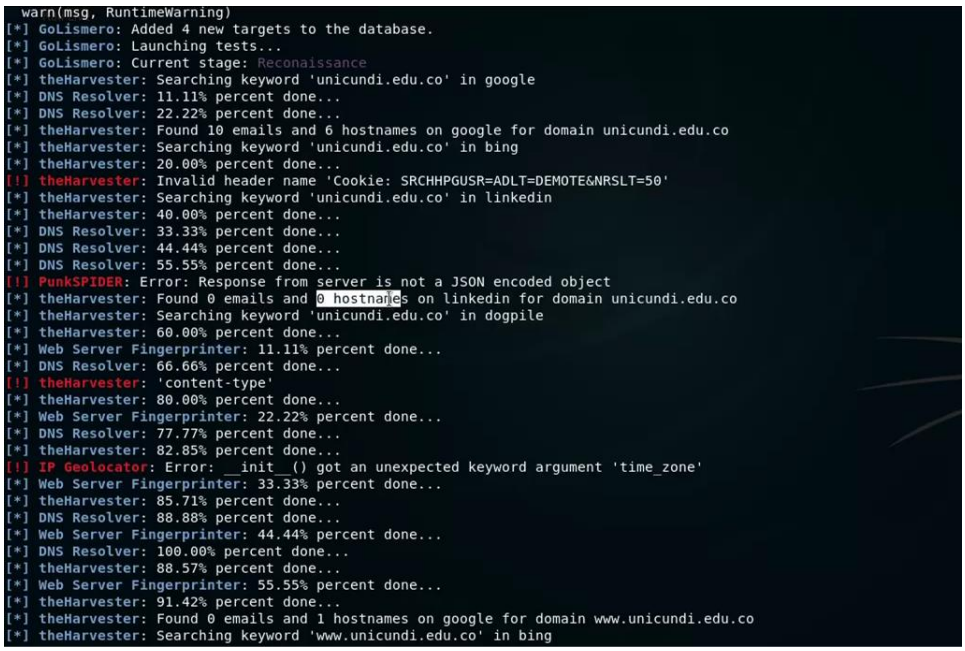


Figura No. 34, Scan de Golismero en www.unicundi.edu.co ; 2018-Autor

En la imagen No. 35 se evidencia como, golismero después de encontrar el host del sitio web realiza una búsqueda de los emails disponibles en la web y encuentra 31 correos, en dos búsquedas distintas además del servidor de correros de la institución mail.unicundi.edu.co.

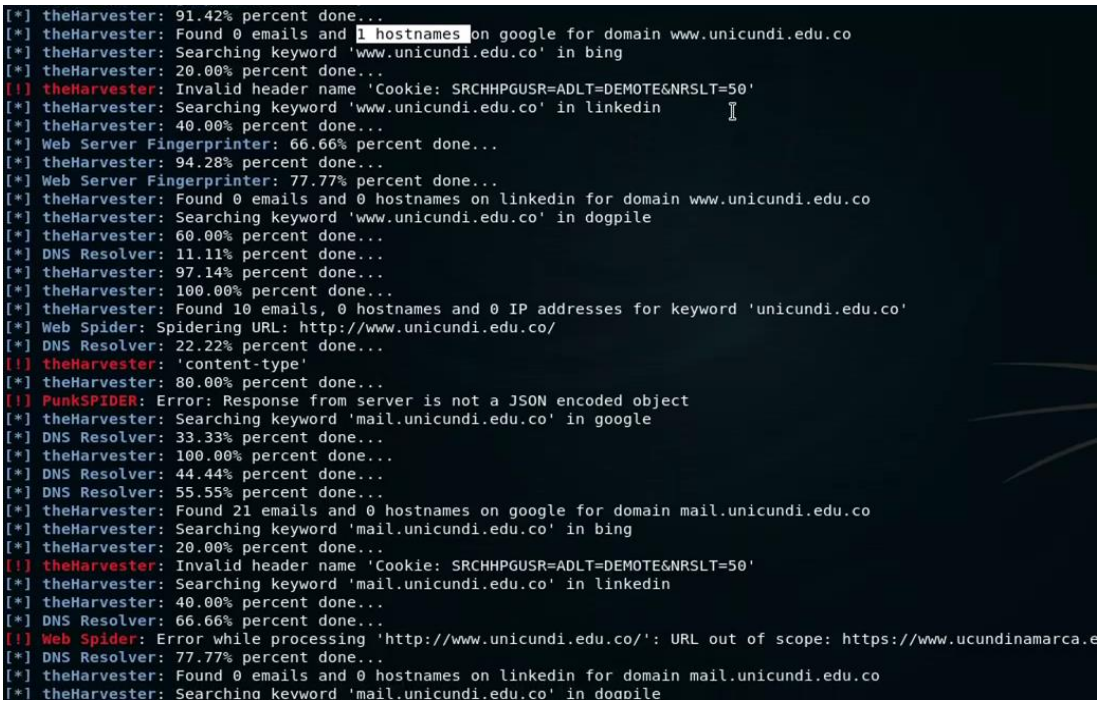


Figura No. 35, Scan de Golismero en www.unicundi.edu.co ; 2018-Autor

Una vez termina la etapa de scaneo la herramienta, se puede observar que esta encuentra cuatro subdominios para el dominio indicado. Imagen No. 36.

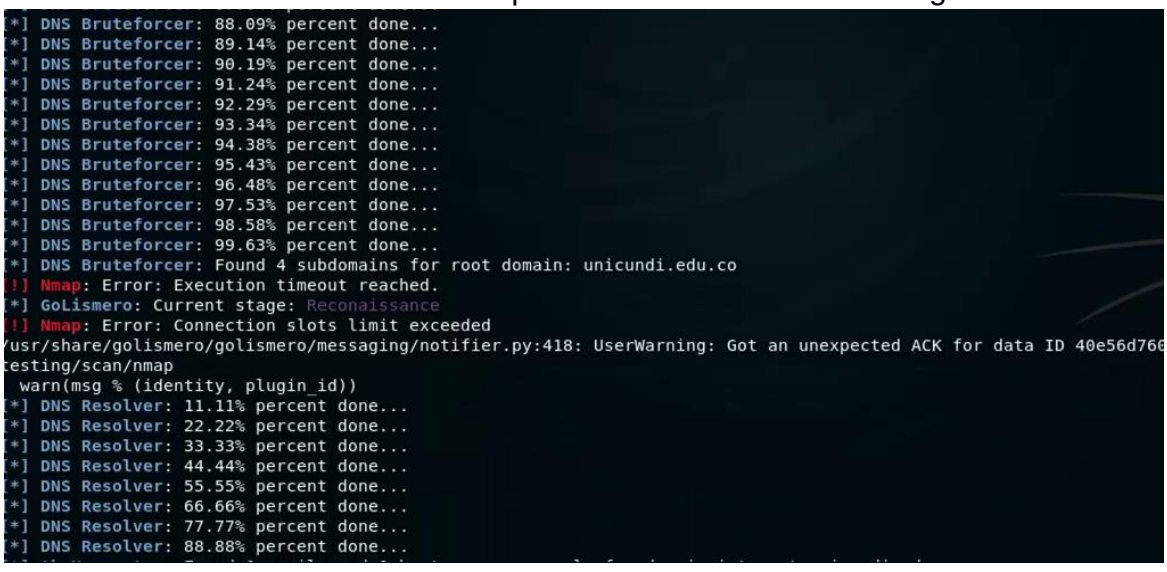


Figura No. 36, Scan de Golismero en www.unicundi.edu.co ; 2018-Autor

2.2.2 EXPLORACIÓN

La fase de exploración, consiste en conocer cuáles son los servicios que está corriendo el portal universitario. Trabajando con el sitio web, se evidencia que este exige un pluig-in o un software de flash, el cual es necesario para poder acceder a las actas y formatos, usados en su mayoría por los estamentos de la institución Imagen No. 37.

Figura No. 37, Requisito de flash en la web principal de la UdeC; 2018-Autor

Gracias a la herramienta golismero se puede apreciar información de los servicios del servidor, tales como: Apache /2.4.25, Sistema Unix OpenSSL/1.0.2, PHP/7.1.1 y módulos de PERL/ 2.0.8-DEV V5.16, así como identifica el redireccionamiento de www.unicundi.edu.co a www.ucundinamarca.edu.co, la conexión realizada al certificado SSL y testeando el puerto 443 además de identificar que no se encuentran vulnerabilidades en los protocolos TLS, el cual es el sucesor de SSL. Como se puede observar en la figura No. 38.

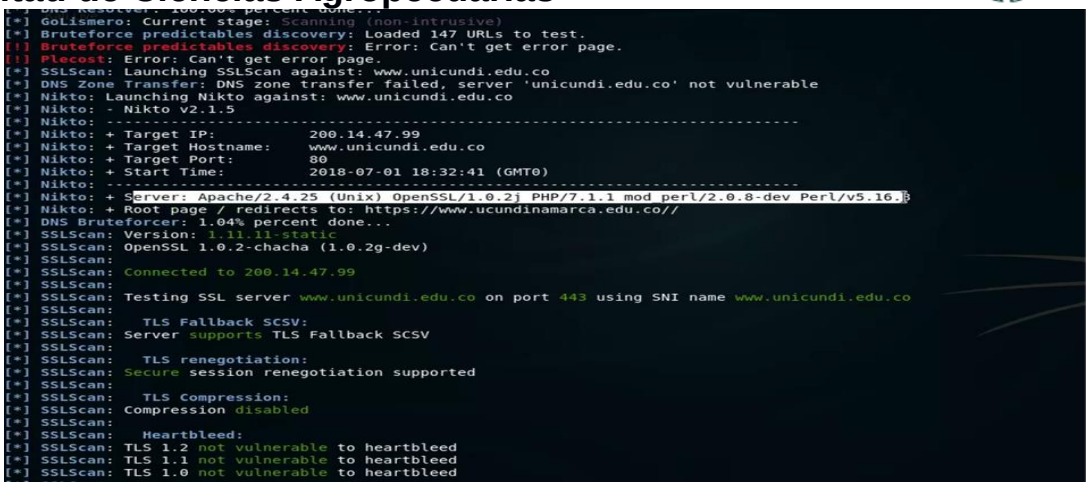


Figura No. 38, Servicios y protocolos utilizando Golismero en UDEC; 2018-Autor

En la imagen 39 y 40. Se evidencia como, la misma herramienta, logra identificar el tipo de criptografía que soporta y trabaja de manera preferencial el servidor. Identificando tres veces el mismo tipo de criptografía preferencial TLSv1.2 256 bits ECDHE-RSA-AES256-GCM-SHA383 Curve P-256 DHE 256

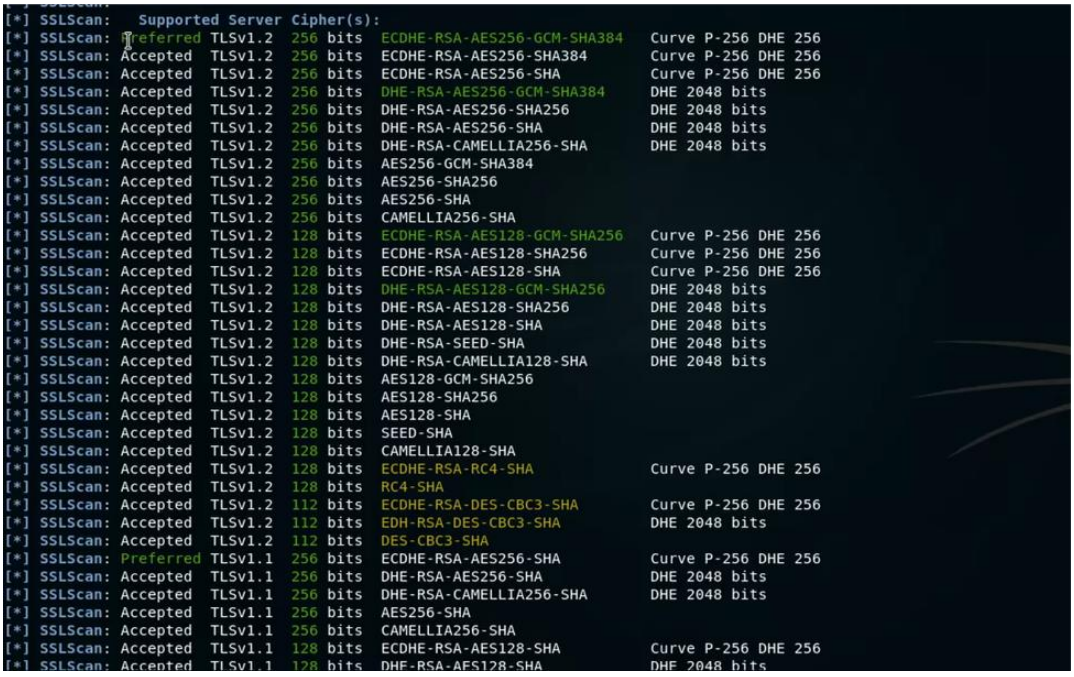


Figura No. 39, Criptografía utilizada en el servidor de la UDEC; 2018-Autor

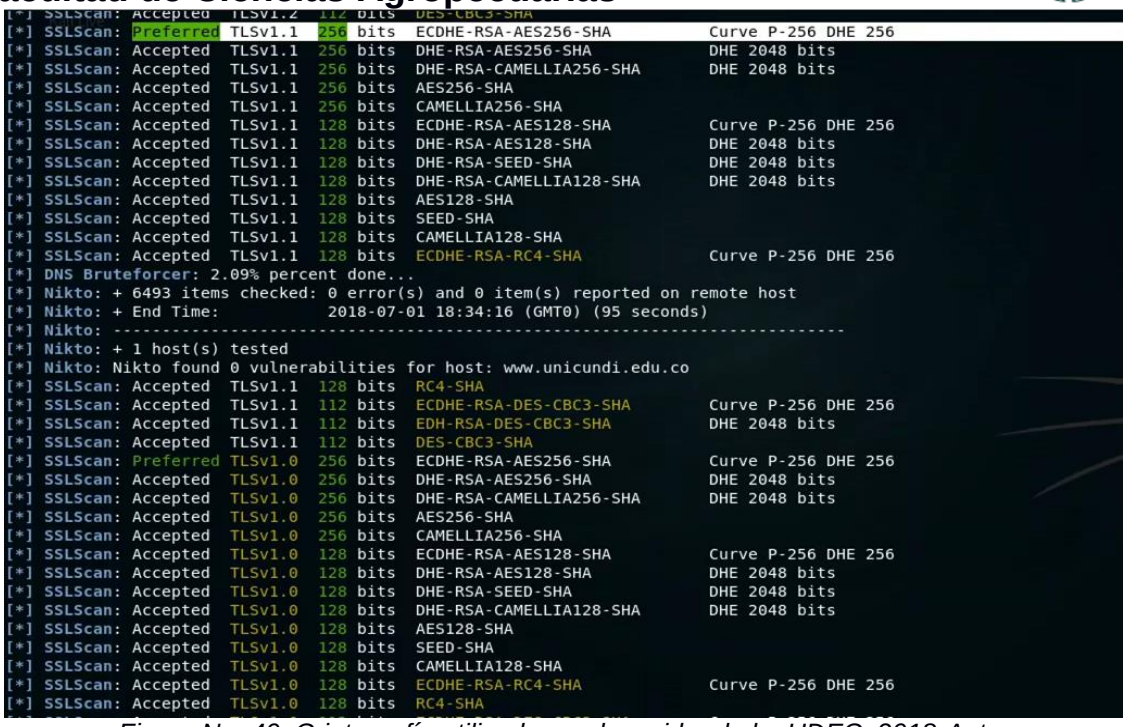


Figura No. 40, Criptografía utilizada en el servidor de la UDEC; 2018-Autor

Por otro lado, la herramienta Zenmap identifica que en el puerto 443 que se encuentra activo utiliza un protocolo TCP para el control de las trasmisiones de los distintos documentos que permite descargar este puerto imagen No. 41. Además de utilizar un servidor APACHE httpd 2.4.25 Utilizado desde un ordenador con OS Unix que trabaja un OpenSSL/1.0.2J con lenguajes de programación PHP y PERL.

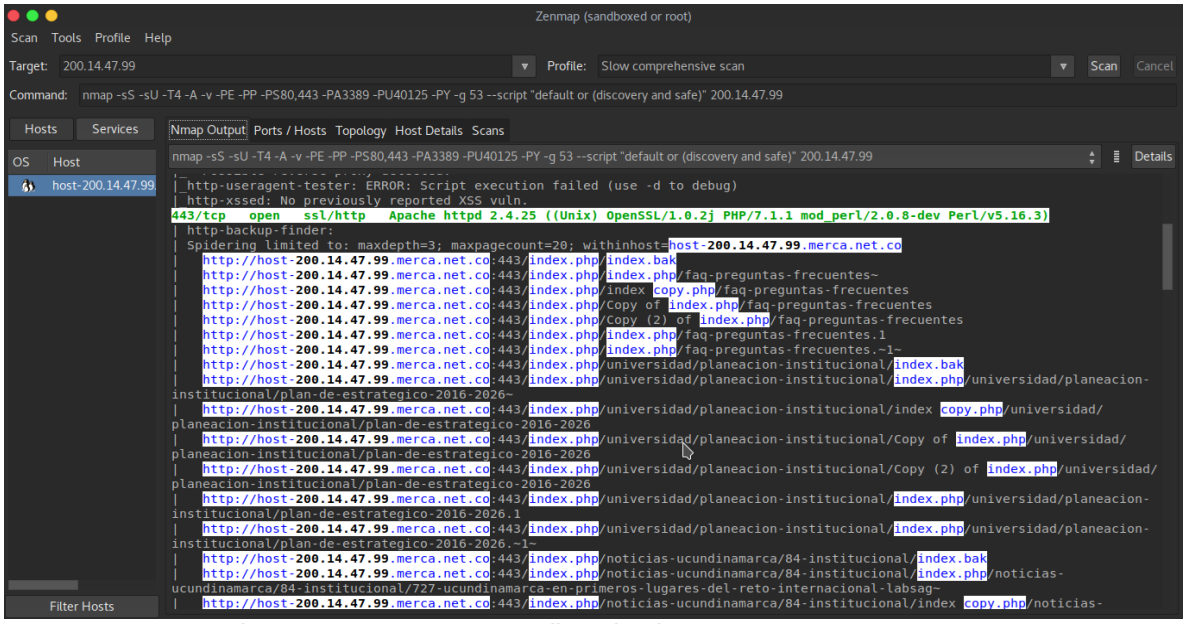


Figura No. 41, Zenmap analizando el puerto 443 UDEC; 2018-Autor

De la misma manera, los servicios que corren en el puerto 80 trabajan con un servidor APACHE httpd 2.4.25 Utilizado desde un ordenador con OS Unix que trabaja un OpenSSL/1.0.2J con lenguajes de programación PHP y PERL Imagen No 42.

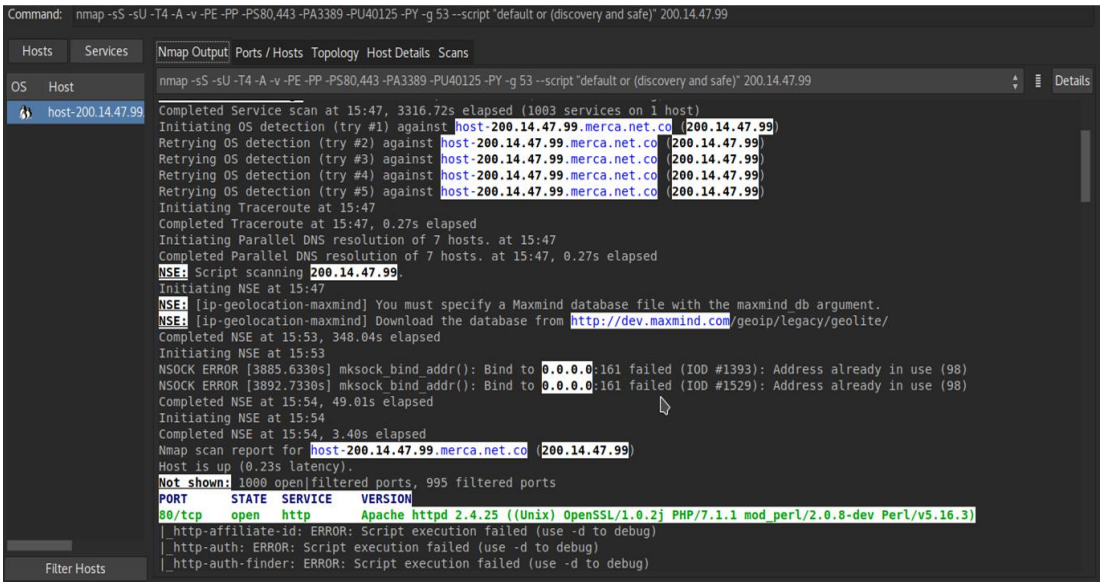


Figura No. 42, Zenmap analizando el puerto 443 UDEC; 2018-Autor

Pero en el caso del puerto 1500 se encuentra un protocolo de control de transmisión TCP, sumado a un certificado SSL que utiliza WEBMIN que es una interfaz basada en la web para administración del sistema para Unix. Que utilizando cualquier navegador web moderno, puede configurar cuentas de usuario, Apache, DNS, intercambio de archivos y mucho más. Webmin elimina la necesidad de editar manualmente los archivos de configuración de Unix como / etc / passwd, y le permite administrar un sistema desde la consola o de forma remota. Este servicio utiliza la versión MINSERV/1.870.

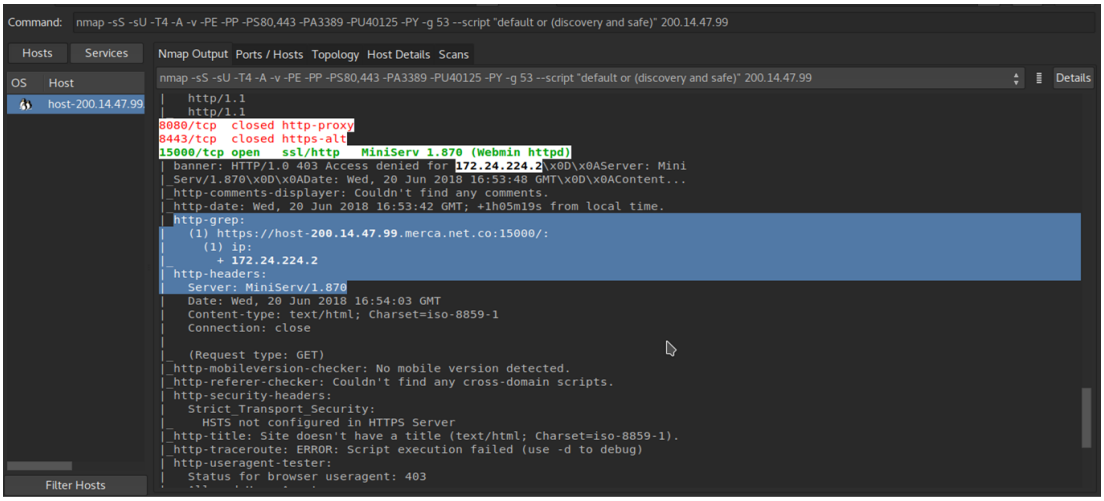


Figura No. 43, Zenmap analizando el puerto 15000 UDEC; 2018 -Autor

En la plataforma Windows se utiliza la herramienta Foca 3.4 la cual nos permite identificar el servidor de la institución, con los distintos servicios que se encuentran activos en él. Estos como se han mencionado anteriormente es un servidor APACHE, con módulos en php y perl además de un certificado de seguridad OpenSSL. Además de encontrar los dominios y los roles de este sitio web.

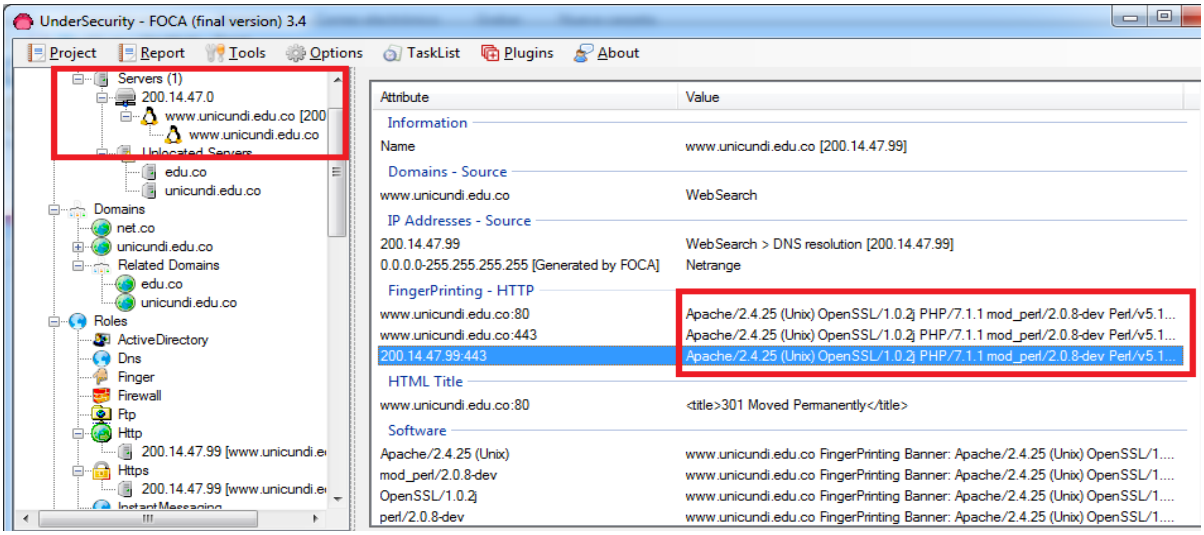


Figura No. 44, Foca 3.4 explorando el dominio de la UDEC; 2018 -Autor

Posterior a esto se realiza una búsqueda de documentos disponibles en la web de la institución para lo cual se trabaja con los buscadores: Google, Bing y Exalead. Por medio de la misma herramienta se logran extraer 771 archivos con información valiosa de la entidad, respecto a su funcionamiento interno y externo.

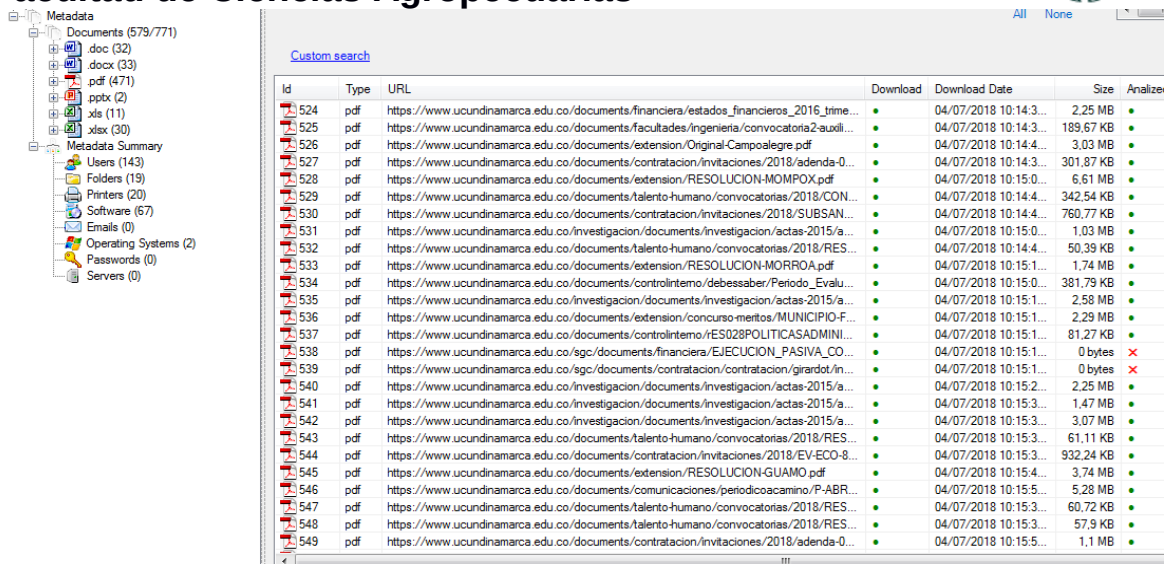


Figura No. 45, Foca 3.4 documentos descargados del puerto 443 de la UDEC; 2018-Autor

De esta manera una vez se descargan los documentos, se procede a extraer los metadatos de dichos documentos, es importante mencionar que el valor de los metadatos es el uso que se les dé a estos. Entre los metadatos se pudieron encontrar 135 clientes, identificando el tipo de sistema operativo utilizado.

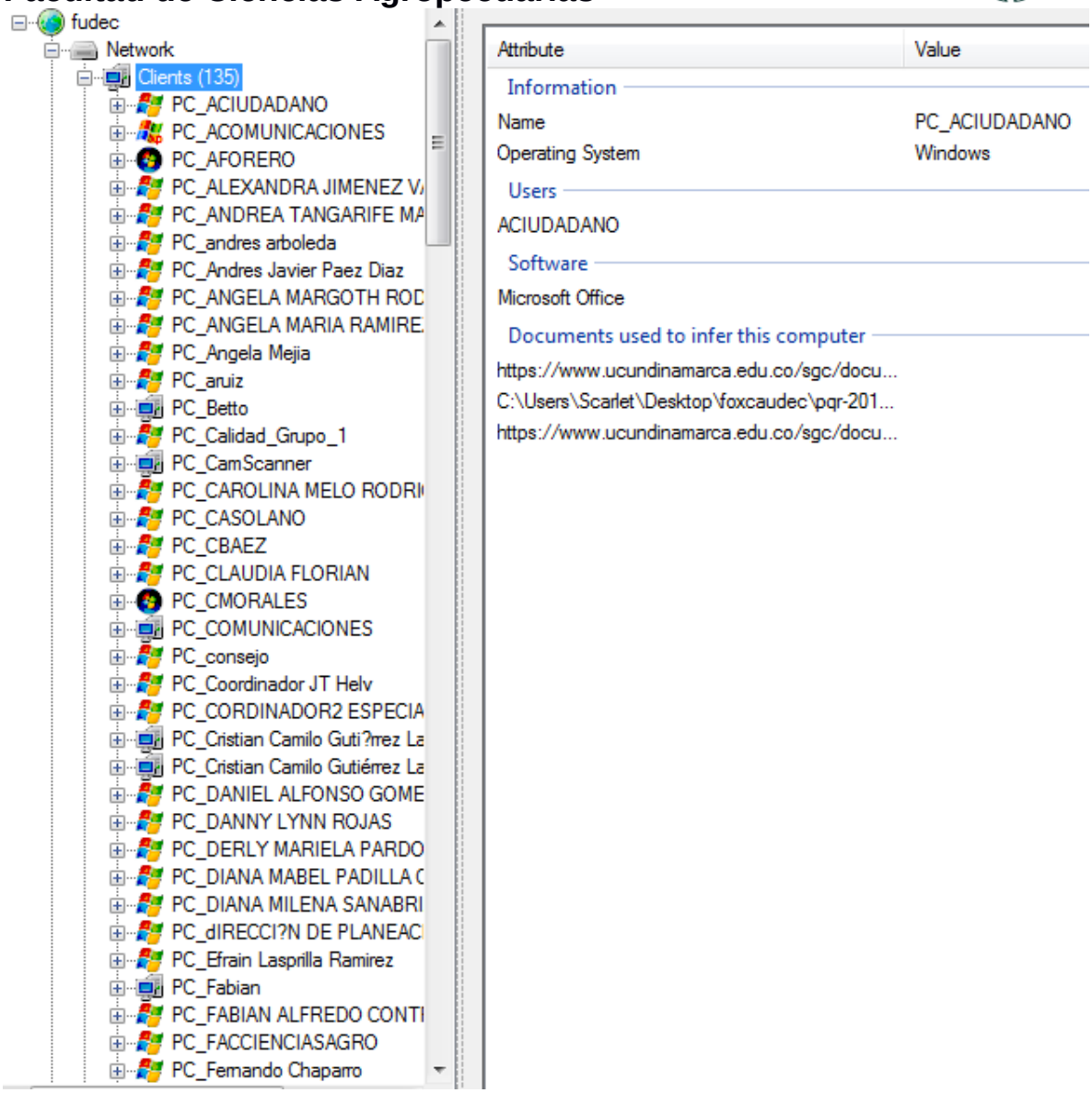


Figura No. 46, Foca 3.4 clientes del servidor de la UDEC; 2018-Autor

Además de encontrar los software's utilizados por estos usuarios que en total fueron 67, foca identifica algunas veces si el software es licenciado o no, además como se puede ver en la figura 47. Se encontraron 20 impresoras lo que quiere decir que de los 143 usuarios encontrados al menos 20 son del personal administrativo de la universidad.

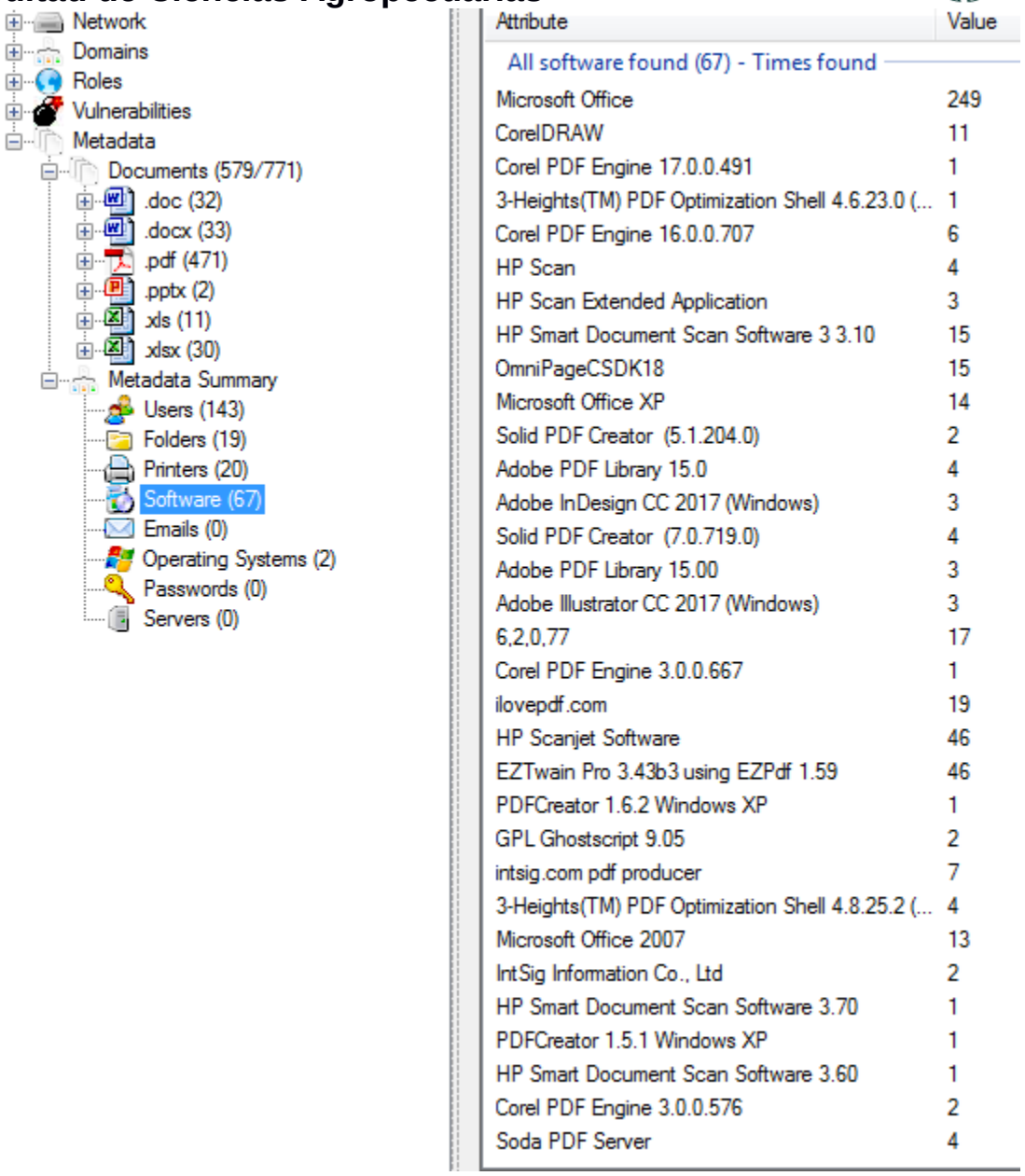


Figura No. 47, Foca 3.4 software de los clientes del servidor de la UDEC; 2018-Autor

He incluso después de realizar la extracción y análisis de metadatos se encuentra el nombre de algunos usuarios que tienen acceso al servidor.

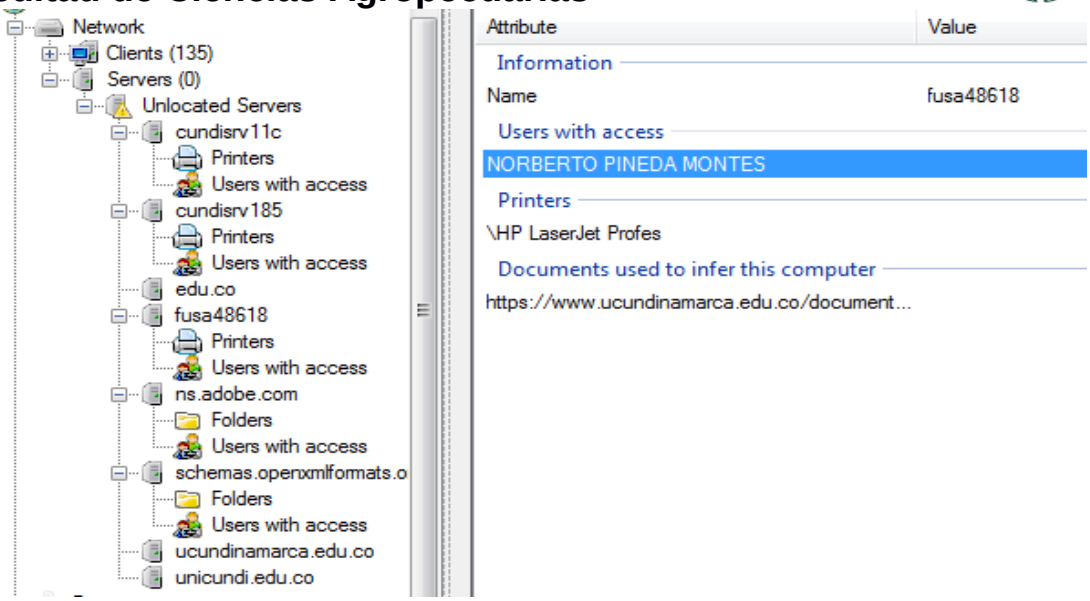


Figura No. 48, Foca 3.4 clientes con acceso al servidor de la UDEC; 2018-Autor

En el caso en concreto de NORBERTO PINEDA MONTES se puede verificar si este es un trabajador activo de la universidad solo con realizar una búsqueda en google. Donde no solo se pudo verificar que el 12 de junio del 2018 cargo un archivo al servidor el cual contenía las matrículas de honor otorgadas por la universidad, sino que este trabajo en la oficina asesora de comunicaciones y/o en análisis financiero.

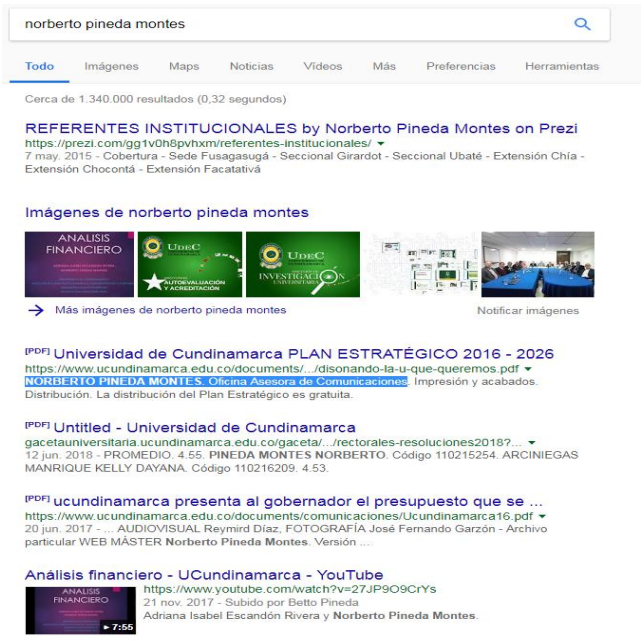


Figura No. 49, Identificación de clientes con privilegios en el servidor de la UDEC; 2018-Autor

Por medio de los plugins de foca se logra obtener los certificados SSL los cuales son otorgados por un intermediario de este tipo de certificados “Symantec Class” en su versión 3 EV SSL CA – G3 el cual es válido desde 01/062017 hasta el 03/06/2019.

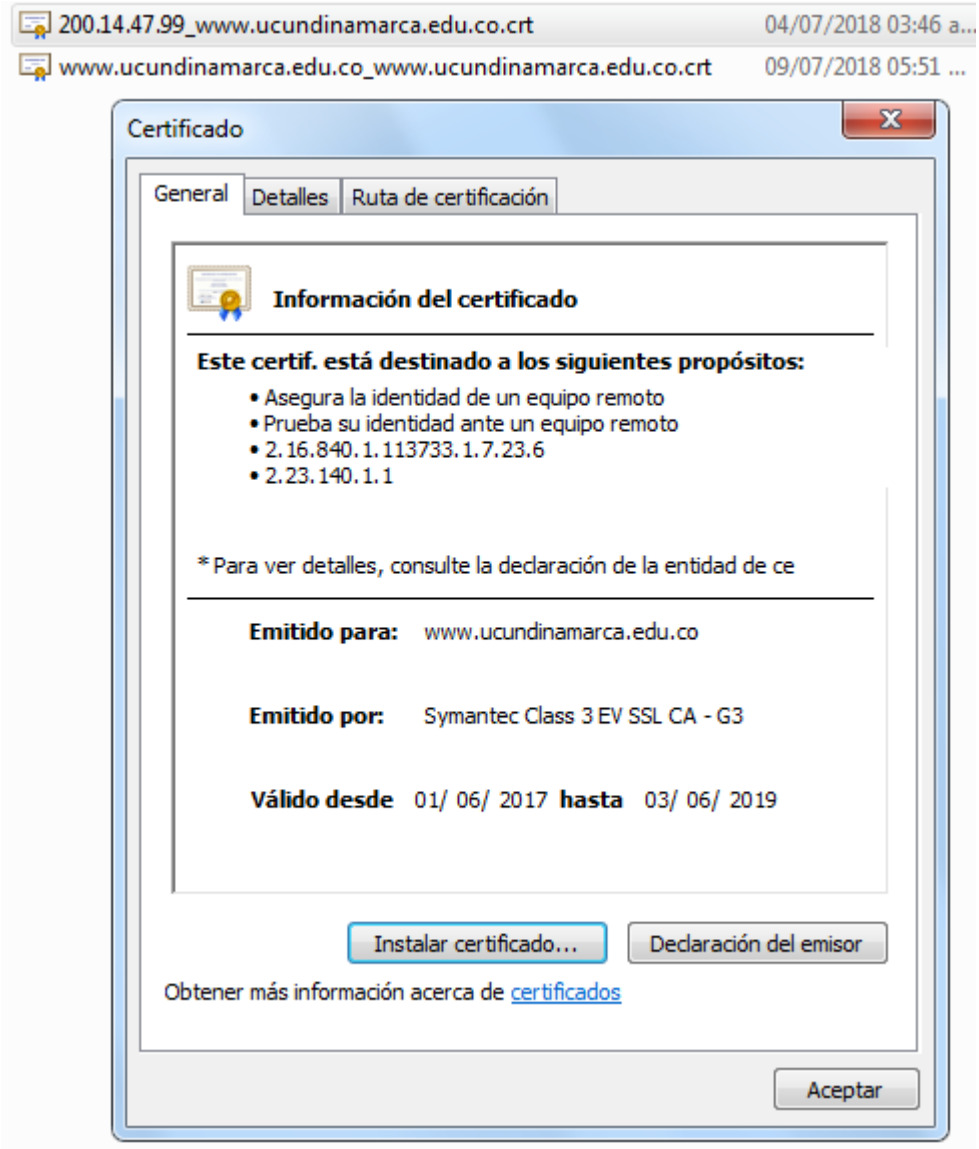


Figura No. 50, Certificado SSL de la UDEC; 2018-Autor

En una búsqueda anterior de estos certificados se encontró información relevante respecto a la huella digital, la firma digital y algunos de los caracteres especiales que utiliza la universidad.

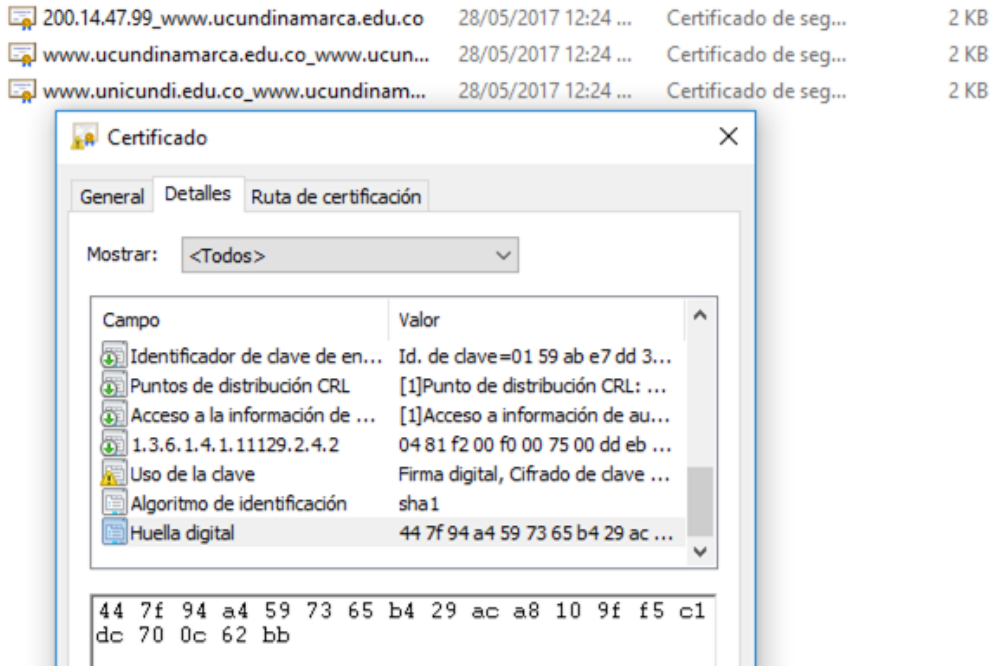


Figura No. 51, Certificado SSL de la UDEC; 2018-Autor

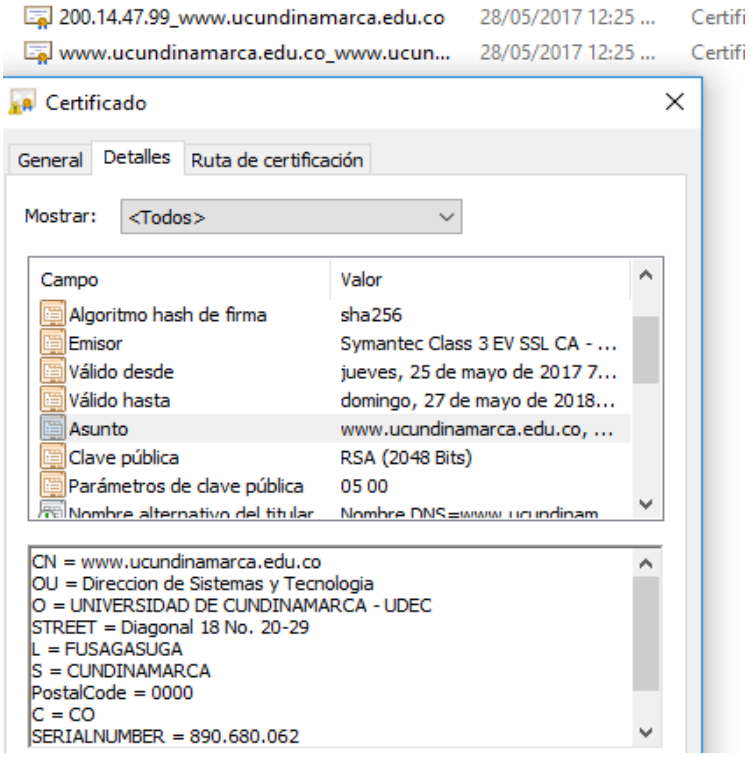


Figura No. 52, Certificado SSL de la UDEC; 2018-Autor

Para finalizar esta herramienta permite generar un informe de manera automática de la información más relevante encontrada.

```
Information:
Name    www.ucundinamarca.edu.co [200.14.47.99]
Domains - Source:
www.ucundinamarca.edu.co        WebSearch
IP Addresses - Source:
200.14.47.99    WebSearch > DNS resolution [200.14.47.99]

FingerPrinting - HTTP:
www.ucundinamarca.edu.co:80     Apache/2.4.25 (Unix) OpenSSL/1.0.2j PHP/7.1.1 mod_perl/2.0.8-dev Perl/v5.16.3
200.14.47.99:80 Apache/2.4.25 (Unix) OpenSSL/1.0.2j PHP/7.1.1 mod_perl/2.0.8-dev Perl/v5.16.3

FingerPrinting - DNS:
www.ucundinamarca.edu.co:53

HTML Title:
www.ucundinamarca.edu.co:80     <title>301 Moved Permanently</title>
200.14.47.99:80 <title>301 Moved Permanently</title>

Software:
Apache/2.4.25 (Unix)    www.ucundinamarca.edu.co FingerPrinting Banner: Apache/2.4.25 (Unix) OpenSSL/1.0.2j PHP/7.1.1 mod_perl/2.0.8-dev Perl/v5.16.3
mod_perl/2.0.8-dev      www.ucundinamarca.edu.co FingerPrinting Banner: Apache/2.4.25 (Unix) OpenSSL/1.0.2j PHP/7.1.1 mod_perl/2.0.8-dev Perl/v5.16.3
OpenSSL/1.0.2j  www.ucundinamarca.edu.co FingerPrinting Banner: Apache/2.4.25 (Unix) OpenSSL/1.0.2j PHP/7.1.1 mod_perl/2.0.8-dev Perl/v5.16.3
perl/2.0.8-dev  www.ucundinamarca.edu.co FingerPrinting Banner: Apache/2.4.25 (Unix) OpenSSL/1.0.2j PHP/7.1.1 mod_perl/2.0.8-dev Perl/v5.16.3
PHP/7.1.1       www.ucundinamarca.edu.co FingerPrinting Banner: Apache/2.4.25 (Unix) OpenSSL/1.0.2j PHP/7.1.1 mod_perl/2.0.8-dev Perl/v5.16.3
```

Figura No. 53, Informe de la información recolectada con Foca 3.4; 2018-Autor

2.3 ANÁLISIS DE RIESGOS Y VULNERABILIDADES

Basándose en la información recolectada, con las distintas herramientas y procesos, se realizará el análisis de riesgos y vulnerabilidades. El cual consiste en identificar los riesgos, a los que puede estar expuesta la entidad, cuantificando los impactos que este puede llegar a tener y basándose en la información previa que posee la institución, en su *control interno* como también en la *matriz de identificación de riesgos y oportunidades, la valoración de riesgo residual* y *la valoración de riesgo inherente* del *macroproceso estratégico de la Universidad de Cundinamarca*.

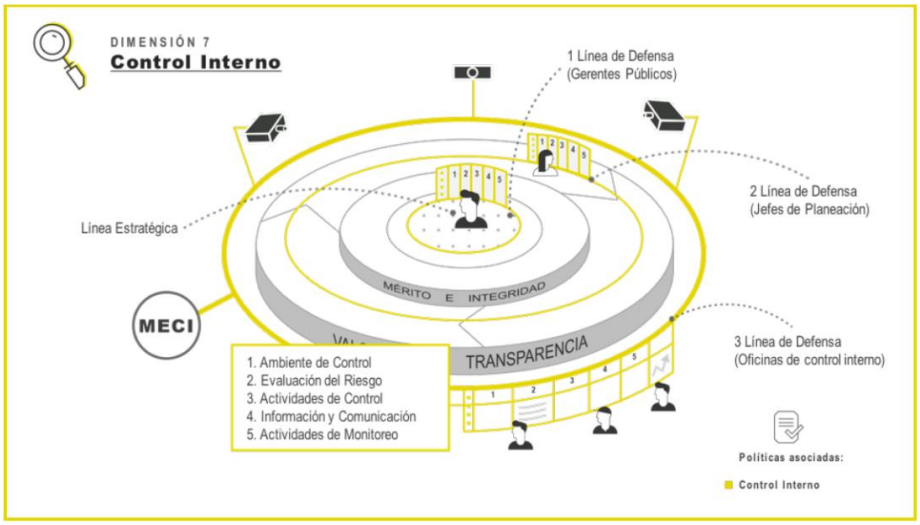


Figura No. 54, Diseño de seguridad del control interno UDEC; 2018-Ofc. Control Interno

	MACROPROCESO ESTRATEGICO	CODIGO: ESGr028
	PROCESO GESTION SISTEMAS INTEGRADOS	VERSION: 8
	MATRIZ DE IDENTIFICACION DE RIESGOS Y OPORTUNIDADES	VIGENCIA: 2018-03-02
		PAGINA: 1 de 5

NOMBRE DEL PROCESO	GESTIÓN ADMISIONES Y REGISTRO
FECHA DE ACTUALIZACIÓN	MARZO 13 DE 2018
OBJETIVO DEL PROCESO	Administrar y controlar las actividades de Admisiones y Registro, para garantizar el cumplimiento de los requisitos y normas vigentes sobre la selección, admision, permanencia, promocion, permanencia, promocion y graduacion de los estudiantes de la Universidad de Cundinamarca.

FACTORES INTERNOS DE LA UNIVERSIDAD DE CUNDINAMARCA DEBILIDADES
Enumere los factores que en el proceso se consideran una debilidad; por ejemplo: 1. Equipo de trabajo insuficiente en número de personas
D1. Inestabilidad laboral (en la renovación de los contratos) de algunos funcionarios adscritos a la oficina.
D2. Personal insuficiente para las actividades del proceso.
D3. En todas las seccionales y extensiones no se cuenta con las condiciones adecuadas para la conservación de los documentos.
D4. Dependencia de otras areas para la ejecucion de las actividades del proceso
D5. Falta de línea telefónica en la extensión de Soacha y Chía.
D6. Documentación existente en archivo físico que no se encuentra digitalizado o sistematizado.
D7. Los consejos de Facultad y las direcciones de programa no envían oportunamente a la oficina de Admisiones y Registro, las actas de consejo, actas de sustentación y vistos buenos, para iniciar el proceso de Revisión de carpeta para Grados y Novedades Académicas.
D8. Demora de la oficina de tesorería en cargar archivos planos de los pagos realizados por parte de los estudiantes y aspirantes.
D9. Falta de digitación oportuna de Notas por parte de los docentes de los diferentes programas Académicos.
D10. No contar con un Rubro propio
D11. Equipos de Computo con capacidad limitada

FACTORES EXTERNOS DE LA UNIVERSIDAD DE CUNDINAMARCA AMENAZAS
Enumere los factores que en el entorno se consideran una amenaza para el proceso; por ejemplo: 1. Oferta académica innovadora de las universidades competidoras
A1. Hackers y virus informáticos
A2. Actualizaciones en plataforma del ICFES
A3. Falta de interés por parte del aspirante en consultar el Instructivo en el portal web.
A4. Fenómenos naturales como inundaciones e incendios
A5. Paros Estudiantiles

FACTORES INTERNOS DE LA UNIVERSIDAD DE CUNDINAMARCA FORTALEZAS
Enumere los factores que en el proceso se consideran una debilidad; por ejemplo: 1. Presupuesto aprobado suficiente para las necesidades del proceso
F1. Equipo de trabajo calificado y comprometido.
F2. Liderazgo centralizado en la Sede Principal.
F3. Oportunidad y calidad en la prestación del servicio.
F4. Construcción y Disponibilidad de información estadística.
F5. Interacción operativa con otras dependencias.
F6. Promoción y divulgación de los programas en la Universidad de manera virtual.
F7.Capacitaciones y socializaciones de los procedimientos que la oficina de admisiones ha

FACTORES EXTERNOS DE LA UNIVERSIDAD DE CUNDINAMARCA OPORTUNIDADES
Enumere los factores que en el entorno se consideran una oportunidad para el proceso; por ejemplo: 1. Amplia oferta tecnológica de equipos y aplicativos en el mercado.
O1. Demanda en la Educación virtual en programas de Postgrado.
O2. Crecimiento de la población estudiantil.
O3. Becas otorgadas por convenios interinstitucionales.
O4. Baja competencia en la región donde hace presencia la Institución.
O5. La expedición de la norma de Inclusión

IDENTIFICACIÓN DOFA | CRUCE RIESGOS | MAPA RIESGOS | CRUCE OPORTUNIDADES | MAPA OPORTUNIDADES

Figura No. 55, Matriz de identificación de riesgos y oportunidades*; UDEC 2018*

VALORACIÓN DE RIESGO RESIDUAL							CONCLUS
MAGNITUD DEL IMPACTO	VALORACIÓN	NIVEL	FECHA DE SEGUIMIENTO	OBSERVACIONES Y RECOMENDACIONES	FECHA DE SEGUIMIENTO	OBSERVACIONES Y RECOMENDACIONES	FECHA DE SEGUIMIENTO
2	6	MODERADO	09/10/2017	Se realizo el proceso de envió a la Oficina de Gestión Documental de Hojas de Vida de Estudiantes Retirados ITUC. Se tienen listos los archivos de Retirados UCundinamarca para entrega al proceso de gestión documental y se esta realizando la respectiva clasificación y verificación de los mismos. Se anexa evidencia de Inventario Documental el cual se encuentra totalizado en el equipo de placa 44904 y Placa 44905	24/04/2018	Depuración, Clasificación y Organización de Hojas de Vida de Estudiantes Retirados de la Universidad de Cundinamarca. Actualización de Hojas de Vida en el Archivo del Proceso de Admisiones y Registro.	25/04/2018
4	4	ALTO	10/10/2017	Todos los reportes se realizaron de manera oportuna según Calendario Académico	24/04/2018	Todas las actividades programadas se reportaron de manera oportuna en cumplimiento al Calendario Académico	
1	2	BAJO	11/10/2017	Recordatorio a Direcciones de programa sobre el envió oportuno de Actas de Sustentación, Visto Bueno del programa para el procedimiento de Grados y Titulo Académicos y el reporte Oportuno de Notas a los docentes de los diferentes programas académicos.	24/04/2018	Se notifica a las Direcciones de Programa recordatorio de Actividades en cumplimiento al calendario Académico.	

Figura No. 56, Matriz de valoración de riesgo residual*; UDEC 2018*

	MACROPROCESO ESTRATEGICO	CODIGO: ESGr028
	PROCESO GESTION SISTEMAS INTEGRADOS	VERSION: 8
	MATRIZ DE IDENTIFICACION DE RIESGOS Y OPORTUNIDADES	VIGENCIA: 2018-03-02
		PAGINA: 1 de 5

NOMBRE DEL PROCESO	Control Interno
FECHA DE ACTUALIZACIÓN	Febrero 8 de 2018
OBJETIVO DEL PROCESO	Realizar verificación, seguimiento, evaluación y control de manera oportuna y sistemática a los Macroprocesos que conforman el modelo de operación de la Universidad a través de mecanismos e instrumentos que garanticen el cumplimiento de la normatividad aplicable y el mejoramiento continuo.

FACTORES INTERNOS DE LA UNIVERSIDAD DE CUNDINAMARCA DEBILIDADES	FACTORES EXTERNOS DE LA UNIVERSIDAD DE CUNDINAMARCA AMENAZAS
Enumere los factores que en el proceso se consideran una debilidad; por ejemplo: 1. Equipo de trabajo insuficiente en número de personas	Enumere los factores que en el entorno se consideran una amenaza para el proceso; por ejemplo: 1. Oferta académica innovadora de las universidades competidoras
D1. Faltan lineamientos de Gestión Ambiental.	A1. Falta de actualización en la Legislación Externa e Interna.
D2. No hay suficiente capacidad instalada para atender las necesidades de la Universidad.	A2. Posibilidad de que por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
D3. Falta de sistematización en la Oficina.	A3. No continuidad de las practicas por lineamientos políticos
D4. Falta de conocimiento del Plan de Seguridad Vial.	A4 Hackers informáticos
D5. Falta de continuidad en la Contratación de personal Administrativo.	A5. Requisitos de propiedad intelectual
D6. Falta de capacitación para el personal de la Oficina.	A6. Sanciones por incumplimiento a entes de control
D7. Retrasos en la Información solicitada a los procesos.	
D8. Falta de lineamientos en Seguridad de la Información.	
D9. Falta apropiación del personal a los lineamientos de seguridad de la información	
FACTORES INTERNOS DE LA UNIVERSIDAD DE CUNDINAMARCA FORTALEZAS	**FACTORES EXTERNOS DE LA UNIVERSIDAD DE CUNDINAMARCA OPORTUNIDADES**
Enumere los factores que en el proceso se consideran una debilidad; por ejemplo: 1. Presupuesto aprobado suficiente para las necesidades del proceso	Enumere los factores que en el entorno se consideran una oportunidad para el proceso; por ejemplo: 1. Amplia oferta tecnológica de equipos y aplicativos en el mercado.
F1. Liderazgo del Gestor Responsable.	O1. Generar transferencia de conocimiento a través de la Educación Continuada.
F2. Equipo de Trabajo Multidisciplinario.	O2. Información Actualizada enviada por Entes de Control Interno.
F3. Buen clima Organizacional.	O3. Modelo Integrado de Planeación y Gestión.
F4. Adaptación al cambio.	O4. Falta de competencia de las oficinas de control interno de la región
F5. Mayor receptibilidad del Proceso.	O5. Auditorías por parte de entes de control
F6. Mayor cobertura en el desarrollo de actividades de los Procesos.	
F7. Utilización de los medios de Comunicación de la Universidad.	
F8. Posicionamiento de la Oficina de Control Interno a nivel regional.	
F9. Los profesionales de la oficina tiene mayor empoderamiento debido al fortalecimiento de las competencias	
F10. Cultura de trabajo enfocada a resultados	

IDENTIFICACIÓN DOFA | CRUCE RIESGOS | MAPA RIESGOS | CRUCE OPORTUNIDADES | MAPA OPORTUNIDADES

*Figura No. 57, M*atriz de identificación de riesgos y oportunidades*; UDEC 2018*

VALORACIÓN DEL RIESGO INHERENTE					
MAGNITUD DEL IMPACTO	VALORACIÓN	NIVEL	CONTROLES APLICABLES	CLASIFICACIÓN DE LOS CONTROLES	ENTREGABI
5	15	EXTREMO	Unidad Virtual en la Nube Archivo documental Entrega Inventario documental de la Oficina	PREVENTIVO	Drive Actualizado Aplicativo SICR – Formato Inventario Document
5	10	EXTREMO	Actualización del Normograma del Proceso Capacitaciones Internas Actualizaciones por parte de Entes Externos Revisión en el ejercicio de Auditoria de los criterios	PREVENTIVO	Normograma Listas de Asistencia Reportes de entes Externos Informes de Auditoría
4	12	EXTREMO	Cronograma de Actividades Seguimiento a las actividades del Proceso	PREVENTIVO	Cronograma de Actividades Listas de Asistencia Informes de Auditoría Informe de Gestión de Control Interno
3	9	ALTO	Matriz de No Conformidades Aplicativo de Acciones Preventivas y de Mejora	PREVENTIVO	Matriz de No Conformidades Informes de Auditoría
4	12	EXTREMO	Mediciones Trimestrales Seguimientos Mensuales	PREVENTIVO	Matriz de Plan de Acción
5	10	EXTREMO	Actualización de conocimientos y competencias del equipo auditor Metodología para Auditorías Mesas de Trabajo para unificación de criterios	PREVENTIVO	Listas de Asistencia Certificados de formación Informes de Auditoría

IDENTIFICACIÓN DOFA | CRUCE RIESGOS | MAPA RIESGOS | CRUCE OPORTUNIDADES | MAPA OPORTUNIDADES

Figura No. 58, Matriz de valoración del riesgo inherente; UDEC *2018*

F	G	H	I	J	K	L
CIÓN DE LAS OPORTUNIDADES		VALORACIÓN DE LA OPORTUNIDAD INHERENTE				
CONSECUENCIA (OPORTUNIDADES)	CLASIFICACIÓN	PROBABILIDAD DE OCURRENCIA	MAGNITUD DEL IMPACTO	VALORACIÓN	NIVEL	CONTROLES AP
Implementación de aplicativos relacionados a las actividades de la oficina de control interno	Oportunidad Operativa: Comprenden oportunidades provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad, de la articulación entre dependencias.	3	4	12	ALTO	Actualización de aplicativos Cronogramas de desarrollo de software
Implementación de la inducción del MECI hacia la comunidad	Oportunidades de Cumplimiento: Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.	1	5	5	FAVORABLE	Desarrollo del módulo virtual Lanzamiento Videos

Figura No. 59, Matriz de valoración de la oportunidad inherente*; UDEC 2018*

Y en información relevante respecto, a la administración de información documentada, en resultados de la matriz de identificación de riesgos y oportunidades, los tiempos de respuesta, cierre de requerimiento y usuarios autorizados del manual de sistemas y tecnología y el diagrama de manejo de información de la Universidad de Cundinamarca.

	MACROPROCESO ESTRATÉGICO	CÓDIGO: ESGP01
	PROCESO GESTIÓN SISTEMAS INTEGRADOS	VERSIÓN: 15
	ADMINISTRACIÓN DE INFORMACIÓN DOCUMENTADA	VIGENCIA: 2018-07-12
		PAGINA: 4 de 11

ACTIVIDAD	RESPONSABLE	CONTROL	DOCUMENTO DE REFERENCIA	REGISTRO RESULTANTE
revisión de su estructura documental.				calidad@ucundinamarca.edu.co
2. Realizar apertura del Módulo SAD –Sistema de Actualización de Documentos los tres primeros días hábiles de cada mes o extraordinariamente cuando fuere necesario.	Gestor Oficina de Calidad	Las Solicitudes Extraordinarias, se deben soportar en una solicitud formal del Gestor Responsable del Proceso, mediante correo electrónico	ADOr001 Solicitudes mediante Correo electrónico: calidad@ucundinamarca.edu.co	Correo electrónico: calidad@ucundinamarca.edu.co
3. Enviar correo electrónico a todos los procesos informando las fechas en las que podrán hacer las Solicitudes de Actualización de Documentos.	Gestor Oficina de Calidad	N/A	EPIr001	ADOr001 Correo electrónico: calidad@ucundinamarca.edu.co
4. Registrar Solicitud mediante el módulo SAD y adjuntar los soportes respectivos.	Gestor Responsable del Proceso	N/A	Correo electrónico: calidad@ucundinamarca.edu.co	Listado de Solicitudes en el módulo SAD
5. Revisar las Solicitudes y verificar los documentos que soportan la solicitud asegurando el cumplimiento de los criterios establecidos para la elaboración de documentos del Sistema de Gestión de la Calidad.	Gestor Oficina de Calidad	En caso de no cumplir con los criterios establecidos, informar mediante correo electrónico al Gestor responsable del proceso, las inconsistencias presentadas para que en el término de los tres (3) días	ESGI001	Listado de Solicitudes en el módulo SAD Correo electrónico: calidad@ucundinamarca.edu.co

Figura No. 60, Administración de información documentada en la UDEC*; UDEC 2018*

	MACROPROCESO ESTRATÉGICO	CÓDIGO: ESGr028
	PROCESO GESTIÓN SISTEMAS INTEGRADOS	VERSIÓN: 9
	MATRIZ DE IDENTIFICACIÓN DE RIESGOS Y OPORTUNIDADES	VIGENCIA: 2018-07-12
		PAGINA: 7 de 8

CONTROL DE CAMBIOS				
VERSIÓN	FECHA DE APROBACIÓN			DESCRIPCIÓN DEL CAMBIO
	AAAA	MM	DD	
1	2013	10	08	Emisión del Documento.
2	2013	12	17	Inclusión de la casilla "Estado de avance de las acciones implementadas".
3	2014	08	29	Se requiere la eliminación de la columna calificación, agregar columnas de observaciones del Proceso Gestión Calidad y Gestión Control Interno.
4	2014	11	08	Mejora del formato, se agregan campos necesarios para su diligenciamiento.
5	2017	06	06	Inclusión de contexto a través de la herramienta DOFA, adición de oportunidades, Inclusión de mapa de riesgos y oportunidades, ajustes de acuerdo a los requisitos 4.1 y 6.1 de la ISO 9001:2015.
6	2017	08	10	Se modifica el lenguaje del documento.
7	2018	02	05	Se modifica tabla de Riesgos y Oportunidades, siguiendo lineamientos de DAFP.
8	2018	03	01	Se modifica códigos del documento, en razón a la actualización documental (Resolución 156 de 2017).
9	2018	07	12	Se agregan campos para evidenciar la Trazabilidad de la información contenida en el formato.

Figura No. 61, Matriz de identificación y oportunidad de la UDEC*; UDEC 2018*

Servicio	Tipo de Requerimiento	¿Quién puede solicitar?	días para la respuesta previa	días para cerrar el requerimiento
Gestión de la Infraestructura Tecnológica y los Recursos Informáticos	Solicitud de Recursos informáticos	Gestor responsable del proceso	8 días hábiles	Vigencia del proyecto
Desarrollo de Software: Por medio de esta categoría los procesos podrán solicitar soluciones de software para sus actividades que realizan dentro de sus procedimientos cotidianos.	Actualización	Gestor responsable del proceso	3 días hábiles	De 30 a 90 días hábiles
	Calidad de Software	Gestor responsable del proceso	3 días hábiles	De 1 a 30 días hábiles
	Nuevo Desarrollo	Gestor responsable del proceso	3 días hábiles	De 30 a 90 días hábiles
Soporte a Recursos Informáticos: Por medio de esta categoría los usuarios podrán realizar solicitudes para resolver las fallas técnicas que se presenten con los	Asistencia técnica	Gestor responsable o gestores del proceso	2 días hábiles	De 1 a 5 días hábiles
	Copia de Seguridad (Backup)	Gestor responsable o gestores del proceso	2 días hábiles	De 1 a 5 días hábiles

Figura No. 62, tiempos de respuesta, cierre de requerimiento y usuarios autorizados del manual de sistemas y tecnología; UDEC 2018

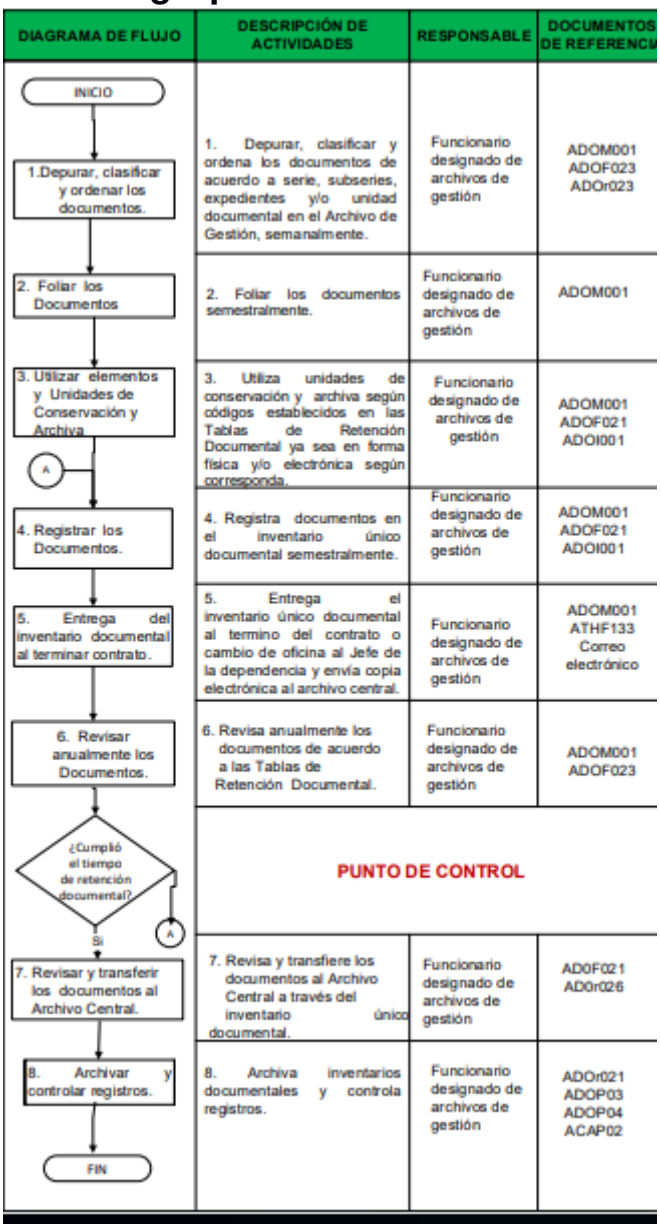


DIAGRAMA DE FLUJO	DESCRIPCIÓN DE ACTIVIDADES	RESPONSABLE	DOCUMENTOS DE REFERENCIA
INICIO			
1.Depurar, clasificar y ordenar los documentos.	1. Depurar, clasificar y ordena los documentos de acuerdo a serie, subseries, expedientes y/o unidad documental en el Archivo de Gestión, semanalmente.	Funcionario designado de archivos de gestión	ADOM001 ADOF023 ADOr023
2. Foliar los Documentos	2. Foliar los documentos semestralmente.	Funcionario designado de archivos de gestión	ADOM001
3. Utilizar elementos y Unidades de Conservación y Archiva	3. Utiliza unidades de conservación y archiva según códigos establecidos en las Tablas de Retención Documental ya sea en forma física y/o electrónica según corresponda.	Funcionario designado de archivos de gestión	ADOM001 ADOF021 ADOI001
A			
4. Registrar los Documentos.	4. Registra documentos en el inventario único documental semestralmente.	Funcionario designado de archivos de gestión	ADOM001 ADOF021 ADOI001
5. Entrega del inventario documental al terminar contrato.	5. Entrega el inventario único documental al termino del contrato o cambio de oficina al Jefe de la dependencia y envía copia electrónica al archivo central.	Funcionario designado de archivos de gestión	ADOM001 ATHF133 Correo electrónico
6. Revisar anualmente los Documentos.	6. Revisa anualmente los documentos de acuerdo a las Tablas de Retención Documental.	Funcionario designado de archivos de gestión	ADOM001 ADOF023
¿Cumplió el tiempo de retención documental?	PUNTO DE CONTROL		
Si			
A			
7. Revisar y transferir los documentos al Archivo Central.	7. Revisa y transfiere los documentos al Archivo Central a través del inventario único documental.	Funcionario designado de archivos de gestión	ADOF021 ADOr026
8. Archivar y controlar registros.	8. Archiva inventarios documentales y controla registros.	Funcionario designado de archivos de gestión	ADOr021 ADOP03 ADOP04 ACAP02
FIN			

Figura No. 63, diagrama de manejo de información de la UDEC; UDEC 2018

Esta información relevante, respecto a los procesos de control interno, de la universidad, son documentos que se pudieron encontrar y descargar, por medio de la herramienta Foca y la información disponible en el siguiente enlace https://www.ucundinamarca.edu.co/index.php/control-interno.

Bajo los conceptos, utilizados por el ***Consejo Nacional de Rectores,*** en lo que respecta al *Catálogo de Riesgos de Sistemas de Información,* que provee información vital, sobre la *Identificación de amenazas, vulnerabilidades y riesgos* se evaluaran en este estudio según los siguientes criterios:

1. HARDWARE: Los componentes físicos del sistema: servidores.

2. SOFTWARE: bases de datos, herramientas de desarrollo y licenciamiento.

3. COMUNICACIONES: Los dispositivos y enlaces que conforma la Red.

4. SEGURIDAD: Elementos de protección y seguridad de la información, accesos y sistema

5. PERSONAL: El capital humano involucrado en el desarrollo, puesta en producción, y mantenimiento del Sistema.

6. PROVEEDORES: Los contratos suscritos para el outsourcing parcial o total del sistema.

7. GESTIÓN DEL PROYECTO: Administración del Proyecto

8. CONTINUIDAD DE PROCESOS DEL NEGOCIO: Aspectos que garantizan la continuidad del servicio

9. DOCUMENTOS y DATOS: Documentación y resguardo de la información del proyecto

10. AUDITORÍA DEL PROYECTO: Seguimiento y evaluación del control interno en cuanto a los riesgos

11. MEJORA CONTINUA: Planes de mejoramiento

Para ver con mayor claridad remitirse a los archivos Excel adjuntos a este proyecto.

CATÁLOGO DE RIESGOS DE SISTEMAS DE INFORMACIÓN					
AMENAZAS			Bajo	Medio	Alto
1	HARDWARE	Adquirir y mantener infraestructura tecnológica			
		Daños en equipos de cómputo, servidores y otros elementos informáticos			
		Ausencia de soporte técnico			
		La infraestructura física y equipos			
		Daño en los equipos			
		Perdida por robo/hurto de información de orden institucional			
2	SOFTWARE	Gestión y desempeño de la Aplicación			
		Protección de los datos de prueba			
		Daños en el sotware			
		Bitácoras de los eventos			
		Procedimientos para la administración de la Información			
		Fallas en la administración de excepciones del proyecto			
		Ausencia de soporte técnico para la Base de Datos del Proyecto			
		Calidad baja en los productos entregados			
		Perdida de información			
		El sistema carece de usabilidad en las interfaces			
3	COMUNICACIONES	No cumplimiento de las directrices de manejo de información			
		Interrupción del acceso a la red Internet			
		Fallas en el acceso a recursos compartidos dentro de la institución			
		Intromisión por parte de personas y/o elementos inoportunos a la red de datos interna de la institución			
		Débil interacción del Sistema con otros sistemas			
		Pruebas de aceptación para la integración del sistema incompletas			
4	SEGURIDAD	Derechos de acceso del usuario			
		No contar con las copias de seguridad oportunas.			
		No implementar copias de seguridad en forma periódica.			
5	PERSONAL	Educar y entrenar a los usuarios			
		Administrar Proyectos			
		Proyecto mal administrado por fallas en el Grupo de Administración de Proyectos			
		Proceso de comunicación incipiente			
6	PROVEEDORES	Software desarrollado por outsourcing			
		Entregables del proyecto no cumplen expectativas de clientes			
		Plazos definidos para el desarrollo del sistema son cortos o irreales.			
		Plazos establecidos para las pruebas del sistema son cortos o irreales.			
		Plazos de revisión del sistema son cortos e irreales.			
		Incumplimiento en los trabajos solicitados			
7	GESTIÓN DEL PROYECTO	Impactos en el cliente no identificados ni satisfechos			
		Proyecto con deficiente desarrollo y control			
		Proyecto excedido en alcance y costos			
		Proyecto con problemas de comunicación.			
		Administrar la configuración			
		Cierre de proyecto realizado de manera no efectiva			
		Pruebas de Aceptación inadecuadas.			
		Plazos de revisión del sistema son cortos e irreales.			
		No apropiación de los usuarios al proyecto			
		Se inicia la ejecución de contratos sin el cumplimiento de requisitos de ejecución			
		Falta compromiso por parte de los responsables y/o fiscalizadores durante la ejecución del contrato.			
		Se inicia la ejecución de contratos sin el cumplimiento de requisitos de ejecución			
		Incumplimiento de términos			
		Apoyo mínimo del Director de la oficina en la toma de deciciones			
		Aceptación del sistema			
8	CONTINUIDAD DE PROCESOS DEL NEGOCIO	Garantizar la continuidad del servicio			
		No contar con las copias de seguridad oportunas			
		No implementar copias de seguridad en forma periódica			
		Dificultad en la contratación de profesionales que apoyen diferentes áreas del Proyecto			
		falta de continuidad de la vigilancia de los factores de riesgo.			
		Compromiso en el cumplimiento de las medidas de prevención			
9	DOCUMENTOS Y DATOS	Descontrol en el recibo de comunicaciones oficiales del Proyecto			
		Perdida y deterioro documentos			
		Sustracción de documentos			
		Desorganización de la información			
		Proyectos sin la debida documentación			
10	AUDITORIA DEL PROYECTO	Baja cobertura en el desarrollo de la evaluación independiente			
		No se tienen en cuenta las recomendaciones generadas de los procesos de Auditoria			
		No seguimiento de los riesgos			
		Baja calificación en el sistema de Control Interno			
11	MEJORA CONTINUA	No mantenimiento del Sistema de Expdiente Electrónico			
		No ejecución de Planes de Mejoramiento			
		No llevar a cabo procesos de autoevaluación			
		No suscribir oportunamente los acuerdos de gestión en el nivel gerencial.			

Figura No. 64, Catalogo de riesgos en el sistema de información*; Daniel Rodríguez 2018*

- Para ver con mayor detalle, dirigirse al documento Excel, llamado valoración de activos.

En datos cuantitativos, se muestra la realidad de la institución educativa Universidad de Cundinamarca, respecto al nivel de amenazas a las cuales está expuesta.

Amenaza	Total
Baja	21
Media	24
Alta	16
Total	61

Figura No. 65, Resultado de los riesgos en el sistema de información de la UDEC*; 2018-Autor*

Al identificar y tener claridad en los procesos que tienen falencias y los que se encuentran en un buen estado, se puede llegar a prever lo previsible, que es el objetivo de cualquier análisis de riesgos y vulnerabilidades. Dado a que el riesgo es inminente y puede suceder en cualquier circunstancia.

2.3.1 PRUEBAS

A continuación, se agregan como pruebas algunas de las vulnerabilidades descubiertas en el transcurso de esta investigación, queriendo recalcar la importancia de este proyecto y los efectos negativos que puede llegar a tener estas en la institución se plantearán situaciones hipotéticas. Así mismo estas estarán organizadas según la importancia que el investigador considera en cada una de ellas.

En cuanto a la estructura de la organización se generó un script en lenguaje bash, que iba realizando peticiones al servidor, analizando el segmento de red conocido como 200.14.47.1 – 200.14.47.255. Por el que se pudo encontrar una serie de hosts activos que brindan apoyo y complemento al sistema informatico de la institucion.

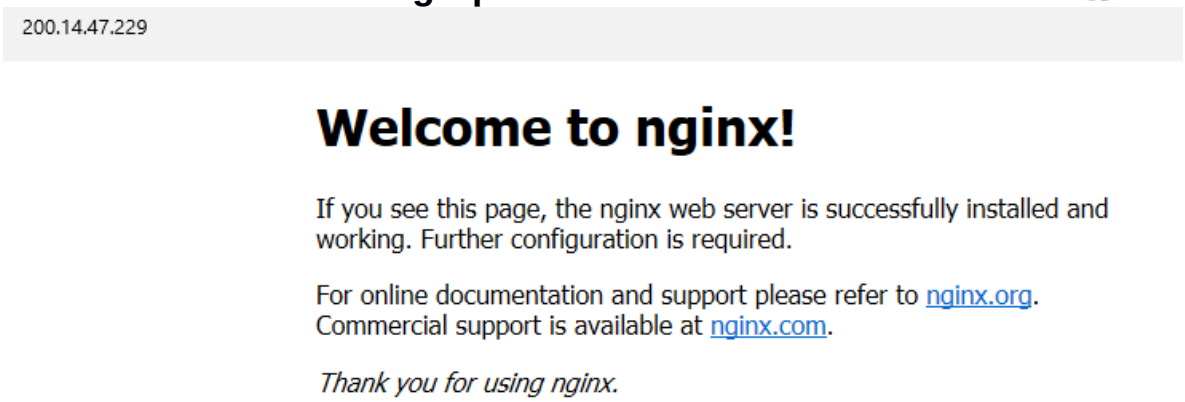


FIGURA No. 66, 200.14.47.229 APLICACIÓN NGINX UTILIZADA EN UDEC. 2018

Consultando la web oficial de Nginx, sabemos que "El sitio web al que intenta acceder usa NGINX como su servidor web. ¿Qué es NGINX? NGINX es un servidor web de código abierto utilizado por más de 287 millones de sitios web y más del 64% de los mejores 10.000 sitios web del mundo. NGINX Plus, construido sobre NGINX de código abierto, agrega capacidades de nivel empresarial como el equilibrio de carga con comprobaciones de estado de aplicaciones, caché de contenido, controles de seguridad y capacidades de gestión y monitoreo de aplicaciones."

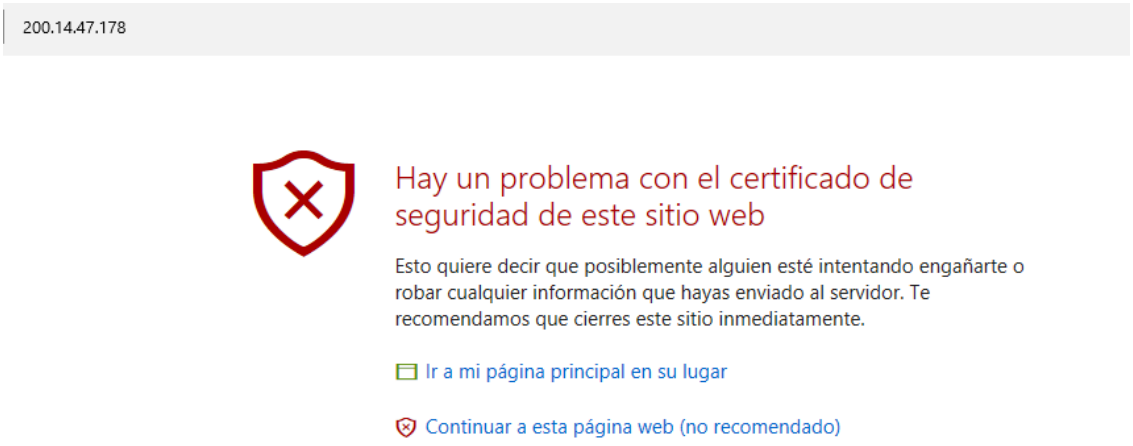


FIGURA No. 67, 200.14.47.178 CERTIFICADO DE SEGURIDAD. 2018

En la direccion IP 200.14.47.178, se encuentran los certificados de seguridad de la Universidad de Cundinamarca. Este host es un servicio que se compra el cual se encarga de proporcionar el https:// del inicio de la pagina, asi como se menciono.

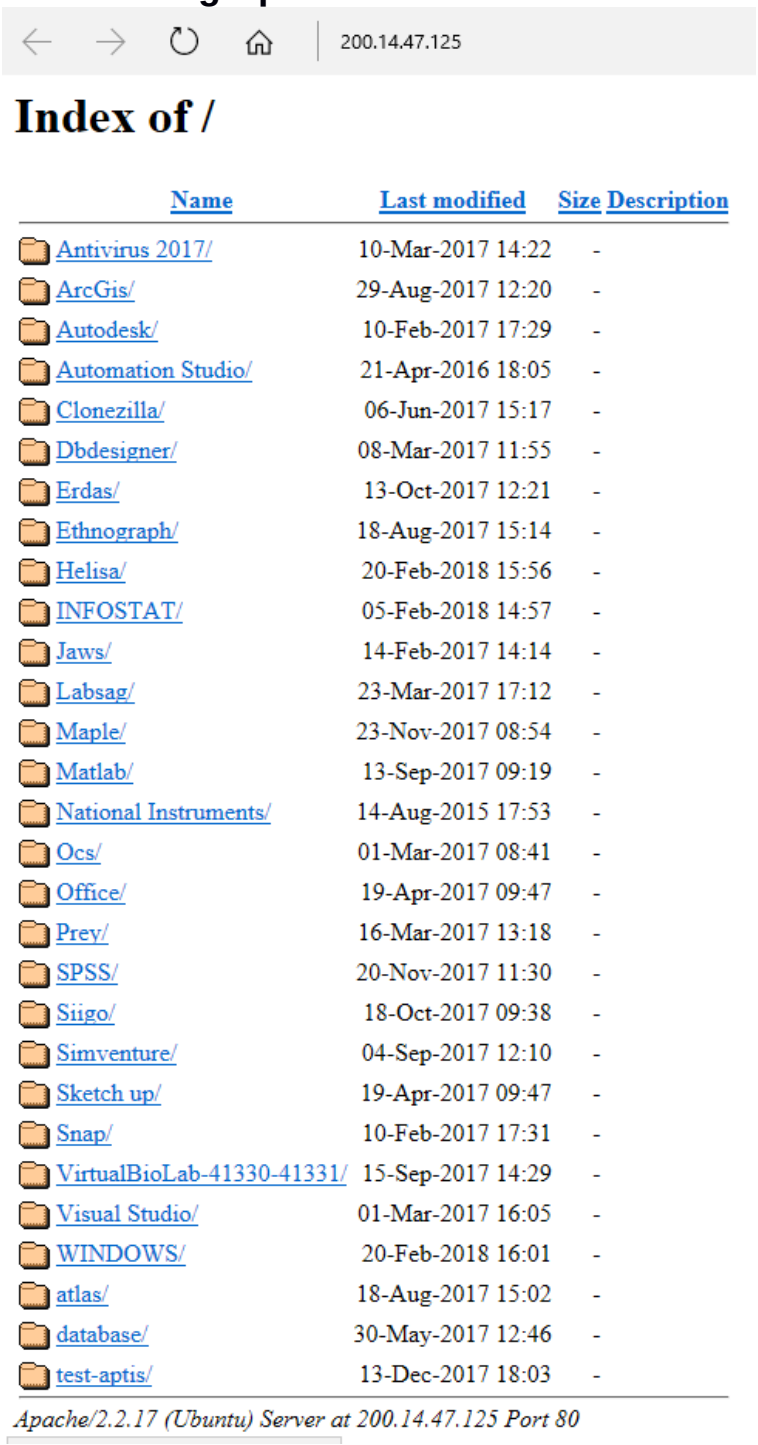


Figura No. 68, 200.14.47.125 software a disponiblidad de consulta y descarga. 2018

El servidor de descarga FTP de los software utilizados por los estamentos de la universidad. Donde no solo se encuentran los distintos software sino que tambien los manuales de instalacion y algunas de las licencias que la universidad compra

muchas veces en grandes sumas de dinero. Lo importante he interesante es que para acceder a este servidor no se requiere una autenticacion.

Figura No. 69, 200.14.47.117 servidor xampp. 2018

Se ve el servidor utilizado para la transferencia de datos y como gestor del codigo php, perl y sql. El cual esta corriendo en la IP 200.14.47.117, conocer el servidor que usan para administrar el sistema permite muchas ventajas, asi como facilidades para encontrar vulneravilidadedes segun la versión que se este manejando.

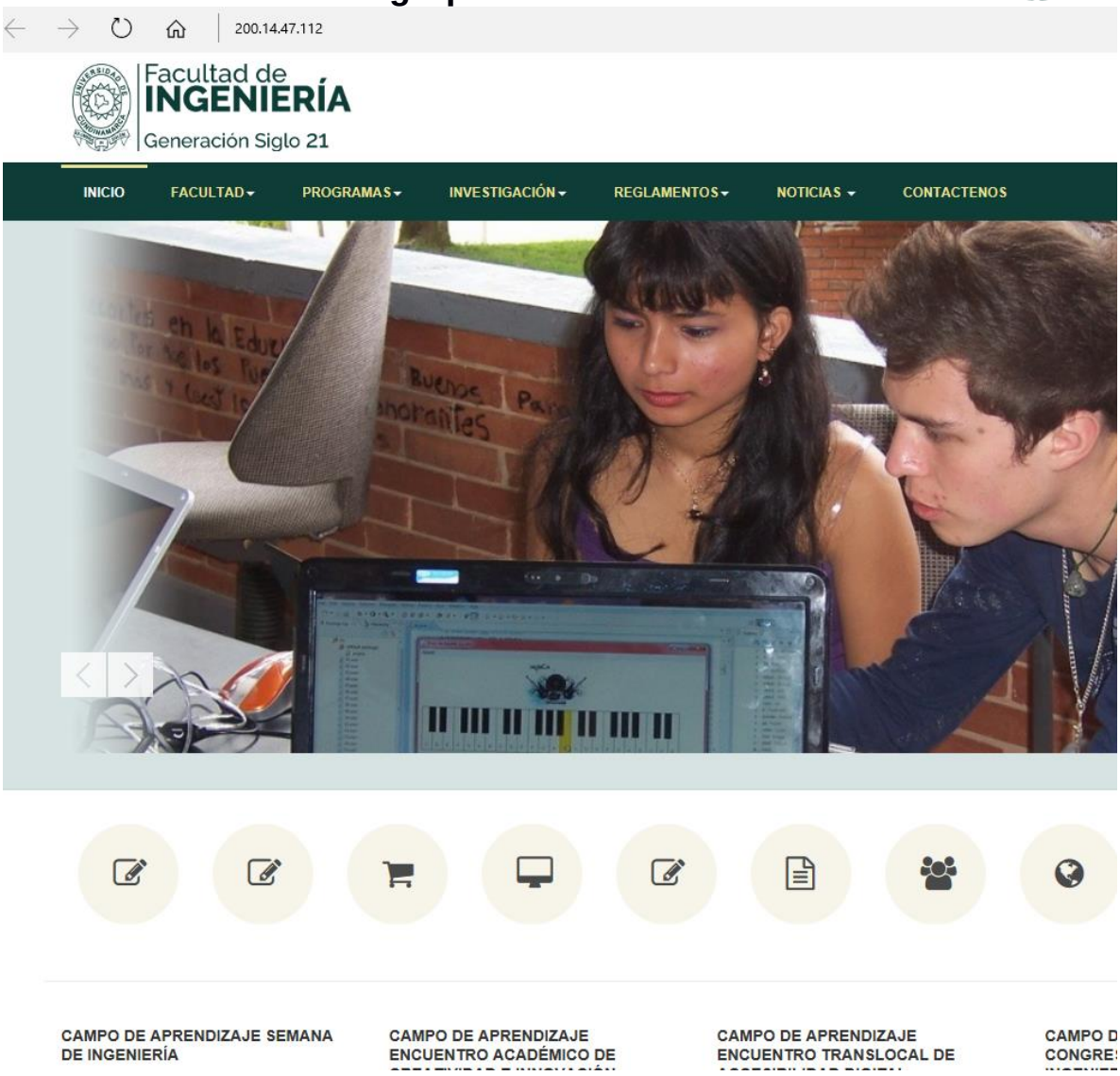


FIGURA No. 70, 200.14.47.112 FACULTAD DE INGENIERIA. 2018

La facultad de ingenieria tiene su propio host, al contrario de las demas facultades que solo cuentan con una pagina del dominio principal. Es decir para la universidad la facultad de ingenieria se encuenta a un mismo nivel de la biblioteca y el aula virtual. Esto debe ser por que los estudiantes, docentes y funcionarios de esta facultad tienen bastante contacto con el sistema virtual.

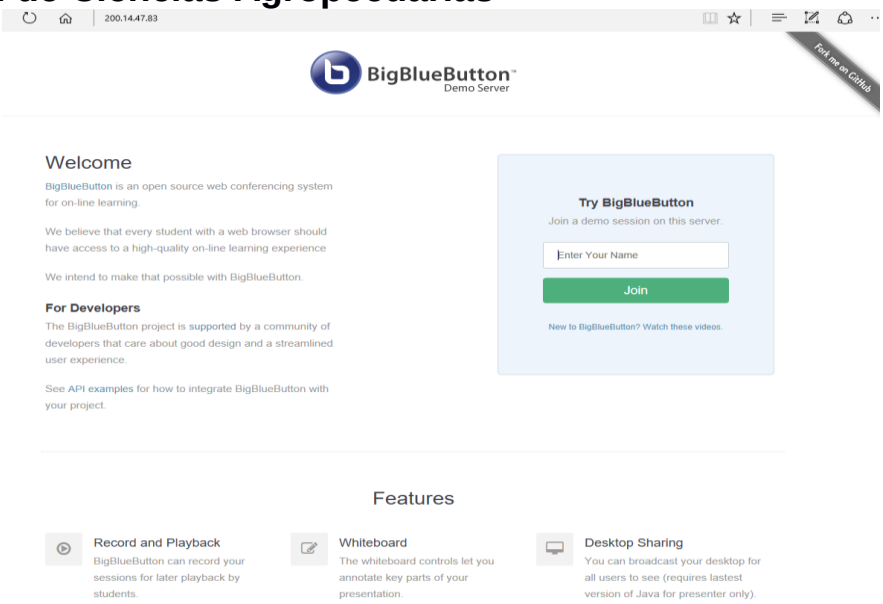


FIGURA No. 71, 200.14.47.83 BIGBLUEBUTTON. 2018

Bigbluebutton es definido en su pagina principal como: *"Un sistema de conferencia web de código abierto. Está basado en el sistema operativo GNU / Linux y se ejecuta en Ubuntu 16.04. Además de varios servicios de conferencia web, tiene integraciones para muchos de los principales sistemas de gestión de contenido y aprendizaje"*

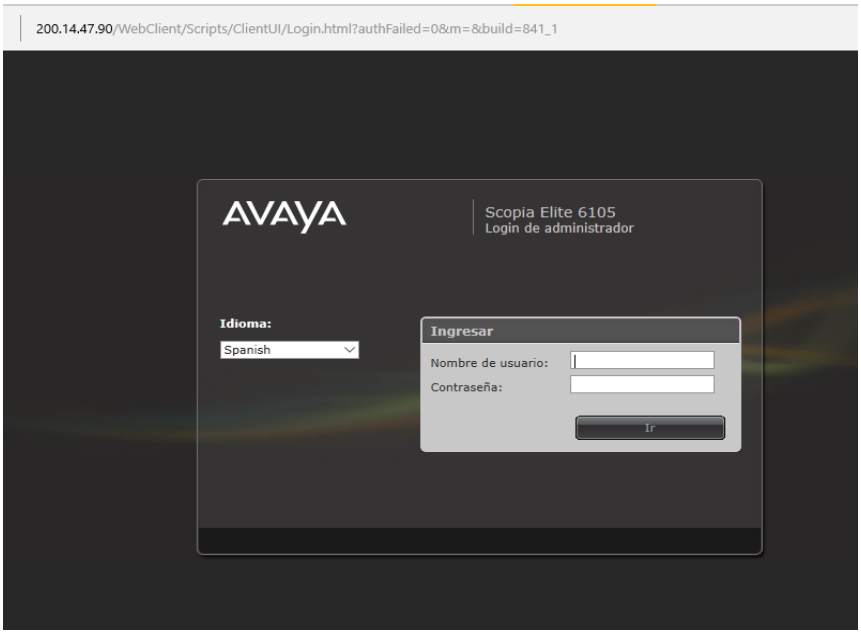


FIGURA No. 72, 200.14.47.90 AVAYA. 2018

Avaya se encuentra en el host 200.14.47.90. Este software presta servicios de comunicación, tal como lo indica en su pagina oficial "Avaya presenta el portafolio más completo de software y servicios para centros de contacto multicontacto y

comunicaciones unificadas en las instalaciones, en la nube o de manera híbrida”

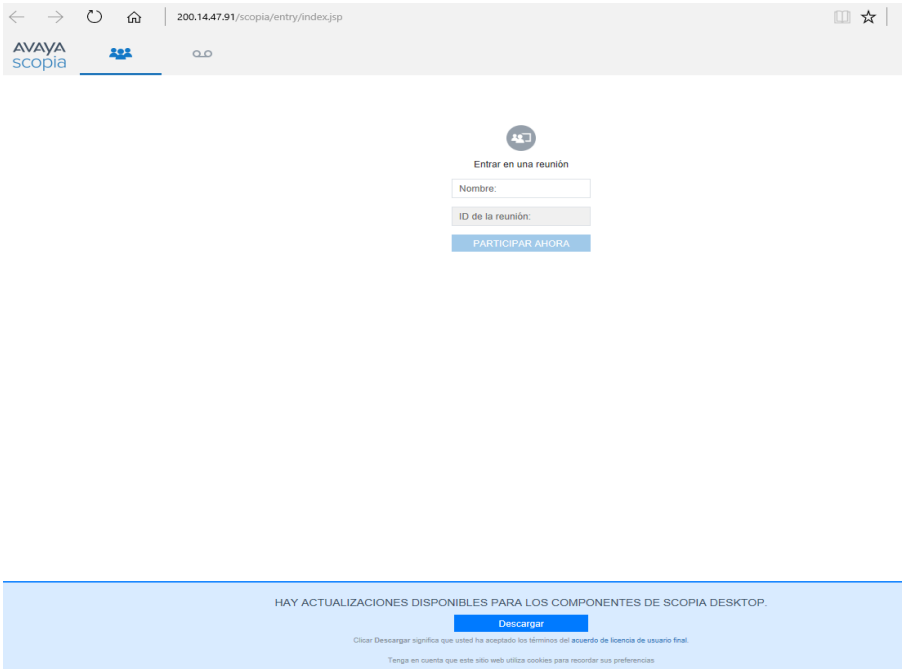


FIGURA No. 73, 200.14.47.91 AVAYA SCOPIA. 2018

Avaya Scopia, es un complemento del software Avaya que ademas de permitir una comunicación efectiva, permite realizar videoconferencias, apoyados en las ultimas tendencias de las tecnologias en comunicación.

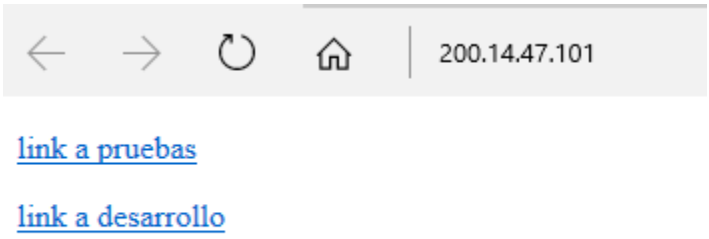


FIGURA No. 74, 200.14.47.101 HOST DE PRUEBAS. 2018

Este host, es en el que aparentemente el administrador del sistema genera sus pruebas. Por decirlo de cierta manera es como un servidor de producción interna. El cual debería estar con un sistema de autenticación y/o de cifrado.

FIGURA No. 75, 200.14.47.102 SNIES. 2018

Este es el portal del ministerio de educacion y la universidad de Cundinamarca, en la paguina oficial del SNIES se puede encontrar la siguiente descripción “El Sistema Nacional de Información de la Educación Superior (SNIES), es un sistema de información que ha sido creado para responder a las necesidades de información de la educación superior en Colombia. En este sistema se recopila y organiza la información relevante sobre la educación superior que permite hacer planeación, monitoreo, evaluación, asesoría, inspección y vigilancia del sector.”

FIGURA No. 76, 200.14.47.107 Autenticacion realizada por XAMPP. 2018

En el host 200.14.17.107, se encuentra la intranet. Y tal como se puede observar,

esta pide un usuario y contraseña. Al introducir datos erroneos, se informa que esta autenticacion se realiza por XAMPP lo cual sugiere que este sitio web tiene bastante desarrollo en php.

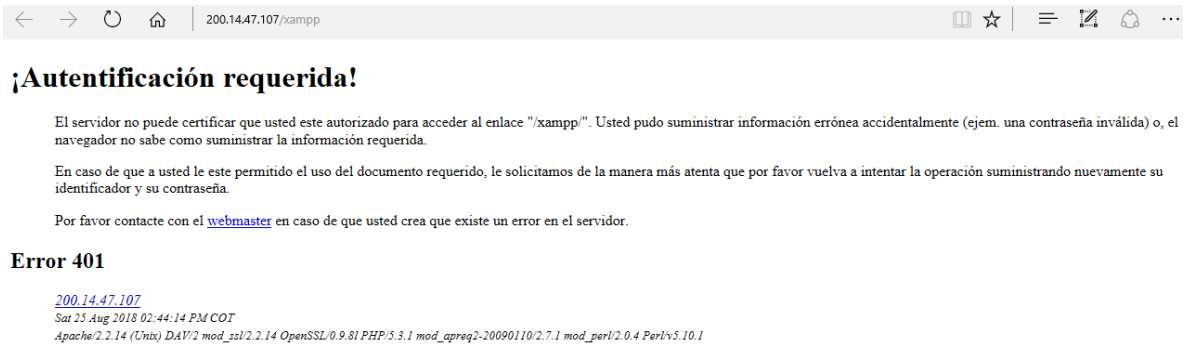


FIGURA No. 77, 200.14.47.107 Error Intranet. 2018

Simplemente al cancelar la autenticacion, el servidor nos muestra un error, que proporciona datos relevantes sobre los servicios utilizados por el administrador. (Apache/2.2.14(Unix) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.81 PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1) aHR0cCUzQSUyRiUyRnZ1bG5lcmFiaWxpZGFkZXMtdWRlYy5taXByb3BpYS5jb20lMkY=

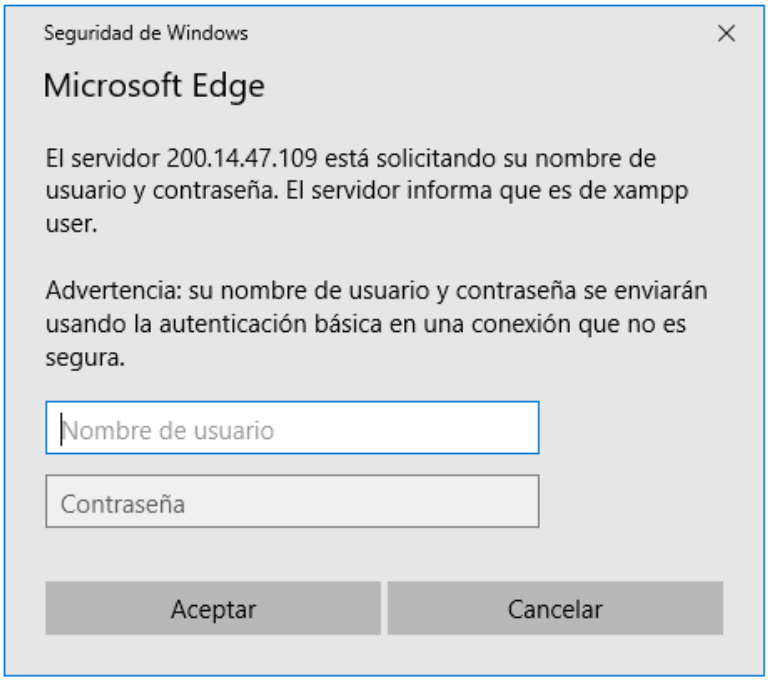
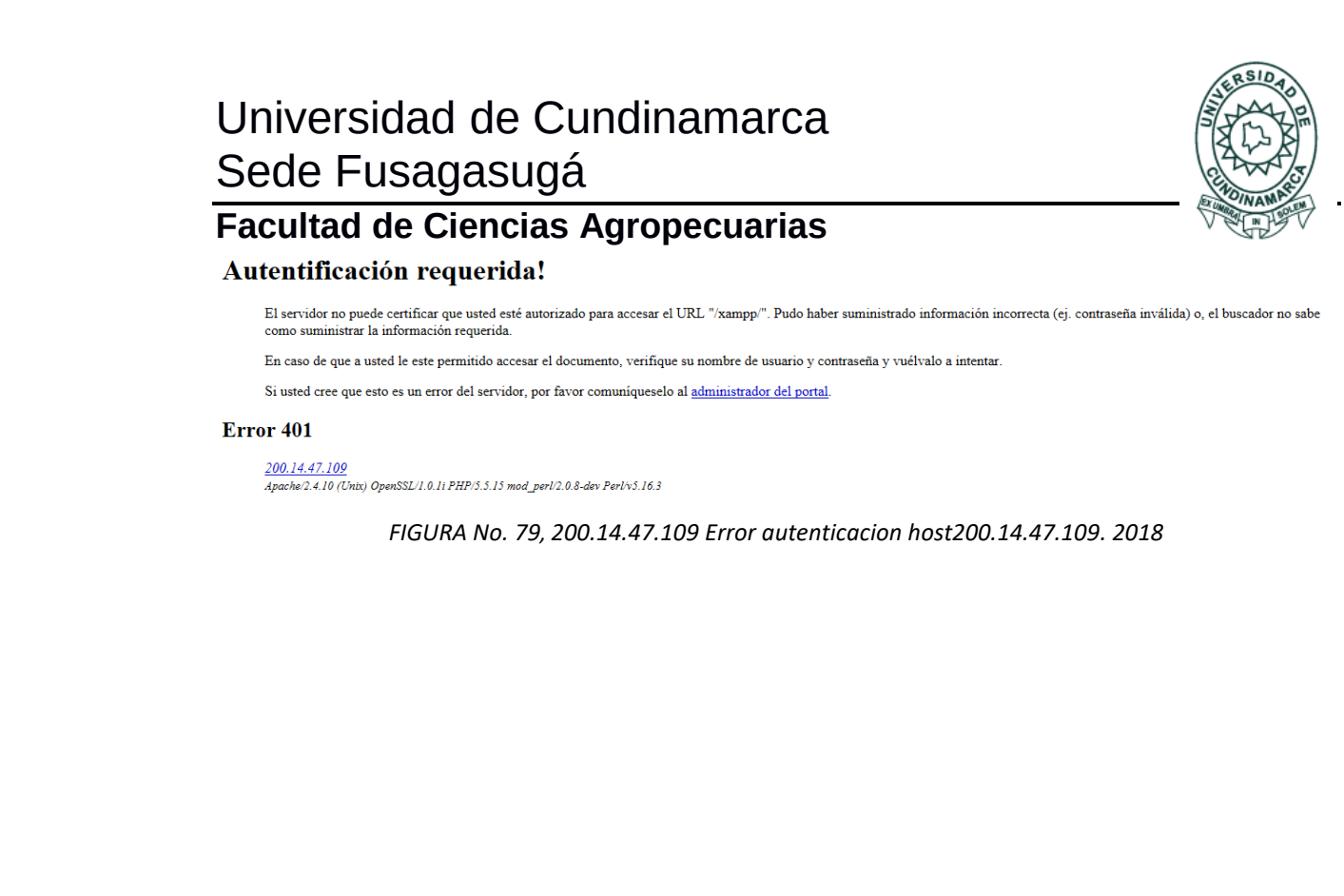


FIGURA No. 78, 200.14.47.109 Atenticacion XAMPP. 2018



Autentificación requerida!

El servidor no puede certificar que usted esté autorizado para accesar el URL "/xampp/". Pudo haber suministrado información incorrecta (ej. contraseña inválida) o, el buscador no sabe como suministrar la información requerida.

En caso de que a usted le este permitido accesar el documento, verifique su nombre de usuario y contraseña y vuélvalo a intentar.

Si usted cree que esto es un error del servidor, por favor comuníqueselo al administrador del portal.

Error 401

200.14.47.109
Apache/2.4.10 (Unix) OpenSSL/1.0.1i PHP/5.5.15 mod_perl/2.0.8-dev Perl/v5.16.3

FIGURA No. 79, 200.14.47.109 Error autenticacion host200.14.47.109. 2018

3. RESULTADOS Y ANEXOS

3.1 ACTIVOS DE INFORMACIÓN

Los activos presentes en la Universidad de Cundinamarca, son identificados y clasificados tomando como base la clasificación de activos puesta a disposición en el marco teórico.

ID	TIPO	NOMBRE DEL ACTIVO	CANTIDAD
1	SW	Portal universitario	2
2	SW	Intranet	1
3	SW	Ubuntu	1
4	SW	Windows	1
5	SW	Apache	1
6	SW	BD	1
7	SW	Licencia de aplicaciones	1
8	SW	Php	1
9	SW	Perl	1
10	SW	Html5	1
11	SW	css	1
12	SW	Avaya	1
13	SW	SNIES	1
14	SW	Servidor FTP	1
15	SW	Webmin	1
16	SW	Adobe flash	1
17	SW	JavaScript	1
18	SW	Xampp	1
19	SW	OpenSSL	1
20	SW	NGINX	1
21	SW	Bigbluebutton	1
22	HW	Servidores	4
23	HW	Ordenadores	100+
24	SI	Plataforma	1
25	SI	Aula virtual	1
26	S	Correo electrónico	1
27	S	SGC	1
28	Media	Biblioteca	1
29	Media	Oficina de Archivo	1
30	AUX	Telecomunicaciones	1
31	COM	Red Ucundinamarca	1
32	COM	Red Almamater	1
33	AUX	Suiches	30+
34	P	Oficina del aula virtual	1

35	P	Oficina de Apoyo y soporte informático	1
36	P	Dirección de Sistemas y Tecnología	1
37	P	Asistencia técnica	1
38	P	Mantenimiento	1
39	L	Bloque A	1
40	L	Bloque F	1
41	L	Bloque Administrativo	1
42	D	Resoluciones	
43	D	Actas	
44	D	Registros	
45	D	Documentos de funcionamiento interno	
46	D	Documentos de salida al público.	
47	D	Datos de configuración	
48	D	Datos de personales de clientes	
49	D	Copias de respaldo	

Para ver en detalle el inventario de activos encontrados a la fecha, consultar los archivos Excel.

3.2 MAPAS

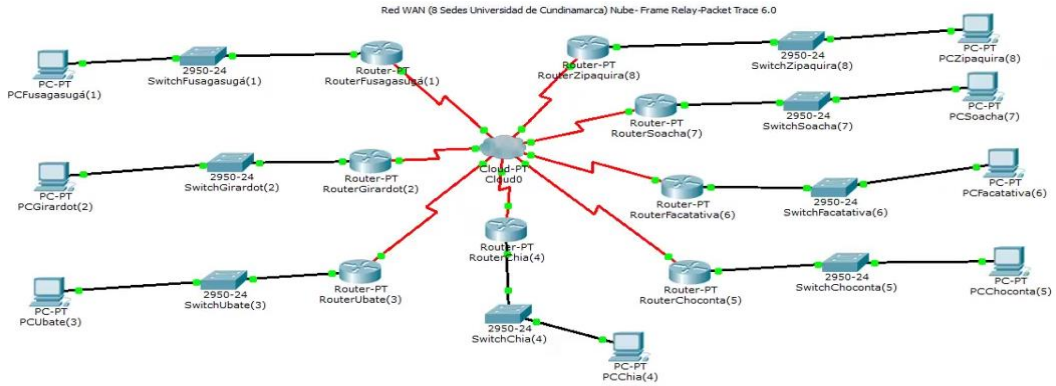


Figura No. 80,Mapa de la red Wan (8 sedes Universidad de Cundinamarca); Julián Prieto 2013

- Para ver con mayor detalle, los mapas topológicos, que son mostrados a continuación, remitirse a la carpeta productos finales, donde se encontrarán estos en varios formatos.

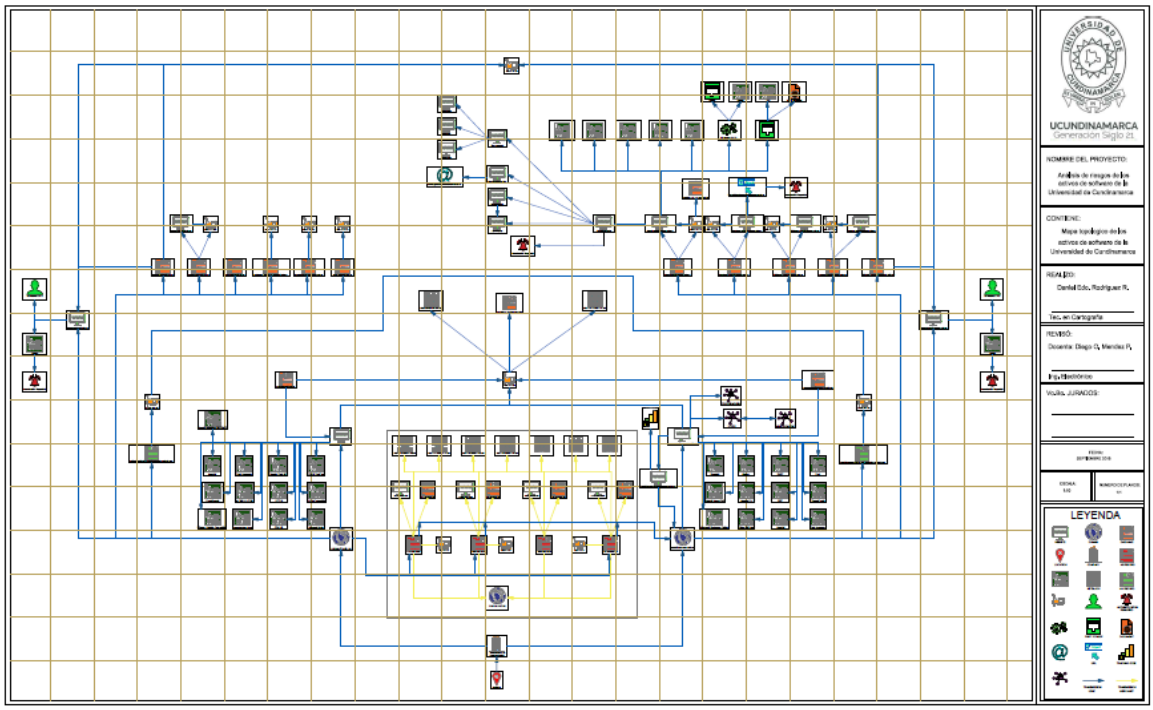


Figura No. 81, Mapa topológico de la Universidad de Cundinamarca; Daniel Rodríguez 2018

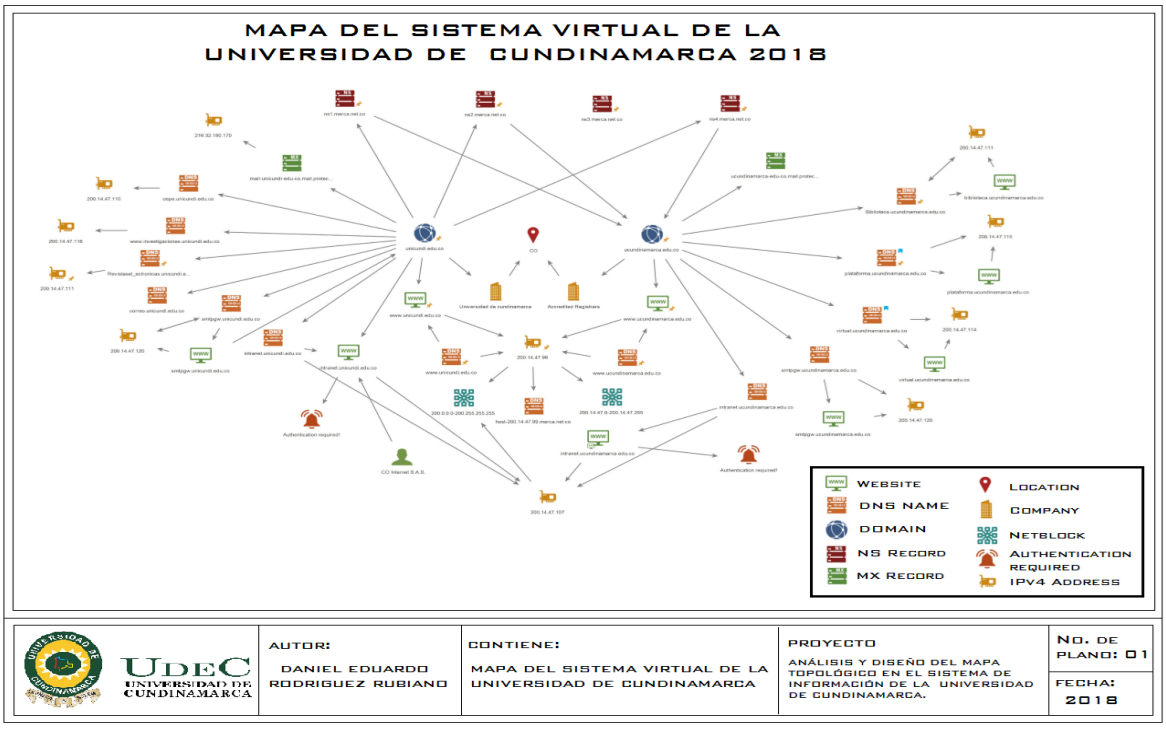


Figura No. 82, Mapa del sistema virtual de la UDEC; Daniel Rodríguez 2018

4. CONCLUSIONES Y RECOMENDACIONES

De acuerdo al trabajo realizado se concluye que la Universidad de Cundinamarca tiene un sistema informático considerablemente amplio. Por tal razón son bastantes los riesgos a los que esta se encuentra sometida, además de estar obligada a reportar información a otras entidades y utilizar servicios externos a la institución. Lo que de una manera indirecta extiende el riesgo un segundo y tercer nivel. Además de tener una gran cantidad de clientes activos e inactivos a los cuales muchas veces se deja en un segundo plano en materia de seguridad. Bajo estos factores primordiales se concluye:

- La institución educativa se encuentra en un riesgo medio, como se observa en la figura 65. En los resultados del catálogo de riesgos del sistema de información de la UDEC.
- La Universidad de Cundinamarca tiene deficiencias en los productos y servicios que dispone al público. Por tal razón se recomienda realizar prácticas de seguridad en un espacio ajeno al sistema informático, antes de sacar los productos al público.
- La Universidad de Cundinamarca debe plantearse la creación de una metodología estratégica para la toma de decisiones relevantes. Que incremente la integridad y eficacia de sus sistemas. Generando nuevas políticas de seguridad.
- La institución cuenta con políticas de seguridad bajas en cuanto al personal humano que está realmente tiene. Se recomienda modificar los ingresos dado a que geográficamente la universidad tiene sus sedes en lugares relativamente pequeños, la mayoría de la población ha llegado a tener contacto con ella. La universidad debe tomar mayores precauciones con los clientes y trabajadores que se encontraron alguna vez en contacto con su sistema informático.
- Se debe implementar un diseño del mapa de la topología física de cada una de las sedes de la institución educativa UdeC.

La investigación realizada deja datos detallados en este informe bajo los siguientes aspectos:

- La clasificación de activos de software, logro encontrar y reportar 39 (Treinta y nueve) activos de la Universidad de Cundinamarca. Los cuales fueron identificados desde un rol externo a la institución educativa.

- Los espacios de contenido fueron analizados por medio de 55 Herramientas utilizadas en la fase de reconocimiento y exploración, además de apoyarse en los conceptos teóricos del *Consejo Nacional De Rectores* se analizaron 63 riesgos en el sistema de información de la Universidad de Cundinamarca. Y se encontraron 8 vulnerabilidades del top 10 de la OWASP.

- Los espacios de contenido fueron representados en (2) dos mapas y basado en el análisis de riesgos se genera un tercer mapa, que reúne a los anteriores y agrega los posibles vectores de ataque.

Con esto se busca apoyar a la Universidad de Cundinamarca en su proceso de calidad, acorde al objetivo de la misma, leer más en:

https://www.ucundinamarca.edu.co/index.php/noticias-ucundinamarca/84-institucional/745-vamos-por-la-iso-90001-2015

5. BIBLIOGRAFÍA

ZUCCARDI GIOVANNI & GUTIÉRREZ JUAN. (2006). *SEGURIDAD INFORMATICA.*

ADMINISTRATIVA, D. (2012). *MAGERIT – VERSIÓN 3.0. METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN*

BETANCOURT JUAN & CARDONA CATALINA. (2013). *DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL GRUPO EMPRESARIAL LA OFRENDA.* PEREIRA: UNIVERSIDAD TECNOLOGICA DE PEREIRA.

C, A. (2016). *PENTESTING CON FOCA.* MADRID: 0XWORD.

CARLOS, M. (s.f.). *SEGURIDAD INFORMATICA VS SEGURIDAD DE LA INFORMACION*. Obtenido de SEGURIDAD DE LA INFORMACION, REDES Y TELECOMUNICACIONES.

CUENCA, D. (2012). *ANÁLISIS DE RIESGOS DINÁMICOS EN.* MADRID: UNIVERSIDAD COMPLUTENSE DE MADRID (UCM).

DANIEL, A. L. (2005). *SEGURIDAD EN INFORMATICA (AUDITORIA DE SISTEMAS).* MEXICO, D.F.: UNIVERSIDAD IBEROAMERICANA.

ERICKA, Y. (2015). *ANALISIS DE LAS HERRAMIENTAS PARA EL PROCESO DE AUDITORIA DE SEGURIDAD INFORMATICA UTILIZANDO KALI LINUX.* MADRID: UNIVERSIDAD POLITECNICA DE MADRID.

FERNANDO, B. (2014). *LABORATORIO DE SEGURIDAD INFORMATICA CON KALI LINUX.* UNIVERSIDAD DE VALLADOLID.

FERNANDO, H. (2007). *PROPUESTA DE SEGURIDAD DE LA INFORMACION: CASO "SYSTEMATICS DE MEXICO,S.A".* MEXICO D.C.: INSTITUTO POLITECNICO NACIONAL.

GUSTAVO, M. (2009). *METODOLOGIA DE IMPLANTACION DE UN SGSI EN UN GRUPO EMPRESARIAL JERARQUICO.* URUGUAY: UNIVERSIDAD DE LA REPUBLICA.

J, C. (2014). *ANALISIS DE RIESGOS DE LA SEGURIDAD DE LA INFORMACION PARA LA INSTITUCION UNIVERSITARIA COLEGIO MAYOR DEL CAUCA.* INSTITUCION UNIVERSITARIA COLEGIO MAYOR DEL CAUCA.

JOHANA, S. (2012). *ANÁLISIS DE RIESGOS .* BOGOTA D.C.

LÓPEZ JAVIER & RODRÍGUEZ MAURICIO. (2015). *ASEGURAMIENTO DE LOS SISTEMAS COMPUTACIONALES DE LA EMPRESA SITIOSDIMA.NET.* BOGOTA D.C.: UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD .

MANUEL, B. (2016). *OPERACIONES MILITARES EN EL CIBERESPACIO. CONJUNTO DE CIBERDEFENSA.* ESPAÑA: CYBERCAMP2016.

MIGUEL, S. (s.f.). *SEGURIDAD EN REDES Y SEGURIDAD DE LA INFORMACIÓN .* Czech Republic : České vysoké učení technické v Praze .

MORA, D. E. (2013). *RIESGOS, AMENAZAS Y VULNERABILIDADES DE LOS SISTEMAS DE INFORMACIÓN GEOGRÁFICA.* BOGOTÁ: UNIVERSIDAD CATÓLICA DE COLOMBIA