REVISIÓN TÉCNICA DE LA PLATAFORMA AULAS VIRTUALES DE LA UNIVERSIDAD ECCI MEDIANTE EL USO DE HERRAMIENTAS OSINT

MILLER EDUARDO HURTADO ESPITIA

DANA VALENTINA LOZADA CORTES

UNIVERSIDAD ECCI

Programa Tecnología en Desarrollo Informático

Proyecto de Grado

Bogotá D.C

2020

REVISIÓN TÉCNICA DE LA PLATAFORMA AULAS VIRTUALES DE LA UNIVERSIDAD ECCI MEDIANTE EL USO DE HERRAMIENTAS OSINT

Presentado por:

MILLER EDUARDO HURTADO ESPITIA

DANA VALENTINA LOZADA CORTES

Presentado a:

Msc. Ing. ANA ROCIO LEON LUGO – Director Proyecto

M. Ed. Ing. OSCAR ALBERTO ZAMBRANO OSPINA – Asesor Metodológico

UNIVERSIDAD ECCI

Programa Tecnología en Desarrollo Informático

Proyecto de Grado

Bogotá D.C

2020

Dedicatoria

Este proyecto está dedicado principalmente a Dios porque nos dio la vida, nos llenó de bendiciones, con su amor y su bondad nos dio la fuerza para seguir adelante en cada uno de esos momentos cuando sentíamos que cada esfuerzo no valía la pena, segundo a nuestros padres a quienes les debemos toda la vida, nos educaron, nos dieron los valores y principios los cuales nos han ayudado a salir adelante y tomar el mejor camino de vida, ellos siempre han sido las personas que han puesto todo su esfuerzo para que en estos momentos tengamos todo lo que tenemos, nuestros padres y hermanos son los que siempre han estado ahí apoyándonos, ellos han estado en los momentos más difíciles, son los que nos han dado los mejores consejos de vida y superación, nuestros hermanos son nuestros mejores amigos y siempre nos han alegrado nuestro existir, así nos molesten sabemos que siempre vamos a contar con ellos para lo que sea, a nuestros amigos con los que hemos paso momentos increíbles, finalmente a nuestros maestros que son los que nos han brindado sus conocimientos y su tiempo para conocer nuevas cosas cada día.

Agradecimientos

Queremos agradecer primeramente a Dios por habernos dado la vida, por todas las bendiciones que nos han llegado hasta este momento, por habernos puesto en el camino correcto y este proyecto en el que estuvimos trabajando, gracias porque tus caminos son perfectos y sabemos que esto no se hubiera podido lograr sin ti, gracias por habernos puestos todas esas personas que nos acompañaron durante esta lucha, gracias porque tú eres perfecto y tu palabra también y sabemos que tú no nos ibas a dejar, por el contrario nos ayudas para que todo salga según tu voluntad, gracias padre amado por habernos dado tu amor y comprensión.

Le queremos dar las gracias a la profesora Ana Rocío León y al profesor Oscar Zambrano por acompañarnos en todo el proceso, ya que, sin el apoyo de ellos no hubiese sido posible la elaboración de todo este proyecto, por estar ahí para darnos asesoría y ayuda en todo lo que hizo falta. Igualmente queremos agradecer a nuestros padres y familiares que nos han apoyado en el proceso de estudio y que nos han acompañado desde que éramos unos niños, principalmente gracias a ellos es que podemos estudiar y descubrir nuevas tecnologías cada día, a todos ellos muchas gracias por el apoyo brindado.

Abstract

The purpose of this research project was to carry out a technical audit on the Virtual Classrooms platform of the ECCI University, using different methods to obtain information such as social engineering, through internet cafes but the most important one using OSINT tools (Open Source Intelligence, which refers to any declassified information that can be collected in public access sources), this surgical idea since this university does not have an ISMS (Information Security Management Systems), already a Through this platform (Virtual Classrooms), personal data of students and teachers are manipulated which can be used incorrectly such as impersonation, theft of sensitive information, publication of sensitive information, etc. it was desired to determine how safe this platform is, to be able to give recommendations is adjustments taking into account the safety of the students that is one of the university's concerns.

Resumen

La elaboración de este proyecto de investigación tuvo como propósito realizar una revisión técnica en la plataforma Aulas Virtuales de la Universidad ECCI se utilizaron de diferentes métodos para obtención de información como lo fue la ingeniería social, por medio de cafés internet pero la más importante haciendo uso de herramientas OSINT (Open Source Inteligence, que hace referencia a cualquier información desclasificada que puede recopilarse en fuentes de acceso público), esta idea surgió ya que esta universidad no cuenta con un SGSI (Sistemas de Gestión de la Seguridad de la Información), y a través de esta plataforma (Aulas Virtuales), se manipulan datos personales de los estudiantes y docentes los cuales pueden ser utilizados de manera incorrecta como lo es la suplantación de identidad, robo deu información sensible, publicación de información sensible, etc. Por esta razón, se deseaba determinar qué tan segura es esta plataforma, para poder dar recomendaciones de ajustes teniendo en cuenta la seguridad de los estudiantes que es una de las prioridades de universidad.

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Capítulo 1. Revisión Técnica de la plataforma Aulas Virtuales de la Universidad ECCI Mediante el Uso de Herramientas OSINT

Revisión técnica de la plataforma Aulas Virtuales de la universidad ECCI mediante el uso de herramientas OSINT.

El proyecto investigativo nace de la necesidad que se vio en la universidad ECCI de tener sus sistemas seguros, ya que la mayoría de estos sistemas, sistemas como ARCA y Aulas virtuales, no cuentan con sistemas de un SGSI (Sistemas de Gestión de la Seguridad de la Información) y esto facilita la aparición de ataques cibernéticos que pueden llegar al robo de la información, publicación de información personal y sensible, falsificación de los datos, suplantación de identidad, phishing, etc. La revisión se va a realizar de carácter técnico, debido a que como se realizará en base a herramientas OSINT únicamente, no se realizarán pruebas diagnósticas ni levantamiento de no conformidades respecto a procedimientos y actividades administrativas asociadas a la plataforma de Aulas Virtuales.

Capítulo 2. Problema de la Investigación

2.1 Descripción del Problema

La Universidad ECCI, en la actualidad cuenta con aproximadamente 19000 miembros activos entre estudiantes, docentes y personal administrativo, en el cual los estudiantes y docentes manejan una plataforma llamada Aulas Virtuales en la que se maneja datos personales protegidos por la legislación. Sin embargo, actualmente la Universidad no cuenta con un SGSI (Sistemas de Gestión de la Seguridad de la Información) que permita tener controles asociados a la protección de los mismos, por lo siguiente los estudios de carácter diagnóstico y auditorías serían fundamentales como soporte a la implementación de un sistema de gestión basado en ISO 27001:2013.

Como la Universidad cuenta con sistemas de información orientado al manejo de la misma desde diversas perspectivas, el presente proyecto se realiza sobre una de las principales plataformas que manejan información con perfiles susceptibles a sufrir incidentes de seguridad, por lo tanto, se propone el análisis a la plataforma antes mencionada (Aulas Virtuales), mediante herramientas OSINT.

El proceso consiste en la búsqueda, selección, adquisición, procesado y análisis de dicha información, para obtener conocimiento aplicable en el contexto organizacional. También sirve para revisar fugas de información y tener conciencia de la información que se está "compartiendo" en internet que puede ser usada por terceros como parte de procesos de recolección de información para posteriores ataques.

2.2 Formulación del Problema

¿Cómo realizar una revisión técnica de la plataforma Aulas Virtuales de la universidad ECCI mediante el uso de herramientas OSINT?

Capítulo 3. Objetivos de la Investigación

3.1 Objetivo General

- Realizar una revisión técnica de la plataforma Aulas Virtuales de la universidad ECCI mediante el uso de herramientas OSINT

3.2 Objetivos Específicos

- Evaluar cada una de las herramientas OSINT para determinar cuál de estas son mejores para ser aplicables y proporcionan mayor cantidad de datos para auditar la plataforma aulas virtuales.
- Definir las herramientas que mejor se adecuen a los parámetros definidos en el proyecto de investigación.
- Usar las herramientas OSINT en la plataforma de Aulas Virtuales de la Universidad ECCI, de acuerdo a los parámetros definidos.
- Evaluar y analizar la información obtenida durante la revisión.
- Clasificar los hallazgos encontrados de acuerdo al grado de impacto para la organización que conlleve el riesgo.
- Realizar las recomendaciones de las acciones correctivas a los sistemas de información (Aulas Virtuales).

Capítulo 4. Justificación y Delimitaciones de la Investigación

4.1 Justificación

La Universidad ECCI tiene como principio el bienestar para los estudiantes y también brindar un excelente servicio en todos los ámbitos. Debido a que la Institución maneja una gran cantidad de datos, debe tener un buen control de los sistemas de información en todas las plataformas virtuales y no virtuales, ya que estas pueden llegar a ser manipuladas y usadas de manera no apropiada afectando la integridad de los datos o simplemente utilizar la información para perjudicar a los miembros de la comunidad educativa. Lo que se busca en esta investigación es determinar si las plataformas que usan los miembros activos son lo suficientemente seguras para no caer ante un ataque cibernético y evitar la sustracción de datos para ser usados en contra de las personas.

Por esta razón, con apoyo del semillero de investigación SIRSEG, en el grupo de interés de seguridad informática, los estudiantes que se inclinan al uso y apropiación de herramientas de software libre para la seguridad de la información, se realizó un estudio para el análisis diagnóstico mediante el uso de herramientas OSINT, con el objetivo de proponer recomendaciones para optimizar el manejo de la información en dichas plataformas y con esto beneficiar a todos los miembros de la comunidad educativa y en especial a la Universidad ECCI, brindándoles un estudio pertinente que ayude para la implementación de la ISO 27001:2013 debido a que la Universidad ECCI no cuenta con un SGSI (Sistemas de Gestión de la Seguridad de la Información), lo cual puede la conllevar a problemas legales. Cabe aclarar que este proyecto se realizó en conjunto con otros semilleristas, los cuales harán el mismo estudio, pero a la plataforma ARCA, por esta razón,

se encontraran algunas imágenes iguales ya que las pruebas técnicas se hicieron al mismo tiempo, sin embargo, los resultados y el documento serán diferentes.

4.2 Delimitaciones

En este proyecto se tendrán en cuenta las siguientes delimitaciones: no se implantará la ISO 270001:2013, se darán las recomendaciones pertinentes para que en un futuro se pueda implementar según con los resultados obtenidos, de la misma forma, se escogerá una muestra de la información recopilada, ya que al ser hacer mucha información no toda cumplirá con los objetivos de la investigación, por otro lado, la población objetivo no será toda la comunidad ECCI, solo se tendrá en cuenta a los estudiantes y docentes ya que son los que utilizan Aulas Virtuales.

En este proyecto no se auditarán, ni procesos, ni procedimientos de seguridad de la información, debido a su naturaleza netamente técnica, basado en la aplicación de herramientas OSINT para la búsqueda de hallazgos de la plataforma de Aulas Virtuales de la Universidad ECCI.

Capítulo 5. Marco de Referencia

5.1 Marco Teórico

5.1.1 OSINT

Al hablar de OSINT existe un proceso en el que la información es recibida, transmitida y analizada para así generar inteligencia con base en la información obtenida. Para entender este proceso es importante tener en cuenta varios aspectos de cómo se realiza el proceso de aprendizaje generando inteligencia. J.L Horn y Raymond Cattell, dos psicólogos que llevaron a cabo varias investigaciones de cómo se realiza el proceso de aprendizaje, definieron dos tipos de inteligencia que constituyen el aprendizaje; inteligencia fluida e inteligencia cristalizada. La inteligencia fluida es la que ayuda a las personas a adaptarse a nuevas situaciones de una manera ágil, esta no requiere de ningún conocimiento previo o experiencia (Michael Glassman, 2012). Y la inteligencia cristalizada es aquella que te ayuda a solucionar problemas con base a las experiencias y conocimientos obtenidos anteriormente. La humanidad hoy en día utiliza la web como solución a muchos problemas, el internet se está volviendo cada vez más parte del ser humano, ahora parece ser una extensión de la mente humana, pero esto lleva a un problema el cual es: ¿Cómo tener la información que en realidad necesito de una manera rápida y además de eso de manera libre, es decir sin necesidad de pago por esta información?, aquí es donde OSINT empieza a jugar su rol.

OSINT es definido por varias entidades de distintas formas, pero a modo general se define como una inteligencia de la rama de las ciber inteligencias que permite obtener información de forma abierta, para luego hacerle un análisis a esta información y usarla para cualquier fin, las personas suelen usarlo de diferentes maneras, pero para poder llegar a un resultado OSINT se divide en diferentes fases básicas que muchas veces son intuitivas, estas son: requisitos, fuentes de información, adquisición, procesamiento, análisis y por último, presentación de la inteligencia.

La fase de los requisitos es aquella donde se define qué es lo que se quiere lograr de manera concreta, la fase de fuentes de información se basa en definir los lugares donde se buscará la información así como también las herramientas que nos permitirán obtener dichos datos, en la adquisición se extrae la información con las herramientas de los medios que se han escogido, después de esto en la fase de procesamiento se le da un formato a la información para poder pasar a analizarla de la mejor manera, en el análisis se extrae la información de utilidad y se someten a análisis estadístico para luego sacar conclusiones y tomar decisiones a partir de los datos obtenidos (GL, 2019).

Actualmente OSINT es ampliamente utilizado por muchas personas y entidades ya que esta inteligencia puede ser usada para obtener datos, para buscar personas, para buscar empresas entre otras muchas cosas. Es por esto los investigadores, periodistas, detectives, escritores, estudiantes, hasta policías y miembros del ejército hacen uso de esta inteligencia, ya que se puede dar con información importante a costa de una baja exposición ante el objetivo, también es debido a esto que los ciberdelincuentes utilizan estos métodos para capturar información de manera segura ya que la información que obtienen es libre, gratuita y se obtiene de manera legal (GL, 2019).

5.1.2 Norma ISO 27001:2013

La norma ISO 27001:2013 tiene como propósito establecer, implementar, mantener y mejorar continuamente los SGSI (Sistema de Gestión de la Información), esta también incluye requisitos para evaluar y tratar el riesgo de la seguridad en la información, esta norma presenta objetivos de control y controles que se deben tener en cuenta durante una auditoria de un sistema de información, ya que estos controles ayudan al constante mejoramiento de los hallazgos y no conformidades encontrados durante la auditoria.

5.2 Marco Conceptual

- **OSINT**

Open Source Intelligence o Inteligencia de fuentes abiertas (papelesdeinteligencia.com, s.f.).

- **SGSI**

Sistema de Gestión de la Seguridad de la Información (SGSI, 2015).

- **Revisión Técnica**

Una revisión técnica es hacer un estudio para determinar el estado de una empresa en alguna de las áreas (mantenimientopetroquimica.com, s.f.).

- **Ataque Cibernético**

Consiste en una serie de acciones cuyo objetivo es comprometer los sistemas informáticos de una organización (Carisio, s.f.).

- **Hallazgos**

Se refiere a las debilidades encontradas o detectadas por el por el auditor durante la auditoria (Contraloria General del Estado, s.f.).

- **Incidentes de Seguridad de la Información**

Se refiere al acceso, intento de acceso, divulgación, uso, modificación o destrucción no autoriza de la información (Universidad Nacional de Luján, s.f.).

- **Riesgo**

Se refiere a la probabilidad de que suceda algún evento de peligro y sus consecuencias negativas (ciifen, s.f.).

- **No Conformidades**

Se refiere a la no atención de un requisito preestablecido (Jeison, s.f.).

- **Software Libre**

Se refiere a un programa informático donde los usuarios lo puede copiar, modificar, redistribuir, para el beneficio de la comunidad (significados.com, 2017).

- **Vulnerabilidad Técnica**

Se refiere a las características y circunstancias de un sistema que los hace susceptibles a los efectos de Una Amenaza (ciifen, s.f.).

- **Amenaza**

Se refiere al hecho o acontecimiento que no ha sucedido, pero de concretarse lo dicho, puede perjudicar a varias personas o a un sistema (significados.com, 2017).

- **Información Sensible**

Se refiere a la información personal privada de un individuo, por ejemplo, cedula, contraseña, datos bancarios, etc. (Wikipedia, s.f.).

- **Datos Personales**

Se refiere a toda la información que nos identifica (infodf, s.f.).

- **Ingeniería Social**

Consiste en engañar a las personas para que entregue su información personal como contraseñas, datos bancarios o que le permita el acceso a un computador (avast, s.f.).

- **Suplantación De Identidad**

Consiste en hacerse pasar por otra persona para obtener un beneficio (ayudaleyprotecciondatos, 2018).

5.3 Marco Legal

El proyecto que a continuación se presenta da cumplimiento con las siguientes leyes:

Artículo 15.

"Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. La correspondencia y demás formas de comunicación privada son inviolables" (constitucion colombia, 2020)

Ley 1266 del 2008

Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

Artículo 2. Ámbito de aplicación. La presente ley se aplica a todos los datos de información personal registrados en un banco de datos, sean estos administrados por entidades de naturaleza pública o privada. Se exceptúan de esta ley las bases de datos que tienen por finalidad producir la Inteligencia de Estado por parte del Departamento Administrativo de Seguridad, DAS, y de la Fuerza Pública para garantizar la seguridad nacional interna y externa (colaboracion.dnp, s.f.).

Artículo 4. Principios de la administración de datos, estos son algunos de los principios que están asociados al proyecto, ya se establece como debería administrarse los datos y siendo la universidad una entidad tan grande se deben tener en cuenta.

a) Principio de veracidad o calidad de los registros o datos. La información contenida en los bancos de datos debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el registro y divulgación de datos parciales, incompletos, fraccionados o que induzcan a error;

b) Principio de finalidad. La administración de datos personales debe obedecer a una finalidad legítima de acuerdo con la Constitución y la ley. La finalidad debe informar al titular de la información previa o concomitantemente con el otorgamiento de la autorización, cuando ella sea necesaria o en general siempre que el titular solicite información al respecto;

c) Principio de circulación restringida. La administración de datos personales se sujeta a los límites que se derivan de la naturaleza de los datos, de las disposiciones de la presente ley y de los principios de la administración de datos personales especialmente de los principios de temporalidad de la información y la finalidad del banco de datos. Los datos personales, salvo la información pública, no podrán ser accesibles por Internet o por otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o los usuarios autorizados conforme a la presente ley;

d) Principio de temporalidad de la información. La información del titular no podrá ser suministrada a usuarios o terceros cuando deje de servir para la finalidad del banco de datos;

f) Principio de seguridad. La información que conforma los registros individuales constitutivos de los bancos de datos a que se refiere la ley, así como la resultante de las consultas que de ella

hagan sus usuarios, se deberá manejar con las medidas técnicas que sean necesarias para garantizar la seguridad de los registros evitando su adulteración, pérdida, consulta o uso no autorizado;

g) Principio de confidencialidad. Todas las personas naturales o jurídicas que intervengan en la administración de datos personales que no tengan la naturaleza de públicos están obligadas en todo tiempo a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende la administración de datos, pudiendo sólo realizar suministro o comunicación de datos cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma.

Ley 1581 de 2012

"Régimen General de Protección de Datos Personales, en el que, además, se señalan los principios y obligaciones que tienen todos aquellos que realicen el tratamiento de datos personales para garantizar la protección del derecho fundamental de habeas data".

Artículo 3. Definiciones.

En este artículo se presentan algunas definiciones que al manejar información personal se deben tener en cuenta, para no tener conflictos con la ley

1. Aviso de privacidad: Comunicación verbal o escrita generada por el Responsable, dirigida al Titular para el Tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de Tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del Tratamiento que se pretende dar a los datos personales.

2. Dato público: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio ya su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

3. Datos sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

4. Transferencia: La transferencia de datos tiene lugar cuando el Responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país.

5. Transmisión: Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un Tratamiento por el Encargado por cuenta del Responsable.

Tenido las definiciones se puede desglosar la ley 1581, que se mostrará según la ley como se debe tratar la información (MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO, s.f.).

Capítulo 6. Tipos de Investigación

6.1 Investigación Exploratoria

Será utilizada para toda la primera fase del proyecto para lograr definir las herramientas más acordes que se usarán.

6.2 Investigación Descriptiva

Será utilizada en el definir de los objetivos y el alcance que tendrá el proyecto.

6.3 Investigación Analítica

Será utilizada para comenzar a validar cada una de las herramientas con el fin de determinar cuáles son las ideales en el proyecto.

6.4 Investigación Explicativa

Se utilizará para explicar por qué se escogieron esas herramientas para la búsqueda de información.

6.5 Investigación de Campo

Se utilizará para la recolección de datos y adquisición de información que se usará con las herramientas.

6.6 Investigación Correlacional

Será utilizada para el análisis de toda la información obtenida durante todo el proyecto.

6.7 Investigación Proyectiva

Se utilizará para dar las propuestas de mejora según la información de que se obtuvo, para evitar los posibles ataques de la información.

Tabla 1. Tipos de Investigación de Proyectos y sus Etapas.

Tipo de investigación	Definición	Actividades
Investigación exploratoria	Este tipo de investigación es utilizada en su mayor parte para definir un problema que no está claramente definido	Estudio de la inteligencia
		Búsqueda de referencias anteriores
Investigación descriptiva	Este tipo de investigación es usada para describir una población o un fenómeno, esta no responde preguntas, no va más allá de la descripción de un fenómeno.	Definición del alcance
		Desarrollo de los objetivos
Investigación analítica	Consiste en establecer las diferencias entre las variables de estudio, además es usada para plantear hipótesis que el investigador debe probar	Análisis de herramientas OSINT
Investigación explicativa	Esta se enfoca en explicar el por qué y el para que de un fenómeno o variable dentro de la investigación	Elección de herramientas más apropiadas
Investigación de campo	Investigación de campo es aquella que se aplica extrayendo datos e informaciones directamente de la realidad a través del uso de	Obtención de datos mediante ingeniería social

	técnicas y herramientas de recolección	Adquisición de información(Gathering)
Investigación correlacional	Este tipo de investigación busca establecer la relación que hay entre dos o más variables por medio de datos estadísticos	Procesamiento y análisis de información
Investigación proyectiva	Investigación proyectiva es enfocada en elaborar propuestas para el mejoramiento de una situación o fenómeno	Propuesta para prevención de posibles ataques

Fuente: Los Autores 2020.

Capítulo 7. Diseño Metodológico

7.1 Investigación Exploratoria

En esta parte del proceso se realizaron diferentes consultas que ayudaron a determinar cuáles son las herramientas OSINT que existen.

- Lista de herramientas OSINT consultadas

Tabla 2. Lista de herramientas OSINT

Herramientas OSINT	
Spiderfoot	SocialBearing
EmailHarvester	Socialmention
Theharvester	Twopcharts
HTTrack	VRLCrazy
KeePassXC	OSINTUX
Dataspbit	Maltego
Dmitry	Social
Infoga	Recont
Glassdoor	PIPL
Knowem	OSINT-Spy
Shodan	Opencorporates

Fuente: Los Autores 2020

7.2 Investigación Descriptiva

En esta parte del proceso se determinaron cuáles eran los objetivos de proyecto teniendo en cuenta lo que se deseaba realizar y con la información que se tenía, por otro lado, se pudo determinar los pasos que se iban a seguir para llegar a los objetivos definidos, también se pudo determinar el alcance del proyecto teniendo en cuenta las delimitaciones antes mencionadas esto con el fin de que el proyecto salga con lo planeado.

7.3 Investigación Analítica

Continuando con el proceso, en esta parte se tomaron cada una de las herramientas y se investigaron con más profundidad, para saber cuál era la especialidad de cada una y poder determinar cuáles son las más indicadas para usar en el proyecto.

Tabla 3. Especialidades Herramientas OSINT

Herramientas OSINT	Especialidad
Spiderfoot	IPs, dominios emails, nombres
EmailHarvester	Direcciones de email de un dominio
Theharvester	subdominios y nombres de empleados
HTTrack	Descargas sitios web al PC
Dataspbit	Dominio, nombres de usuario
Dmitry	Host
Infoga	Recopilar información de correos en fuentes abiertas
Glassdoor	Información respecto a una empresa
Knowem	Disponibilidad de nombre de usuario
Shodan	Busca sistemas y servicios conectados a internet
SocialBearing	Búsqueda de personas por redes sociales
Socialmention	Búsqueda de personas por redes sociales
Twopcharts	Relacionado con Twitter
URLCrazy	Ayuda a detectar la variación de un dominio
OSINTUX	Sistema operativo que contiene varias herramientas OSINT
Maltego	Búsqueda de personas y empresas, por medio de redes sociales, servidores de correo, etc.
PIPL	Buscador de personas por medio del nombre, correo, teléfono, etc.
OSINT-Spy	Buscador de personas, correo electrónico, la geolocalización, nombres de dominio, etc.
Opencorporates	Búsqueda de empresas que sea accesible y usable.

Fuente: Los Autores 2020

7.4 Investigación Explicativa

Siguiendo con el proceso en esta parte se pudo determinar que la herramienta a utilizar es OSINTUX, es un sistema operativo de la distribución de Linux en español dedicado a la inteligencia de fuentes abiertas, este sistema operativo se seleccionó porque contiene varias de las

herramientas mencionadas en la Tabla 2. Lista de herramientas OSINT, también porque facilita el proceso de la obtención de las herramientas, es decir, como el sistema operativo ya contiene las herramientas que se van a utilizar, no es necesario descargar una por una, a continuación, se podrá observar el listado de las herramientas que contiene OSINTUX.

- Lista de herramientas instaladas en OSINTUX

Tabla 4. Aplicaciones OSINTUX

Herramientas OSINTUX	
Belati v.0.2.4.1	Opencorporates
Creepy v1.4	Operative Framework
Crunchbase	OSINT-Spy v0.0.1
Datasploit for OSINT	OSRFramework v2018
Dmitry	OSINTFramework
Exiftool v11.03	PIPL
Google Hacking Database	Recon-NG v4.9.3
Infoga – Email Information	SocialBearing
GeoIP	Socialmention
Glassdoor	SpiderFoot v2.12
Knowem	The Harvester v2.2ª
Maltego v4.1.6.11045	Tineye
MentionMap	Tinfoleak v2.1
Metagoofil v2.2	Twopcharts
MrLooquer	ViewDNS
Netcraft	YouGetSignal
Shodan	Whois

Fuente: Los Autores 2020

Con la Tabla 4. Aplicaciones OSINTUX, las aplicaciones que se utilizaran son MALTEGO, Spiderfooot, The Harvester, Shodan, FOCA, etc. estas herramientas se enfocan en la búsqueda de información por internet y lo muestra de forma gráfica para que se mas fácil de analizar, también busca links los cuales están relacionados con la búsqueda echa, entonces lo primero que se desea hacer es buscar el dominio de la Universidad ECCI, e ir desglosando la información hasta encontrar

datos sobre Aulas Virtuales, después con la información que se obtuvo en los cafés internet comenzar a buscar personas, y mirar que se puede inferir de los datos obtenidos.

Ilustración 1. Sistema Operativo OSINTUX

Fuente: (osintux, 2020)

7.5 Investigación de Campo

7.5.1 Encuesta virtual

Siguiendo con el proceso lo primero que se realizó fue ingeniería social (consiste en engañar a las personas para que entregue su información personal como contraseñas, datos bancarios o que les permita el acceso a un computador) la cual se decidió hacer porque se quería determinar qué tan fácil es que una persona entregue sus datos personales, para esto se realizó una encuesta sobre el centro de desarrollo empresarial porque se sabía que era un tema nuevo en la universidad y las personas no dudarían en entregar sus datos personales, las encuestas se realizaron de manera virtual y presencial, en la parte virtual 118 personas de diferentes carreras contestaron la encuesta y en la parte presencial 27 personas realizaron la encuesta.

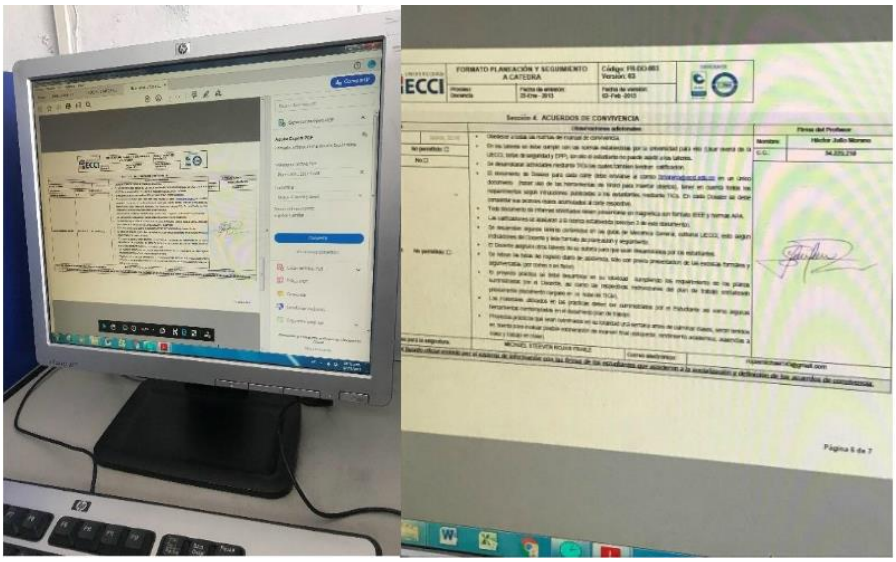
Ilustración 2. Encuesta Virtual

Fuente: Los autores 2020

7.5.1 Obtención de información en el espacio publico

Lo segundo que se realizo fue ir a los cafés internet, y comenzar a revisar los documentos que los estudiantes dejaban de tal forma, que se extrajeron y se revisaron para saber qué información útil tenía para el proyecto como por ejemplo la cedula, el código estudiantil, el nombre, etc. Con el fin de utilizarlo para ingresar a la cuenta de Aulas Virtuales.

Ilustración 3. Café Internet



Fuente: Los Autores 2020

7.5.3 Uso de herramientas OSINT

Lo tercero que se realizó fue bootear una memoria con el sistema operativo OSINTUX, después se comenzó a evaluar el uso de cada una de las herramientas, en especial las aplicaciones que se van a utilizar es MALTEGO, Spiderfoot, Shodan, The Harvester, etc. Hasta entender cómo se utilizan para cumplir con los objetivos del proyecto.

7.6 Investigación correlacional

En esta parte del proceso se puede evidenciar en el capítulo 8. Resultados, donde se muestra cada uno de los hallazgos encontrados y porque es importante pensar en implementar un SGSI (Sistema de Gestión de Seguridad de la Información).

7.7 Investigación Proyectiva

Esta parte del proceso se puede evidenciar más adelante, después del análisis realizado con los hallazgos encontrados, se podrán determinar las acciones de corrección y propuesta de prevención a posibles ataques al robo de la información personal.

Capítulo 8. Resultados

En este capítulo se verán los resultados obtenidos de las actividades realizadas, las cuales se ven en la Tabla 5. Resultados de las actividades realizadas, de estos se obtendrá información para la redacción de los hallazgos y no conformidades.

Tabla 5. Resultados de las actividades realizadas

Numeral	actividades
1	Análisis de encuestas
2	Análisis de obtención de información en espacio publico
3	Uso de herramienta Maltego
4	Uso de herramienta Spiderfoot
5	Uso de herramienta The Harvester
6	Hallazgos con estándar ISO 27001
7	Recomendaciones de acciones de mejora

Fuente: Los autores 2020

8.1 Encuesta Virtual

En esta parte de resultados se trabajó por etapas: en primer lugar, se tomó la información obtenida en la encuesta y se pudo determinar que de las 118 personas que realizaron la encuesta de manera virtual teniendo en cuenta que todos eran estudiantes, solo dos personas no entregaron ni su código estudiantil, ni su cedula, que de las 117 personas restantes que si entregaron sus datos 99 se logró entrar a su cuenta en Aulas Virtuales, que las carreras que más respondieron la encuesta fue gestión de procesos industriales con un total de 30 estudiantes de los cuales 28 tuvimos acceso a su cuenta de Aulas Virtuales, después sigue desarrollo informático con 24 estudiantes en total y se pudo acceder a las cuenta de 19 de ellos, por últimos ingeniería mecánica automotriz con un total de 12 estudiantes de los cuales 9 estudiantes se tiene acceso a la cuenta, estas cifras son alarmantes ya que se quería realizar un estudio por carrera pero no todos aceptaron responder la

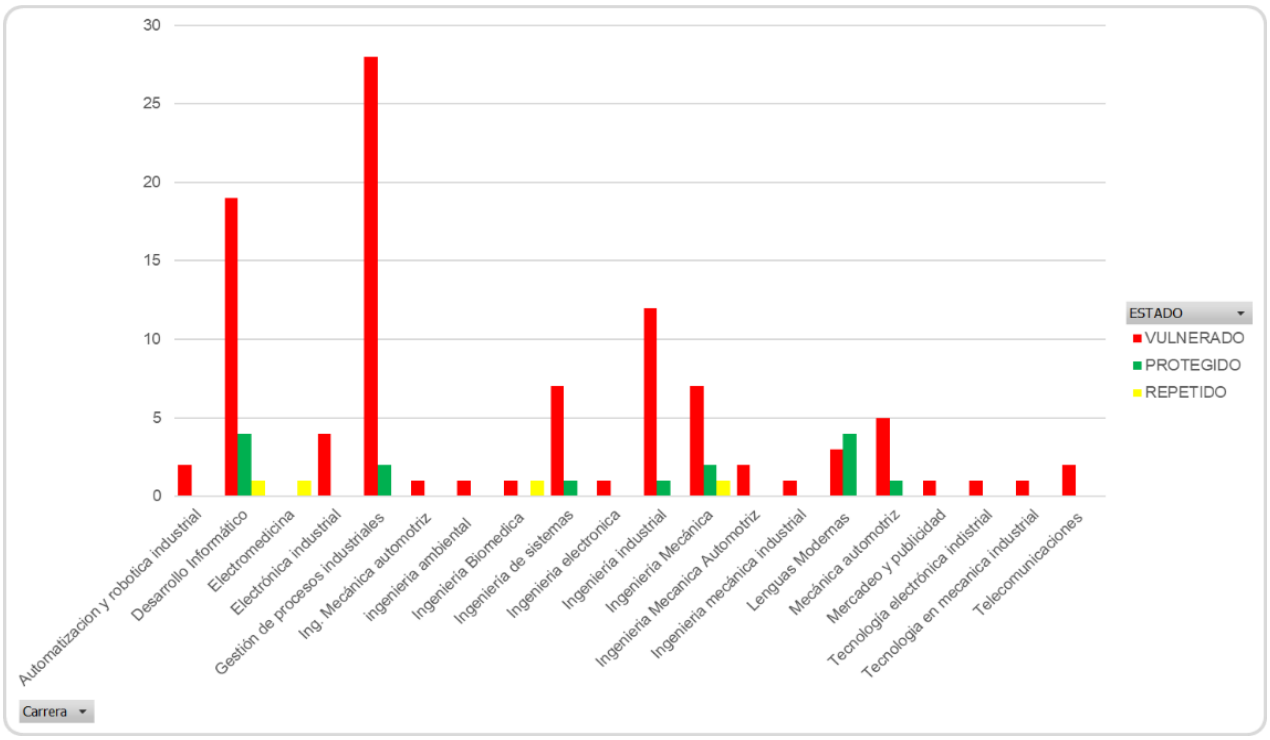
encuesta, sin embargo, con los datos obtenido se puede decir que se podría acceder a la mayoría de la cuenta de Aulas Virtuales de los estudiantes, simplemente obtenido la cedula de ellos.

Tabla 6. Análisis de la encuesta virtual realizada

Cuenta de ESTADO	**Etiquetas de columna**			
Etiquetas de fila	**VULNERADO**	**PROTEGIDO**	**REPETIDO**	**Total general**
Automatización y robótica industrial	2			2
Desarrollo Informático	19	4	1	24
Electro medicina			1	1
Electrónica industrial	4			4
Gestión de procesos industriales	28	2		30
Ing. Mecánica automotriz	1			1
ingeniería ambiental	1			1
Ingeniería Biomédica	1		1	2
Ingeniería de sistemas	7	1		8
Ingeniería electrónica	1			1
Ingeniería industrial	12	1		13
Ingeniería Mecánica	7	2	1	10
Ingeniería Mecánica Automotriz	2			2
Ingeniería mecánica industrial	1			1
Lenguas Modernas	3	4		7
Mecánica automotriz	5	1		6
Mercadeo y publicidad	1			1
Tecnología electrónica industrial	1			1
Tecnología en mecánica industrial	1			1
Telecomunicaciones	2			2
Total general	**99**	**15**	**4**	**118**

Fuente: Los Autores 2020

Ilustración 4. Gráfico de Barras de la Encuesta Realizada



Fuente: Los Autores 2020

Ilustración 5. Grafico Tipo Torta de la Encuesta Virtual

Fuente: Los Autores 2020

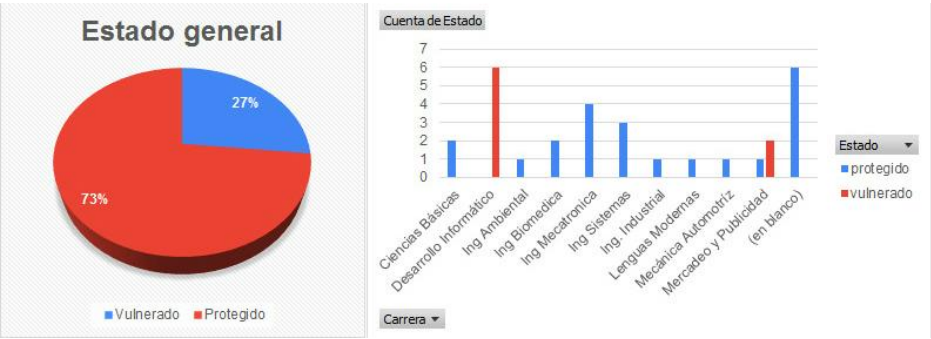
Tabla 7. Resultados encuesta virtual

	Estado General
Vulnerado	**99**
Protegido	15
Repetido	4

Fuente: Los Autores 2020

Por otro lado, se realizaron 30 encuestas presenciales, que se decidieron hacer porque en los resultados de las encuestas virtuales ningún docente accedió a contestar esta y dentro de las delimitaciones, nuestra población objetivo son estudiantes y docentes. En el análisis de las encuestas se puede evidenciar que 19 encuestados eran docentes y 11 estudiantes con lo que se puede concluir, que los docentes tienen un poco más de conciencia al momento de entregar sus datos, que no confían en la información que llega por internet y mirando los resultados en un formato, todos los profesores cambiaron su contraseña en la plataforma de Aulas Virtuales pero eso no significa que todos los docentes tengan las mismas prácticas de seguridad, mirando más a fondo el formato solo hay 26 personas inscritas porque tres docentes y un estudiante no accedieron a entregar su información, sin embargo, los otros 11 estudiantes encuestados solo 2 de ellos tiene su cuenta protegida, es decir, que si lo comparamos con las encuestas virtuales el 83.89% de los estudiantes no tienen cuenta protegida que es un porcentaje bastante similar al de las encuetas presenciales porque 72.72% de los estudiantes no protegieron su cuenta, se puede determinar que es un porcentaje menor comparado con la virtual, pero bastante alto para el numero de encuestados.

Ilustración 6. Grafica Encuesta Presencial



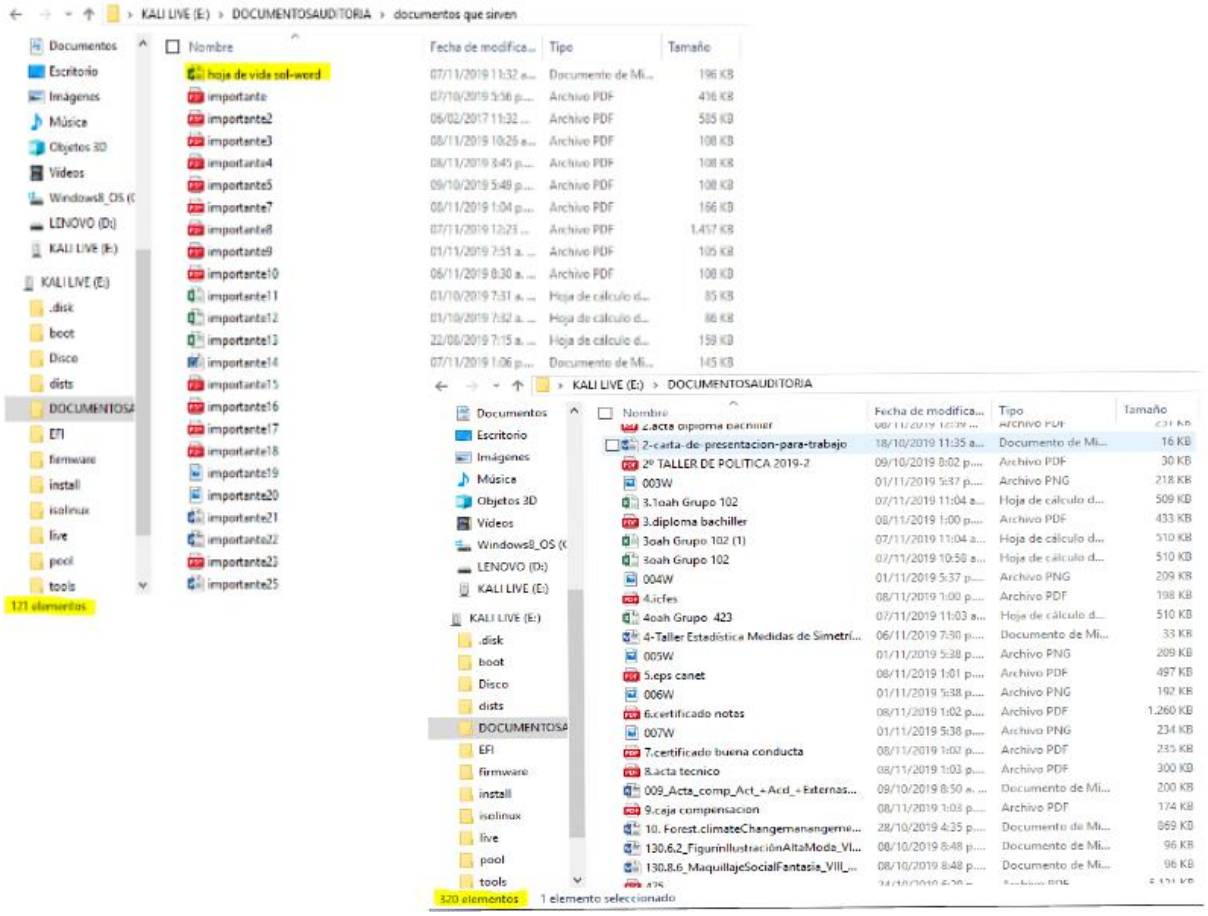
Fuente: Los Autores 2020

8.2 Obtención de Información en el Espacio Público

Segundo se revisaron los documentos obtenidos en los cafés internet y se logró encontrar que de cuatrocientos cuarenta y dos (442), ciento veintiuno (121) documentos tenían información

personal de estudiantes como docentes, los documentos contenían hojas de vida, cedulas, recibos de pago de la universidad, actas de grado y el que más impacto tuvo según nuestra investigación fue que en uno de los computadores un profesor tenía su Dropbox abierto y se puedo obtener mucha información de él como de los estudiantes, con esta información logramos acceder a varias cuentas de Aulas Virtuales de la universidad, y con otra la utilizamos para implementarla en las herramientas OSINT, en esta parte del análisis se logró identificar que mucho de los estudiantes no tiene cuidado con los documentos que descargan en los cafés internet y que por algún descuido los profesores también pueden exponer información de los estudiantes como de ellos.

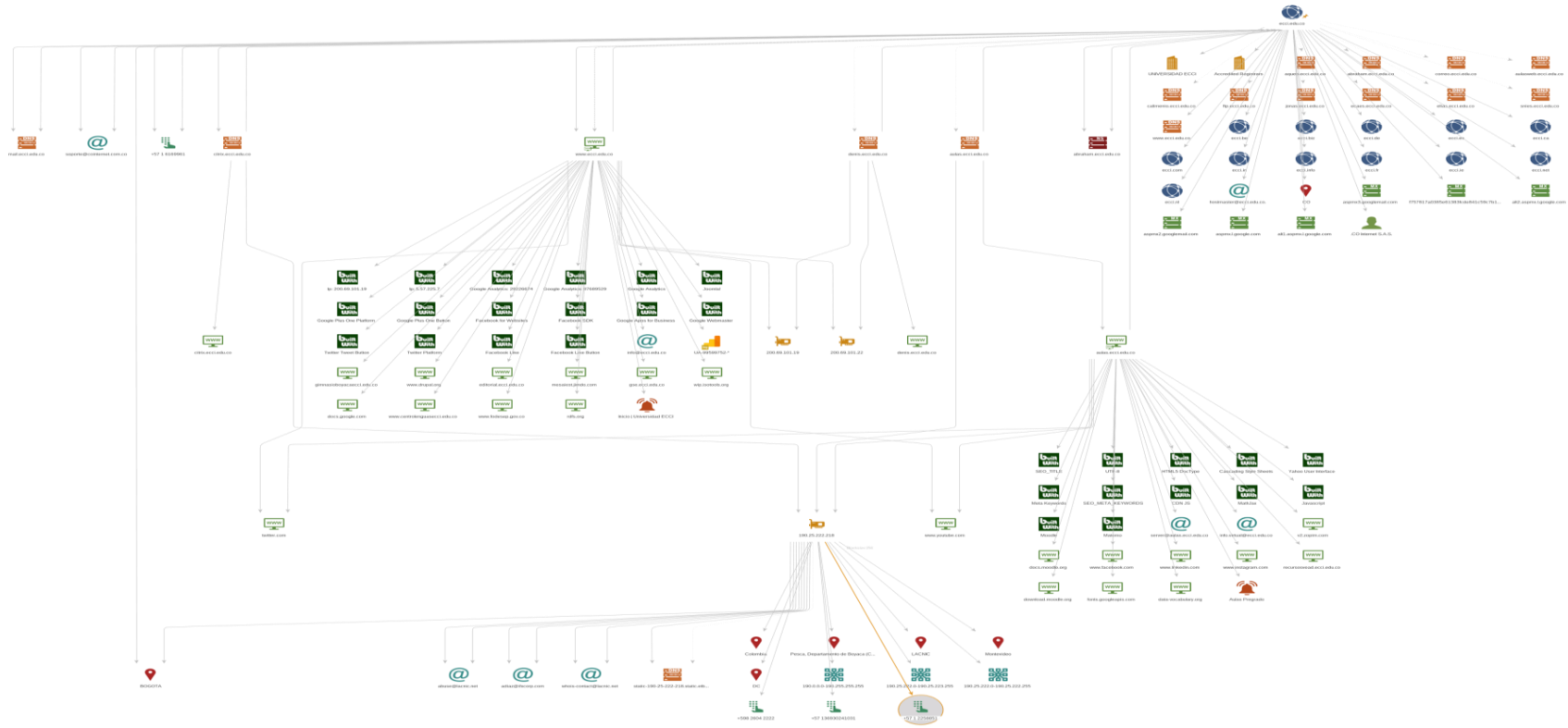
Ilustración 7. Hallazgos en Café Internet



Fuente: Los Autores 2020

8.3 Uso de Herramienta OSINT Maltego

Ilustración 8.Grafo Principal de la Universidad ECCI, Hecho en MALTEGO

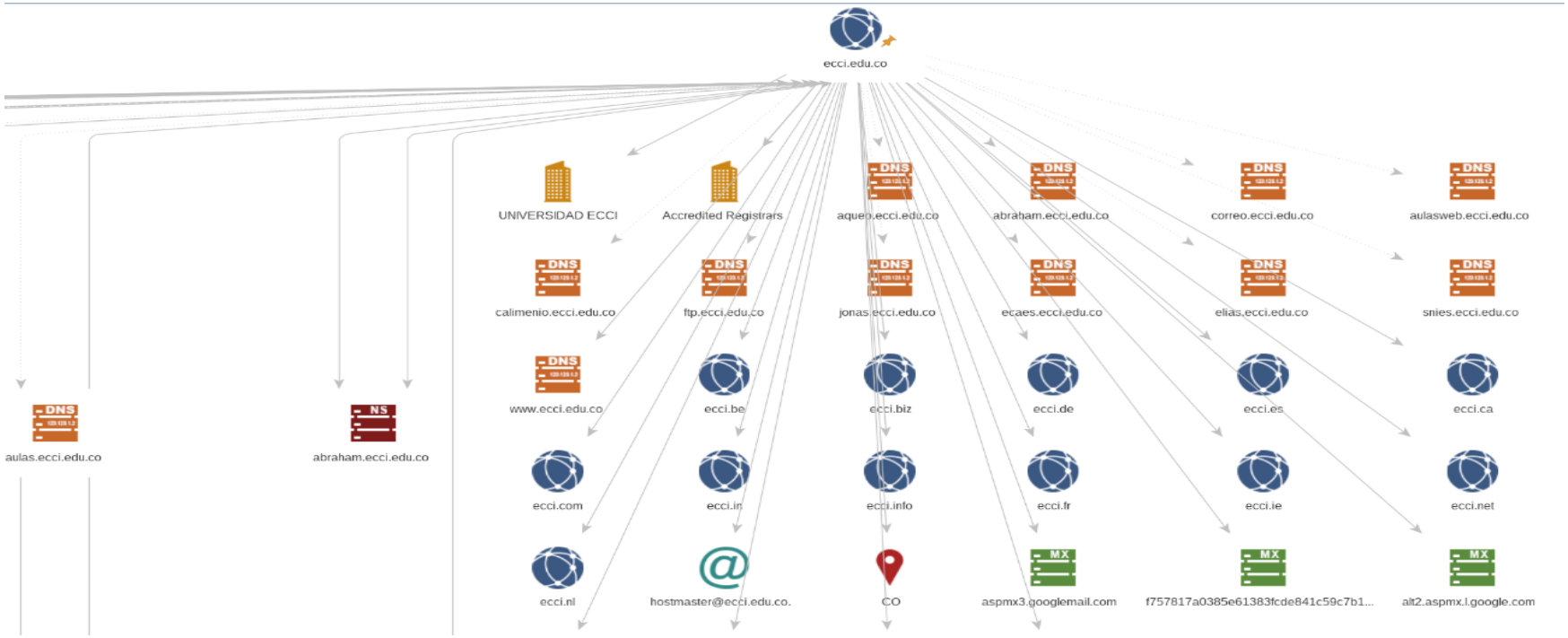


Fuente: los autores 2020

Esta fue la primer investigación que se realizó, se inició realizando la búsqueda de todas las transformaciones que tenía el dominio ecci.edu.co y lo que se encontró al principio fue un conjunto de dominios ecci.* los cuales provenían de otros dominios web ajenos a la

universidad ECCI, también dentro de estas transformaciones se encontraron dos organizaciones o compañías, universidad ECCI y Accredited Registrars como se puede visualizar en la siguiente imagen:

Ilustración 9.Compañías y Servidores DNS Encontrados con la Herramienta MALTEGO

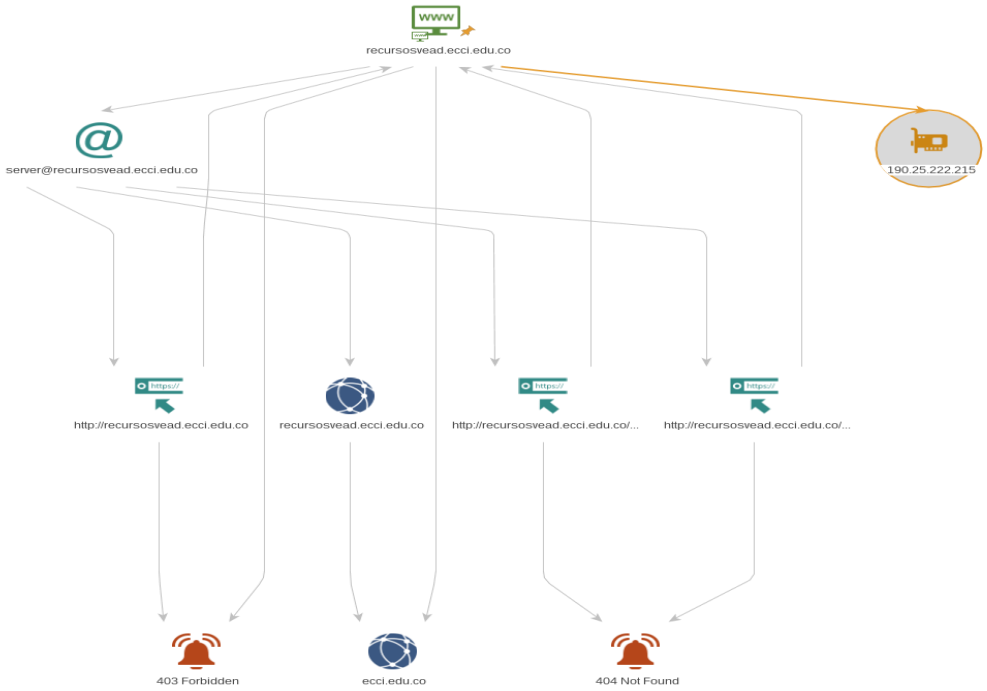


Fuente: Los autores 2020

También pudimos observar que la universidad tiene un vínculo directo con la empresa .co internet Colombia, además de eso se encontraron servidores DNS de los cuales se encontraron dos bien conocidos, aulas.ecci.edu.co y www.ecci.edu.co a los cuales se les hizo las respectivas transformaciones y de ellos se encontraron direcciones IPs y también sitios web como aulas.ecci.edu.co y

www.ecci.edu.co los cueles volvieron a ser transformados y desde este punto se encontró un patrón en común, este patrón fue que la dirección IP publica 190.25.222.218 y la dirección IP 190.25.222.215 que sale de transformar al sitio web recursosvead.ecci.edu.co.

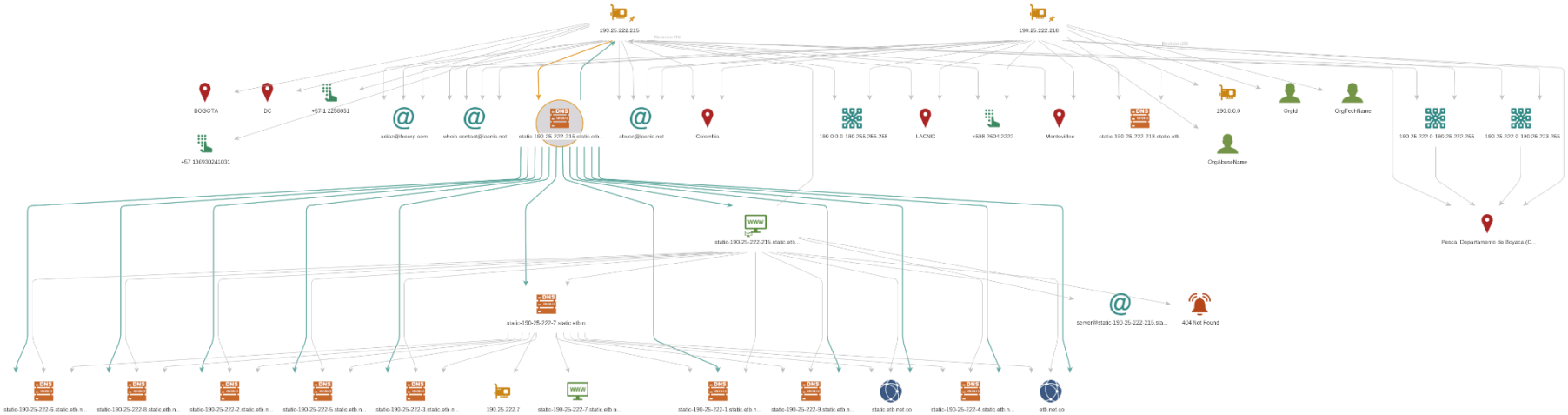
Ilustración 10.Transformaciones Recursos, hecha en MALTEGO



Fuente: Los autores 2020

También dentro de los grafos se encontró un sitio web, recursosvead.ecci.edu.co, de donde se encontró el dominio ecci.edu.co,3 URLs de los cuales 2 no se encuentran en uso y uno de ellos no deja acceder a la página web y también se encontró un correo sever@recursosvead.ecci.edu.co, a continuación se encontró también una dirección IP púbica con la cual se hizo otro grafo.

Ilustración 11.Grafo de IPs Publicas Encontradas, Hecho en MALTEGO



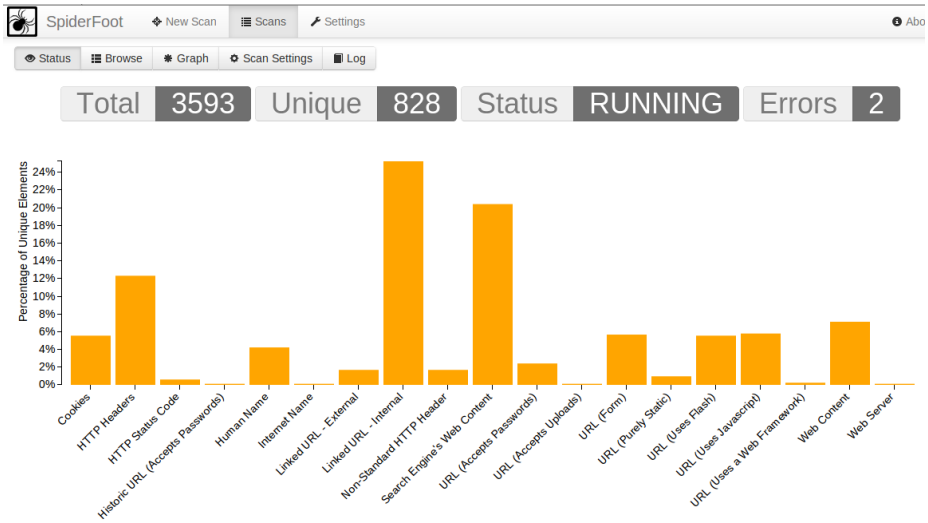
Fuente: Los autores 2020

Después de este hallazgo, en un grafo nuevo se colocaron las 2 IP públicas y se comenzaron a transformar, y de esto se encontró un vínculo entre la universidad ECCI y la empresa de telefonía ETB, de lo que se infiere que el proveedor de servicios de la universidad es ETB y las 2 IPs publicas encontradas las suministró esta empresa, lo que quiere decir que estas dos direcciones IP apuntan a la entrada de alguno de los servidores de la universidad ECCI, probablemente a uno de los servidores DNS.

8.4 Uso de Herramienta OSINT Spiderfoot

El primer hallazgo que se pudo encontrar con la herramienta Spiderfoot fue una gráfica que muestra que encontró 3593 (Ilustración 12. Grafica herramienta Spiderfooot) elementos relacionados con el dominio de Aulas.ecci.edu.co, que de los 3593 elementos 828 de estos eran únicos (significa que logro encontrar mucha información de una URL o dato).

Ilustración 12.Grafica de Herramienta Spiderfoot



Fuente: Los autores 2020

Ilustración 13.Número de Información por Elemento

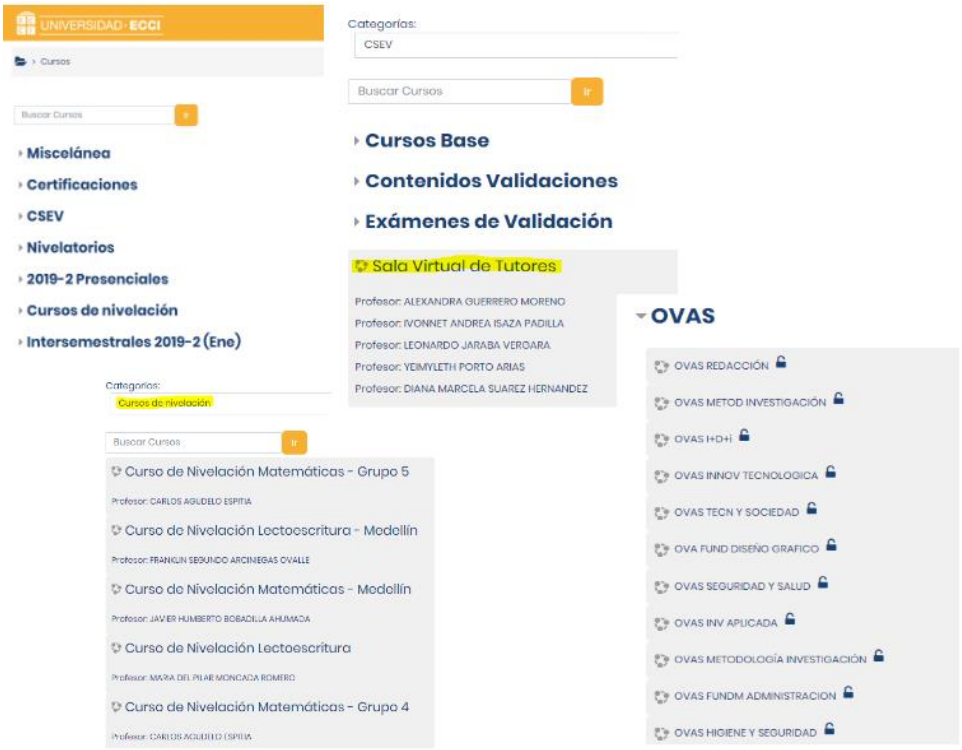
Type	Unique Data Elements	Total Data Elements
Cookies	46	46
HTTP Headers	102	102
HTTP Status Code	5	102
Historic URL (Accepts Passwords)	1	1
Human Name	35	687
Internet Name	1	1
Linked URL - External	14	466
Linked URL - Internal	209	1434
Non-Standard HTTP Header	14	154
Search Engine's Web Content	169	169
URL (Accepts Passwords)	20	20
URL (Accepts Uploads)	1	1
URL (Form)	47	47
URL (Purely Static)	8	8
URL (Uses Flash)	46	46
URL (Uses Javascript)	48	48

Fuente: Los autores 2020

La ilustración 13. Número de información por elemento, es muy importante porque muestra el número de datos encontrados por cada tipo de elemento de la gráfica anterior, sin embargo, el elemento Linked URL – Internal fue el más importante porque obtuvo mayor información en todos los sentidos, primero, como se puede observar que se encontró 1434 elementos, y segundo esos elementos son de los cuales se logró obtener información importante como lo verán a continuación.

El primer link que se va a analizar es https://aulas.ecci.edu.co/course/index.php, en el cual se consiguió ver cierta información que no puede ver un estudiante, como por ejemplo, cursos que se dictan y con el nombre del profesor, nivelatorios, intersemestrales, certificaciones, etc. Esto es muy importante porque es información de la universidad y de los docentes.

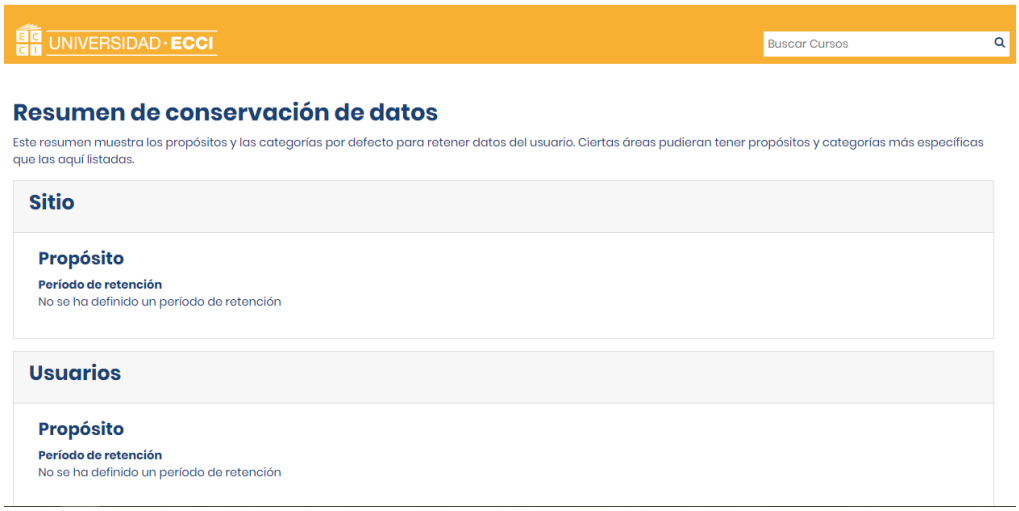
Ilustración 14. Resultados Herramienta Spiderfoot



Fuente: Los Autores 2020

El segundo link fue https://aulas.ecci.edu.co/admin/tool/dataprivacy/summary.php este link es un poco curioso porque habla sobre la conservación de datos que es un tema que se trabaja durante el documento, pero lo importante de esto es la información que muestra, no contiene protección de los datos, no tienen establecidas una normas sobre la información sensible, entre otros, sin embargo, dice que es un resumen por lo que podeos concluir que probablemente el documento completo si lo tenga las políticas del uso de los datos.

Ilustración 15. Resultado Conservación de Datos



Fuente: Los Autores 2020

Los siguientes links, si es información que tiene públicamente la Universidad ECCI, como por ejemplo el PDF del cronograma de actividades (https://recursosvead.ecci.edu.co/ cronograma_2019II.pdf), imágenes que aparecen en la página de la Universidad (https://aulas.ecci.edu.co/pluginfile.php/1177/block_html/content/BANNER%20ECCI-04.png), el link del debido proceso (https://recursosvead.ecci.edu.co/Debido_proceso.html), etc. Otros links no eran visibles para los estudiantes, pero están relacionados con el primer link porque se dirigían a cada uno de los cursos mostrados en la Ilustración 14. Resultados Herramienta Spiderfoot.

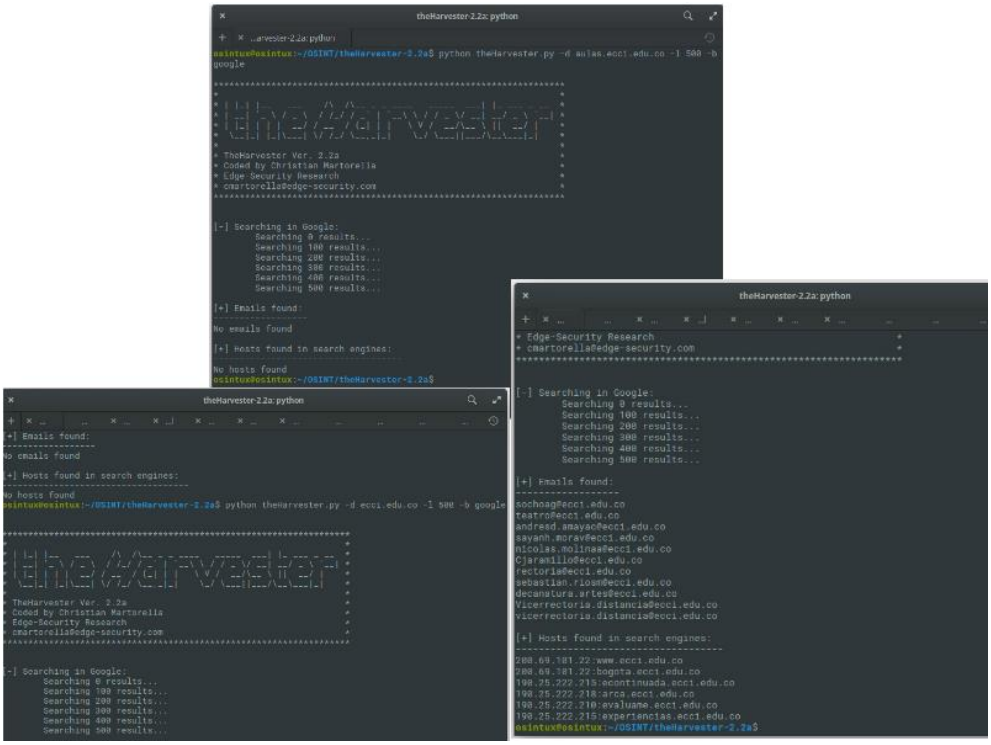
Ilustración 16. Imagen Encontrada por Spiderfoot

Fuente: Los Autores 2020

8.5 Uso de Herramienta OSINT The Harvester

Con la herramienta The Harvester los hallazgos obtenidos fueron al buscar el dominio ecci.edu.co con lo que se encontró unas IPs y correos relacionadas con la Universidad, sin embargo, la IP que más se acerca a la investigación fue de evaluame.ecci.edu.co y experiencias.ecci.edu.co porque son plataformas similares a la de Aulas Virtuales, ya que al indagar el dominio aulas.ecci.edu.co no se encontró nada.

Ilustración 17. Resultados The Harvester



Fuente: Los Autores 2020

8.6 Hallazgos

Después de haber hecho el análisis de la información obtenida se buscaron hallazgos los cuales se clasificaron y se identificaron según los controles del estándar ISO 27001:2013.

Tabla 8. Primer Hallazgo

REVISIÓN TECNICA	NO CONFORMIDAD MAYOR _X_ MENOR
PROCESO REVISADO: Aulas virtuales	
ESTANDAR Y NUMERO DE ELEMENTO 27001:2013, A.13.2. Transferencia de información	
HALLAZGO:	
Se evidencia que las personas son propensas a caer en manipulaciones de ingeniería social, lo que hace que sean expuestos a robo de información sensible, incumpliendo así el control A.13.2.1 Políticas y procedimientos de transferencia de información del estándar ISO 27001:2013.	
AUDITOR:	Miller Eduardo Hurtado Espitia Dana Valentina Lozada Cortes

Tabla 9. Segundo Hallazgo

REVISIÓN TECNICA	NO CONFORMIDAD MAYOR _X_ MENOR
PROCESO REVISADO: Aulas virtuales	
ESTANDAR Y NUMERO DE ELEMENTO 27001:2013, A.9.3 Responsabilidad de usuarios	
HALLAZGO:	
Se evidencia que no existe en la Universidad ECCI una política de seguridad fuerte respecto al uso de las contraseñas, lo cual se evidencia en la tabulación de la información obtenida a través de la encuesta virtual, incumpliendo así el control A.9.1.1 Política de control de acceso y el control A.9.3.1 Uso de información secreta del estándar ISO 27001:2013	
AUDITOR:	Miller Eduardo Hurtado Espitia Dana Valentina Lozada Cortes

Tabla 10. Tercer Hallazgo

REVISIÓN TECNICA	NO CONFORMIDAD MAYOR _X_ MENOR
PROCESO REVISADO: Aulas virtuales	
ESTANDAR Y NUMERO DE ELEMENTO 27001:2013, A.9.3 Responsabilidad de usuarios	
HALLAZGO:	
Se evidencia que los usuarios de los sistemas de la Universidad ECCI pueden ser vulnerados haciendo una búsqueda en lugares públicos cercanos a la Universidad ECCI como cafés internet y esto puede llevar a que un ciberdelincuente logre obtener información privada del usuario, incumpliendo el control A.9.3.1 Uso de información secreta de la norma ISO 27001:2013.	
AUDITOR:	Miller Eduardo Hurtado Espitia Dana Valentina Lozada Cortes

Tabla 11. Cuarto Hallazgo

REVISIÓN TECNICA	OBSERVACIÓN
PROCESO REVISADO: Aulas virtuales	
ESTANDAR Y NUMERO DE ELEMENTO 27001:2013	
HALLAZGO:	
Según los análisis con las herramientas OSINT se evidencia que probablemente el proveedor de servicios de red de la Universidad ECCI es ETB, ya que al consultar la IP encontrada todos los resultados estaban dirigidos a esta empresa, en este caso se cree que la empresa ETB esta incumplido con el control A.15.1.1 Política de seguridad de la información para proveedores de la ISO 27001:2013, ya que está divulgado información de la Universidad.	
AUDITOR:	Miller Eduardo Hurtado Espitia Dana Valentina Lozada Cortes

Tabla 12. Quinto Hallazgo

REVISIÓN TECNICA	NO CONFORMIDAD MAYOR __ MENOR _X_
PROCESO REVISADO: Aulas virtuales	
ESTANDAR Y NUMERO DE ELEMENTO: 27001:2013, A.5.1 Orientación de la dirección para la gestión de SI.	

HALLAZGO:	
No se evidencia que la página de Aulas Virtuales tenga un control total de la información que se maneja, lo cual facilita que una persona tenga acceso a información importante, como lo fue el nombre de los profesor tanto de Medellín como de Bogotá y las materias que dictaban, incumplido de esta forma el control A5.1.1 Políticas para la SI de la norma ISO 27001:2013	
AUDITOR:	Miller Eduardo Hurtado Espitia Dana Valentina Lozada Cortes

8.5 Acciones de Mejora

- Según los hallazgos encontrados durante la investigación, lo primero que se debería hacer es exigir a los estudiantes cambiar la contraseña de sus plataformas una vez sea entregadas o que sea la mismo persona la que cree la cuenta para no tener ese tipo de inconvenientes.
- Otra de la cosas que deberían hacer la Universidad es realizar campañas de concientización de entregar la información tanto a los estudiantes como los docentes mostrándoles métodos y tácticas en las cuales una persona X obtiene información personal o sensibles, como también las estadísticas encontradas para que entiendan el grado de importancia, así mismo mostrarles la importancia de eliminar archivos cada vez que entren a un lugar público enseñándoles que esa podría ser una huella para obtener información más información
- La Universidad debería establecer políticas de seguridad virtuales al momento de manejar la información como, por ejemplo, no publicar datos de los profesores mientras que no estén seguros que la plataforma es completamente segura.
- La Universidad debería pensar en implementar un SGSI (Sistema de Gestión de la Información), para la protección y manejo de datos de toda la comunidad, sería aún más

importante teniendo en cuenta el crecimiento que está teniendo, por otro lado, también tener en cuenta los resultados obtenidos durante esta revisión técnica.

Capítulo 9. Fuentes

A continuación, se citan las múltiples fuentes que fueron consultadas durante el desarrollo de este proyecto, las cuales por su relevancia aportaron de una forma notoria a lo que fue el levantamiento de información de una manera correcta, para así poder alinear las diferentes fases del proyecto presentado y poder suplir la necesidad de nuestro cliente interno en la firma.

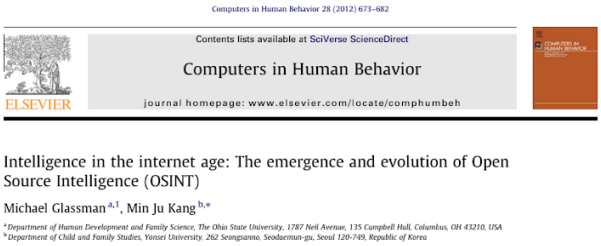
9.1 Fuentes Primarias

9.1.1 OSINT

Ilustración 18. Que es OSINT

Fuente: (Papeles de inteligencia, 2020)

Ilustración 19. Articulo OSINT

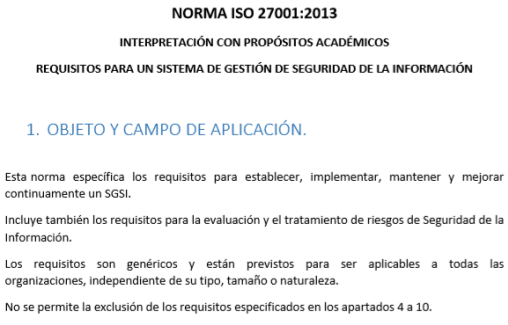


Fuente: (Michael Glassman, 2012)

Ilustración 20. OSINT

Fuente: Los Autores 2020

Ilustración 21.SGSI



Fuente: Los Autores 2020

9.1.2 Listado de herramientas OSINT

Ilustración 22. Lista de Herramientas OSINT

Fuente: (Pastorino, 2019)

Ilustración 23.Lista de Herramientas OSINT 2

Fuente: (J3ss3SHL, 2018)

Ilustración 24. Fuentes OSINT

Fuente: (Corral, 2016)

Ilustración 25. Herramientas OSINT

Fuente: (Domouso, 2018)

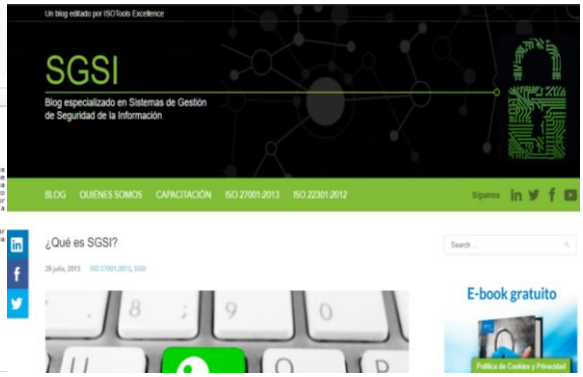
9.2 Fuentes Secundarias

9.2.1. Palabras técnicas del documento

Ilustración 26. Auditoría Técnica

Fuente: (mantenimientopetroquimica.com, s.f.)

Ilustración 27. SGSI Adicional

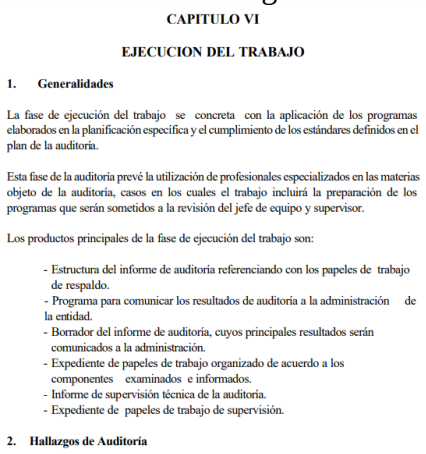


Fuente: (SGSI, 2015)

Ilustración 28. Ataque Cibernético

Fuente: (Carisio, s.f.)

Ilustración 29. Hallazgo



CAPITULO VI

EJECUCION DEL TRABAJO

1. Generalidades

La fase de ejecución del trabajo se concreta con la aplicación de los programas elaborados en la planificación específica y el cumplimiento de los estándares definidos en el plan de la auditoría.

Esta fase de la auditoría prevé la utilización de profesionales especializados en las materias objeto de la auditoría, casos en los cuales el trabajo incluirá la preparación de los programas que serán sometidos a la revisión del jefe de equipo y supervisor.

Los productos principales de la fase de ejecución del trabajo son:

- Estructura del informe de auditoría referenciando con los papeles de trabajo de respaldo.
- Programa para comunicar los resultados de auditoría a la administración de la entidad.
- Borrador del informe de auditoría, cuyos principales resultados serán comunicados a la administración.
- Expediente de papeles de trabajo organizado de acuerdo a los componentes examinados e informados.
- Informe de supervisión técnica de la auditoría.
- Expediente de papeles de trabajo de supervisión.

2. Hallazgos de Auditoría

Fuente: (Contraloria General del Estado, s.f.)

Ilustración 30. Incidente de Seguridad

Universidad Nacional de Luján

REPORTE DE INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN

Un incidente de seguridad de la información se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a la Política de Seguridad de la Información de la Universidad.

El reporte de los incidentes permite responder a los mismos en forma sistemática, minimizar su ocurrencia, facilitar una recuperación rápida y eficiente de las actividades minimizando la pérdida de información y la interrupción de los servicios, mejorar continuamente el marco de seguridad y el proceso de tratamiento de incidentes, y manejar correctamente los aspectos legales que pudieran surgir durante este proceso.

Al presentarse un fallo o incidente de seguridad de la información, por favor complete y presente este formulario, con la mayor cantidad de información posible, dentro de las 24 horas de detectado el incidente. Se solicitan algunos datos de tipo técnico que puede omitir si usted no los conoce.

Este reporte debe entregarse personalmente al Depto. de Seguridad Informática o enviarse mediante correo electrónico a la dirección seguridadinformatica@unlu.edu.ar
Por cualquier consulta puede comunicarse con el personal del Depto. de Seguridad Informática a los

Fuente: (Universidad Nacional de Luján, s.f.)

Ilustración 31. Riesgo

Fuente: (ciifen, s.f.)

9.2.2 Leyes

Ilustración 32. Ley 1581 del 2012

MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO

DECRETO NÚMERO 1377 DE 2013

(27 JUN 2013

"Por el cual se reglamenta parcialmente la Ley 1581 de 2012"

EL PRESIDENTE DE LA REPÚBLICA DE COLOMBIA

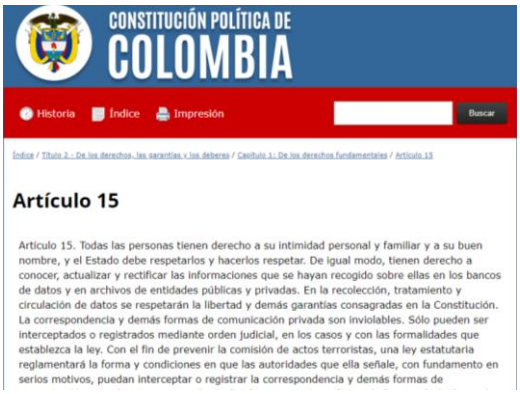
En uso de sus atribuciones constitucionales, y en particular las previstas en el numeral 11 del artículo 189 de la Constitución Política y en la Ley 1581 de 2012 y,

CONSIDERANDO

Que mediante la Ley 1581 de 2012 se expidió el Régimen General de Protección de Datos Personales, el cual, de conformidad con su artículo 1, tiene por objeto *"(…) desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de*

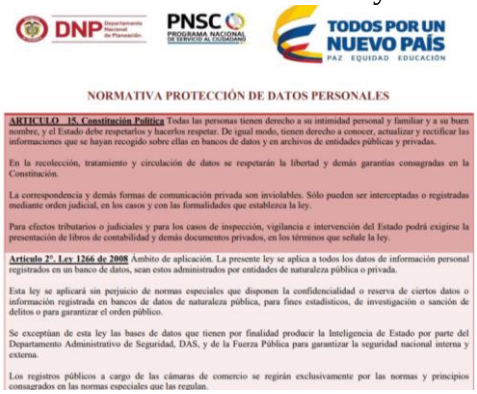
Fuente: (MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO, s.f.)

Ilustración 33. Articulo 15



Fuente: (constitucion colombia, 2020)

Ilustración 34. Resumen de Leyes



Fuente: (colaboracion.dnp, s.f.)

Ilustración 35. Controles Norma 27001:2013

ANEXO A.

OBJETIVOS DE CONTROL Y CONTROLES.

DOMINIO	CATEGORÍAS	CONTROLES
A.5 Política de seguridad de la información	A.5.1 Orientación de la dirección para la gestión de SI.	A5.1.1 Políticas para la SI
		A.5.1.2 Revisión de políticas para la SI.
A.6. Organización de la SI	A.6.1 Organización interna	A.6.1.1 SI: Roles y responsabilidades
		A.6.1.2 Separación de deberes
		A.6.1.3 Contacto con las autoridades
		A.6.1.4. Contacto con grupos de interés especial
		A.6.1.5. SI en la gestión de proyecto
	A.6.2 Dispositivos móviles y teletrabajo	A.6.2.1 Política para dispositivos móviles
		A.6.2.2 Teletrabajo
A.7 Seguridad de los recursos humanos	A.7.1 Antes de asumir el empleo	A.7.1.1. Selección
		A .7.1.2 Términos y condiciones del empleo
	A.7.2 Durante la ejecución del empleo	A.7.2.1 Responsabilidades de la dirección.
		A.7.2.2 Toma de conciencia, educación y formación en la SI
		A.7.2.3 Proceso disciplinario
A.8. Gestión de activos	A.8.1 Responsabilidad de los activos	A.8.1.1. Inventario de activos
		A.8.1.2 Propiedad de los activos
		A.8.1.3 Uso aceptable de los activos

Fuente: (NORMA ISO 27001:2013)

Capítulo 10. Recursos

A continuación, se listan los recursos necesarios, para llevar a cabo el desarrollo del proyecto.

10.1 Recursos Humanos

- Miller Eduardo Hurtado Espitia
- Danna Valentina Lozada Cortes

10.2 Recursos Físicos

- Computador portátil
- Papel
- Esferos
- Herramientas OSINTs
- Material fotocopiado para las encuestas

Capítulo 11. Cronograma de Actividades

En este capítulo se va a representar el cronograma de actividades donde están plasmadas las actividades completas a realizar del sistema de información:

Tabla 13. Cronograma

Numero de meses / actividades	1	2	3	4	5	6	7	8
1. Desarrollo del anteproyecto								
2. Evaluación de herramientas OSINT								
3. Definición de los objetivos y elementos de la revisión.								
4. Uso de herramientas OSINT para la realización de la revisión.								
5. Evaluación y análisis de los resultados								
6. Clasificación de Hallazgos								
7. Recomendaciones de acciones correctivas a los sistemas de información (ARCA y Aulas virtuales)								

Fuente: Los Autores 2020

Bibliografía

avast. (s.f.). Obtenido de ingenieria social: https://www.avast.com/es-es/c-social-engineering

ayudaleyprotecciondatos. (10 de septiembre de 2018). Obtenido de suplantacion de identidad : https://ayudaleyprotecciondatos.es/2018/09/10/suplantacion-identidad/

Carisio, E. (s.f.). *mdcloud*. Obtenido de Media Cloud: https://blog.mdcloud.es/ataque-cibernetico-consecuencias-como-actuar-y-como-protegerse/

ciifen. (s.f.). Obtenido de Aproximación para el cálculo de riesgo: http://www.ciifen.org/index.php?option=com_content&view=category&layout=blog&id=84&Itemid=336&lang=es

colaboracion.dnp. (s.f.). Obtenido de NORMATIVA PROTECCIÓN DE DATOS PERSONALES: https://colaboracion.dnp.gov.co/CDT/Programa%20Nacional%20del%20Servicio%20al%20Ciudadano/NORMATIVA%20PROTECCIÓN%20DE%20DATOS%20PERSONALES.pdf

constitucion colombia. (20 de 01 de 2020). Obtenido de constitucion colombia: http://www.constitucioncolombia.com/titulo-2/capitulo-1/articulo-15

Contraloria General del Estado. (s.f.). Obtenido de EJECUCION DEL TRABAJO: https://www.contraloria.gob.ec/documentos/normatividad/MGAG-Cap-VI.pdf

Corral, Y. (05 de mayo de 2016). *Yolanda Corral*. Obtenido de Yolanda Corral : https://www.yolandacorral.com/que-es-osint-fases-fuentes-herramientas/

Domouso, F. C. (08 de Agosto de 2018). *open webinars*. Obtenido de open webinars: https://openwebinars.net/blog/herramientas-osint/

GL, J. (Diciembre de 2019). *CiberPatrulla*. Obtenido de https://ciberpatrulla.com/que-es-osint/

infodf. (s.f.). Obtenido de que son los datos personales: http://www.infodf.org.mx/index.php/protege-tus-datos-personales/¿qué-son-los-datos-personales.html

J3ss3SHL. (20 de Abril de 2018). *security hack labs*. Obtenido de security hack labs: https://securityhacklabs.net/articulo/osint-herramientas-de-codigo-abierto-de-inteligencia

Jeison, C. y. (s.f.). *blogdelacalidad*. Obtenido de ¿Qué es No Conformidad?: https://blogdelacalidad.com/que-es-no-conformidad/

mantenimientopetroquimica.com. (s.f.). Obtenido de Auditoria Tecnica: http://www.mantenimientopetroquimica.com/auditoriastecnicas.html

Michael Glassman, M. J. (2012). Computers in Human Behavior. *ELSEIVER*, 10.

MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO. (s.f.). Obtenido de MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO: https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf

NORMA ISO 27001:2013. (s.f.). Obtenido de INTERPRETACIÓN CON PROPÓSITOS ACADÉMICOS.

Papeles de inteligencia. (2020). Obtenido de Papeles de inteligancia: https://papelesdeinteligencia.com/que-son-fuentes-de-informacion-osint/

papelesdeinteligencia.com. (s.f.). Obtenido de papelesdeinteligencia.com: https://papelesdeinteligencia.com/que-son-fuentes-de-informacion-osint/

Pastorino, C. (07 de Octubre de 2019). *we live security*. Obtenido de we live security: https://www.welivesecurity.com/la-es/2019/10/07/tecnicas-herramientas-osint-investigacion-internet/

SGSI. (28 de Julio de 2015). Obtenido de pmg-ssi: https://www.pmg-ssi.com/2015/07/que-es-sgsi/

significados.com. (25 de Julio de 2017). Obtenido de Software libre: https://www.significados.com/software-libre/

Universidad Nacional de Luján. (s.f.). Obtenido de REPORTE DE INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: http://www.unlu.edu.ar/doc/seginfo/Como_reportar_un_incidente_de_SI.pdf

Wikipedia. (s.f.). Obtenido de Información sensible: https://es.wikipedia.org/wiki/Información_sensible

Conclusiones

El desarrollo del proyecto tiene como fin hacer una revisión técnica a la plataforma de Aulas Virtuales de la Universidad ECCI por medio de herramientas OSINT y poder implementar nuevos temas en el Semillero SIRSEG. Durante el desarrollo del proyecto se utilizaron diferentes métodos para obtener información que ayudara a determinar qué tan segura era la plataforma, cumpliendo con los objetivos establecidos desde el principio, los resultados que se encontraron se puede determinar que la universidad debería implementar un SGSI (Sistema de Gestión de Seguridad de la Información), con esto poder prevenir posibles ataques cibernéticos que pueden llegar al robo de la información, publicación de información personal y sensible, falsificación de los datos, suplantación de identidad, etc.

Con este proyecto también se desea que a futuro otros compañeros continúen con la investigación, o saquen nuevos proyectos con los temas vistos durante la investigación como, por ejemplo, crear una aplicación que obtenga información de internet, realizar y auditar para implementar la ISO 27001:2013 en la Universidad ECCI, etc. Todo esto con el fin de mejorar la seguridad de los sistemas.