
**UNIVERSIDAD TÉCNICA DE AMBATO**

**FACULTAD DE TECNOLOGÍAS DE LA INFORMACIÓN, TELECOMUNICACIONES E INDUSTRIAL**

**CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS**

**Tema**:

# ANÁLISIS DE RIESGOS INFORMÁTICOS APLICANDO LA METODOLOGÍA OSSTMM PARA LA FUNDACIÓN CULTURAL Y EDUCATIVA AMBATO (UNIDAD EDUCATIVA ATENAS)

Trabajo de Graduación. Modalidad: Proyecto de Investigación, presentado previo la obtención del título de Ingeniero en Sistemas Computacionales e Informáticos.

**AREA:** Administrativas Informáticas

**LÍNEA DE INVESTIGACIÓN:** Auditorías Informáticas

**AUTOR**: Marcelo David Velasco Trujillo

**TUTOR:** Ing. David Omar Guevara Aulestia Mg.

Ambato - Ecuador

Octubre 2020

## APROBACIÓN DEL TUTOR

En mi calidad de Tutor del Trabajo de Investigación sobre el tema: "ANÁLISIS DE RIESGOS INFORMÁTICOS APLICANDO LA METODOLOGÍA OSSTMM PARA LA FUNDACIÓN CULTURAL Y EDUCATIVA AMBATO (UNIDAD EDUCATIVA ATENAS)", desarrollado bajo la modalidad Proyecto de Investigación por el señor Marcelo David Velasco Trujillo, estudiante de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, me permito indicar que el estudiante ha sido tutorado durante todo el desarrollo del trabajo hasta su conclusión, de acuerdo a lo dispuesto en el Artículo 15 del Reglamento para obtener el Título de Tercer Nivel, de Grado de la Universidad Técnica de Ambato, y el numeral 7.4 del respectivo instructivo

Ambato, Octubre 2020

EL TUTOR

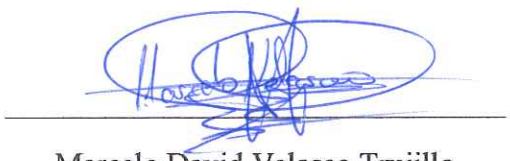
Firmado electrónicamente por:
DAVID OMAR
GUEVARA
AULESTIA

Ing. David Omar Guevara Aulestia Mg.

## AUTORÍA

El presente trabajo de investigación titulado: "ANÁLISIS DE RIESGOS INFORMÁTICOS APLICANDO LA METODOLOGÍA OSSTMM PARA LA FUNDACIÓN CULTURAL Y EDUCATIVA AMBATO (UNIDAD EDUCATIVA ATENAS)", es absolutamente original, auténtico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, Octubre 2020



Marcelo David Velasco Trujillo

CC: 1804874079

## APROBACIÓN DE LA COMISIÓN CALIFICADORA

La Comisión Calificadora del presente trabajo conformada por los señores docentes PHD. Félix Fernández e Ing. Hernando Buenaño, revisó y aprobó el Informe Final del Proyecto de investigación titulado "ANÁLISIS DE RIESGOS INFORMÁTICOS APLICANDO LA METODOLOGÍA OSSTMM PARA LA FUNDACIÓN CULTURAL Y EDUCATIVA AMBATO (UNIDAD EDUCATIVA ATENAS)", presentado por el señor Marcelo David Velasco Trujillo, nos permitimos informar que el trabajo ha sido revisado y calificado de acuerdo al Artículo 17 del Reglamento para obtener el Título de Tercer Nivel, de Grado de la Universidad Técnica de Ambato, y al numeral 7.6 del respectivo instructivo. Para cuya constancia suscribimos, conjuntamente con la señora Presidenta del Tribunal.


Ing. Elsa Pilar Urrutia, Mg.
PRESIDENTA DEL TRIBUNAL


PhD. Ing. Félix Fernández, Mg
DOCENTE CALIFICADOR

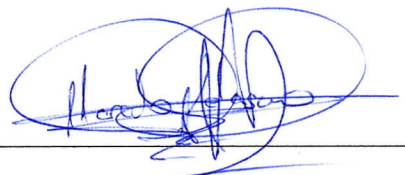

Ing. Hernando Buenaño, Mg.
DOCENTE CALIFICADOR

## DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga uso de este Trabajo de Titulación como un documento disponible para la lectura, consulta y procesos de investigación.

Cedo los derechos de mi Trabajo de Titulación en favor de la Universidad Técnica de Ambato, con fines de difusión pública. Además, autorizo su reproducción total o parcial dentro de las regulaciones de la institución.

Ambato, Octubre 2020



Marcelo David Velasco Trujillo

CC: 1804874079

AUTOR

## DEDICATORIA:

*El presente trabajo y dedicación lo entrego en primer lugar a Dios por haberme guiado y bendecido en este largo camino. A mi Madre Mirian que con sus enseñanzas y la confianza que me ha brindado, han sido un gran impulso para salir adelante en momentos difíciles; a mi hermana menor que siempre ha estado a mi lado por el amor y las fortalezas a pesar de las diferencias.*

*A mi familia que amo mucho y respeto, en especial a mi tía Esther por ser esa madre, que comparte una gran responsabilidad ante momentos de dolor, por apoyarme al momento de tomar decisiones.*

*A mis amigos y compañeros con los cuales compartimos buenas y malas anécdotas, finalmente dedico cada esfuerzo de mi vida a mí mismo, porque no me he rendido hasta alcanzar los objetivos y metas que me he propuesto, afrontar las adversidades siendo constante y perseverar hasta cumplir todo lo que me propuse en este largo camino de mi vida.*

*Marcelo David Velasco Trujillo*

## AGRADECIMIENTO:

*Muy agradecido con Dios por darme la fortaleza, paciencia y sabiduría para afrontar las cosas, pese a las dificultades.*

*Gracias a mi madre Mirian por el apoyo incondicional, los valores y consejos que me supo enseñar durante mi vida, a mi hermana y amigos que de alguna manera aportaron para hacer esto posible, a la Facultad de Tecnologías de la Información, Telecomunicaciones e Industrial de la Universidad Técnica de Ambato y en especial a sus docentes por compartir sus experiencias y conocimiento los cuales me permitirán tener una superación en el ámbito profesional.*

*A mi tutor de Tesis, ing. David Guevara, quien supo guiarme durante las fases que duro la realización del presente trabajo,*

*A la Fundación Cultural y Educativa Ambato (Unidad Educativa Atenas) quienes supieron brindarme la ayuda necesaria al momento de desarrollar mi tesis.*

*Marcelo David Velasco Trujillo*

**ÍNDICE**

## ÍNDICE DE TABLAS

## ÍNDICE DE FIGURAS

**ANEXOS**

## RESUMEN EJECUTIVO

El presente proyecto de titulación tiene como finalidad realizar un análisis de riesgos informáticos aplicando la metodología OSTTMM para la Fundación Cultural y Educativa Ambato (Unidad Educativa Atenas), el cual tiene como objetivo evitar la divulgación de información y detectar posibles vulnerabilidades que intervienen en un sistema informático los cuales se ven afectados por amenazas y ataques.

El desconocimiento de los elementos que pueden perjudicar a un sistema informático, puede evitar dar la importancia necesaria a la seguridad informática que se debe tomar en cuenta cuando el personal trabaja directamente con un computador o con la información que maneje.

Como resultado de la información obtenida con las técnicas utilizadas se pudo observar que la institución no contaba con una metodología que ayude a detectar vulnerabilidades, de esta manera, por medio del estudio y la utilización de métodos de testeo y análisis de la seguridad informática, se determinó que la metodología OSSTMM cuenta con fases y módulos los cuales hacen posibles la realización de este trabajo, también se aplicó ingeniería social la cual es enfocada a vulnerar el factor humano, todo esto para determinar las vulnerabilidades existen y de esta manera poder realizar un plan de seguridad informática el cual ayude a reducir de manera considerada los riesgos encontrados.

## ABSTRACT

The purpose of this degree project is to perform an analysis of computer risks by applying the OSTTMM methodology for the Ambato Cultural and Educational Foundation (Athens Education Unit), which aims to prevent the dissemination of information and detect possible vulnerabilities involved in a system computer science which are affected by challenges and attacks.

The ignorance of the elements that can harm a computer system, can avoid giving the necessary importance to the computer security that must be taken into account when staff work directly with a computer or with the information it manages.

As a result of the information obtained with the techniques used we could observe that the institution did not have a methodology that helps to detect vulnerabilities, in this way, through the study and the use of test methods and computer security analysis, it was determined that the OSSTMM methodology has phases and modules which make it possible to carry out this work, social engineering was also applied which is focused on violating the human factor, all this to determine the vulnerabilities exist and in this way to be able to carry out a plan of computer security which helps to reduce the risks encountered in a considerable way.

# CAPITULO I

# MARCO TEÓRICO

## 1.1. Antecedentes Investigativos

La presente investigación está basada en los siguientes antecedentes investigativos obtenidos de la revisión bibliográfica de repositorios digitales:

Según el trabajo de investigación de Diana Carolina Pacheco Pozo en 2016 titulado "Propuesta de un plan de contingencia de TI para la empresa LOGICIEL" establecido con la intención de desarrollar un modelo basado en marcos de referencia enfocados en la continuidad del negocio para la empresa LOGICIEL que consta de un análisis comparativo de marcos de referencia para poder determinar las principales etapas del proceso de planeación y de contingencias mediante la evaluación de riesgos, en el cual se establece un modelo que explica en detalle cada una de las etapas que conforman el proceso de elaboración de un plan de contingencias de una manera sencilla y fácil de entender que cualquier empresa podría poner en práctica, incluyendo la validación del modelo propuesto [1].

Según el trabajo de investigación de Carolina Anabel Bonilla Vaca en 2017 titulado "Elaboración de una metodología de detección y mitigación de vulnerabilidades de base de datos y su incidencia en la seguridad de la información de la empresa Automekano cía. ltda., de la ciudad de Ambato" concluye que existen muchas razones para aplicar la metodología propuesta, ya que se describe el proceso secuencial que permite realizar etapa por etapa las tareas necesarias para el análisis, búsqueda y detección de vulnerabilidades, además presenta ejemplos que guiarán al investigador en la presentación de los análisis de lo obtenido, así como en la presentación de los informes de mitigación. La metodología hace posible demostrar las vulnerabilidades de la base de datos, sino que también permite al investigador analizar la información encontrada para emitir las recomendaciones de prevención y mitigación a la empresa, con lo que se podrá brindar un trabajo de investigación que será un aporte valioso para la misma [2].

Según el trabajo de investigación de Yolanda de la Nube Cruz Gavilánez en 2016 titulado "Metodología OSSTMM para la detección de errores de seguridad y vulnerabilidad en sistemas operativos de 64 bits a nivel de usuario final" concluye que en la investigación los usuarios finales a los que se realizaron la prueba no tienen conocimientos básicos de seguridad en los sistemas operativos ya que en su mayor parte es personal administrativo y no técnico, por lo que exponen sus equipos a vulnerabilidades informáticas. La metodología ocupada pone a prueba la seguridad que le dan los usuarios a sus sistemas operativos y observar si resistirán a un ataque [3].

## 1.2.Objetivos

### 1.2.1. General

- Analizar el plan de seguridad informático aplicando la metodología OSSTMM para determinar y gestionar los posibles riesgos informáticos que se encontrarán en la Fundación Cultural y Educativa Ambato (UNIDAD EDUCATIVA ATENAS) para mejorar la confidencialidad, integridad y disponibilidad de la información.

### 1.2.2. Específicos

- Determinar los elementos más importantes de la metodología OSSTMM que se aplicará para realizar el análisis de riesgos en la Fundación Cultural y Educativa Ambato (UNIDAD EDUCATIVA ATENAS).
- Realizar un análisis de riesgos, para determinar las amenazas y vulnerabilidades de los activos de información, permitiendo realizar la valoración de cada uno.
- Proponer un plan de seguridad informática que permitirá tener una guía de procedimientos de Seguridad Informática, y recomendar las medidas necesarias y selección de controles para conocer, prevenir, impedir, reducir o controlar los riesgos encontrados.

# CAPITULO II

# METODOLOGÍA

## 2.1. Materiales

El presente proyecto de investigación se desarrolla bajo la metodología de investigación aplicada porque se obtiene información y se la procesa para realizar un análisis de riesgos informáticos, utilizando a su vez una investigación de campo debido a que se lleva a cabo dentro de las instalaciones de la Institución Educativa Atenas.

Para el presente proyecto de investigación se utilizará fundamentación teórica y legal según Normativa de Seguridad Informática en Ecuador.

### SISTEMAS DE INFORMACIÓN

Son conjuntos de activos informáticos y recursos humanos relacionados entre sí, con el objetivo de satisfacer los requerimientos de información para las organizaciones y ayudar así en la toma de decisiones y gestión [4].

### ¿QUÉ ES LA SEGURIDAD?

Se entiende que es un estado o una característica que denota el correcto comportamiento, que se encuentre protegido ante amenazas, libre de peligro o daño de un sistema.

Seguridad de la información "Es un conjunto de medidas de prevención, detección y corrección, orientadas a proteger la confidencialidad, la integridad y la disponibilidad de los recursos informáticos" [5].

En cambio, para Santos C. consiste en "Asegurar que los recursos del sistema de información de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida solo sea posible a las personas que se encuentren acreditadas" [6].

## SEGURIDAD INFORMÁTICA.

Es la disciplina que se encarga de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable.

## SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información es una disciplina que se encarga de la integridad, disponibilidad, control y autenticidad de la información generada y custodiada en diferentes medios informáticos tangibles e intangibles de una empresa u organización, los cuales no deben estar dañados o alterados por circunstancias o factores tanto internos como externos. Además, faculta a los usuarios para hacer un correcto uso de los medios a su disposición.

## DEFINICIÓN DEL RIESGO

El riesgo se ha definido como la posibilidad de que se produzca un impacto dado en la organización, es toda aquella eventualidad que imposibilita el cumplimiento de un objetivo. De manera cuantitativa el riesgo es una medida de las posibilidades de incumplimiento o exceso del objetivo planteado. Así definido, un riesgo conlleva dos consecuencias: ganancias o pérdidas [7].

En lo relacionado con tecnología, generalmente el riesgo se plantea solamente como amenaza, determinado el grado de exposición a la ocurrencia de una pérdida (por ejemplo, el riesgo de perder datos debido a rotura de disco, virus informáticos, etc.).

## ANÁLISIS DE RIEGOS INFORMÁTICOS

El análisis de riesgos es una piedra angular de los procesos de evaluación, certificación, auditoria y acreditación que formalizan la confianza que merece un sistema de información.

Dado que no hay dos sistemas de información iguales, la evaluación de cada sistema concreto requiere amoldarse a los componentes que lo constituyen. En análisis de riesgos proporciona una visión singular de cómo es cada sistema, que valor posee, a que amenazas está expuesto y de que protecciones se ha dotado [8].

## METODOLOGÍAS DE ANÁLISIS DE RIESGOS

A nivel empresarial existen múltiples metodologías para la gestión y análisis de los riesgos en la información, para lo cual ocupamos la metodología OSSTMM ya que nos permite un análisis de vulnerabilidades completo tanto a nivel informático como a nivel de personal.

## OSSTMM

El OSSTMM fue creado por Peter Herzog de la organización ISECOM en diciembre del año 2000, es único y el más extenso estándar certificado disponible para el desarrollo de pruebas de Seguridad en Sistemas de Internet y Redes.

Esta se divide en cinco secciones o ambientes, las que permitirán identificar y enfocar los errores que tienen los sistemas operativos y tomar medidas para evitar posibles inconvenientes. Esta metodología abierta de testeo de seguridad OSSTMM se relaciona directamente con la identificación de errores y vulnerabilidades, además propone en cada sección la ejecución de unas tareas con el fin de encontrar la existencia de problemas que afecten en gran medida la seguridad de una organización o entidad educativa [9].

Esta metodología evalúa la seguridad desde todos los puntos de vista:

- Humano
- Físico
- Wireless
- Telecomunicaciones
- Redes de Datos

En el proceso de un análisis de seguridad, se concentra en evaluar varias áreas de seguridad, que reflejan los niveles de seguridad presentes. Estos son conocidos como las Dimensiones de Seguridad [10]:

### VISIBILIDAD

La visibilidad es lo que puede verse, registrarse, o monitorearse en el nivel de seguridad con o sin la ayuda de dispositivos electrónicos. Esto incluye, pero no se

limita a, ondas de radio, luz por encima del espectro visible, dispositivos de comunicación como teléfonos, GSM, email y paquetes de red como TCP/IP.

**ACCESO**

El acceso es el punto de entrada al nivel de seguridad. Un punto de acceso no requiere ser una barrera física. Esto puede incluir, pero no se limita a, una página web, una ventana, una conexión de red, ondas de radio, o cualquier cosa cuya ubicación soporte la definición de casi-público o donde un computador interactúa con otro por medio de una red. Limitar el acceso significa negar todo excepto lo que este expresamente permitido financieramente y por buenas prácticas [10].

**CONFIANZA**

La confianza es una ruta especializada en relación con el nivel de seguridad. La confianza incluye la clase y cantidad de autenticación, no-repudio, control de acceso, contabilización, confidencialidad e integridad entre dos o más factores dentro del nivel de seguridad.

**AUTENTICACIÓN**

La autenticación es la medida por la cual cada interacción en el proceso está privilegiada.

**NO-REPUDIO**

El no-repudio provee garantía que ninguna persona o sistema responsable de la interacción pueda negar envolvimiento en la misma.

**CONFIDENCIALIDAD**

La confidencialidad es la certeza que únicamente los sistemas o partes involucradas en la comunicación de un proceso tengan acceso a la información privilegiada del mismo.

**PRIVACIDAD**

La privacidad implica que el proceso es conocido únicamente por los sistemas o partes involucradas.

## AUTORIZACIÓN

La autorización es la certeza que el proceso tiene una razón o justificación de negocios y es administrado responsablemente dando acceso permitido a los sistemas.

## INTEGRIDAD

La integridad es la certeza que el proceso tiene finalidad y que no puede ser cambiado, continuado, redirigido o reversado sin el conocimiento de los sistemas o partes involucradas.

## SEGURIDAD

La seguridad son los medios por los cuales un proceso no puede dañar otros sistemas, o procesos incluso en caso de falla total del mismo [10].

## FUNDAMENTACIÓN TEÓRICA

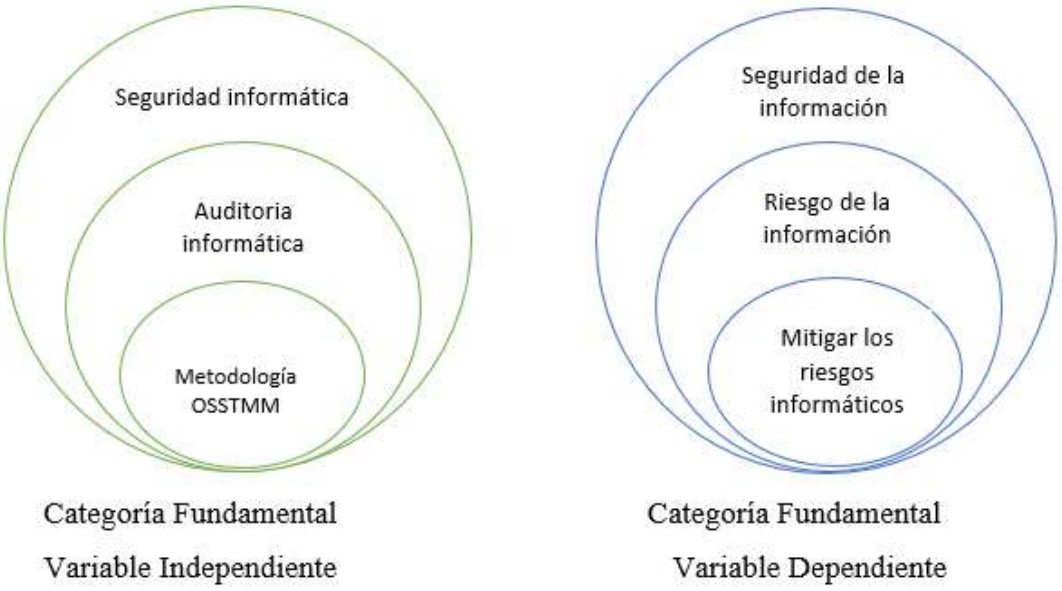



**Fig. 1.** Categorías de variables
**Fuente:** Elaborado por el Investigador

## FUNDAMENTACIÓN LEGAL

Normativa de seguridad informática en Ecuador

"mediante Acuerdos Ministeriales Nos. 804 y 837 de 29 de julio y 19 de agosto de 2011, respectivamente, la Secretaría Nacional de la Administración Pública creó la

Comisión para la Seguridad Informática y de las Tecnologías de la Información y Comunicación conformada por delegados del Ministerio de Telecomunicaciones y de la Sociedad de la Información, la Secretaría Nacional de Inteligencia y la Secretaría Nacional de la Administración Pública y dentro de sus atribuciones tiene la de establecer lineamientos de seguridad informática, protección de infraestructura computacional y todo lo relacionado con ésta, incluyendo la información contenida para las entidades de la Administración Pública Central e Institucional" [11].

Las Tecnologías de la Información y Comunicación son herramientas imprescindibles para el cumplimiento de la gestión institucional de cualquier entidad pública, por lo que deben cumplir con estándares de seguridad para garantizar la confidencialidad, integridad y disponibilidad de la información.

## 2.2. Métodos

El presente proyecto de titulación se basa en una investigación documentada y bibliográfica la cual usa documentación investigativa referenciada en temas similares, proporcionando información necesaria y útil para el desarrollo del proyecto.

El trabajo de investigación consiste en conocer a profundidad la problemática que se suscita en los procesos de recaudación por la ausencia de auditorías informáticas, en las siguientes modalidades:

### Modalidad de la Investigación

La presente investigación es de tipo aplicada ya que se buscó la aplicación y utilización de conocimientos adquiridos durante la formación profesional para dar una solución práctica a los problemas relacionados con la seguridad de la información, con la finalidad de optimizar y mejorar el uso de la información de la Fundación Cultural y Educativa Ambato (UNIDAD EDUCATIVA ATENAS).

### Modalidad de Campo

La presente investigación es de campo porque se lleva a cabo sistemáticamente el estudio en el lugar donde se generó el problema mediante alternativas de solución que permita el adecuado control de la información de la "Fundación Cultural y Educativa Ambato (UNIDAD EDUCATIVA ATENAS)", para lo cual se hace visitas continuas

a la institución con el objetivo de identificar sus actividades y obtener información necesaria para adquirir y manejar datos que permitan desarrollar la propuesta planteada.

**Modalidad aplicada**

Se utiliza la investigación aplicada ya que se procederá a seguir los pasos necesarios para poder aplicar correctamente la metodología que se escogerá para este proyecto.

**Modalidad Bibliográfica o Documentada:**

Se considera la modalidad de la investigación bibliográfica porque es necesario detectar, ampliar y profundizar mediante teorías, conceptualizaciones y criterios de diversos autores la seguridad de la información, apoyándose de fuentes confiables como libros, documentos y publicaciones científicas que aporten el conocimiento requerido para poder alcanzar una adecuada solución del problema.

**Modalidad Descriptiva**

Mediante la obtención de los datos obtenidos y verificados a través de encuestas, aplicaciones de métodos de obtención de información. Se procederá a la interpretación de resultados los cuales nos ayudaran a resolver la problemática expuesta.

## 2.3. Población y muestra

Según las características del proyecto y lo que se propuso realizar no fue necesaria una población, debido a que investigador recolectó la información directamente en la Institución Educativa Atenas tomando en cuenta la verificación de los resultados.

## 2.4. Recolección de información

**Plan de Recolección de Información**

La técnica utilizada para recolectar la información son las encuestas usando la guía de entrevista como instrumento. Estos datos permitieron un mejor análisis de la información que se requirió para el desarrollo del proyecto. Por otra parte, se acudirá a la de la Fundación Cultural y Educativa Ambato (UNIDAD EDUCATIVA ATENAS)", para proponer la metodología que más se ajusta a esta investigación

tomando en cuenta levantamientos previos de riesgos de la información obtenidos en la entrevista. Se realizará el análisis siguiendo la metodología propuesta.

### 2.5. Procesamiento y análisis de datos

Una vez obtenida la información se procede a realizar los siguientes pasos:

- Revisión de la información recopilada.
- Análisis estadístico de datos, gráficas, u otras operaciones en los datos de forma apropiada.
- Selección de alternativas para dar solución al problema planteado.
- Análisis e interpretación de los resultados.

### Plan de análisis e interpretación de resultados

El análisis de los resultados se realizará desde el punto de vista descriptivo y estadístico, proceso que permite realizar la interpretación adecuada basada en el marco teórico, relacionado las variables de la investigación y la propuesta lo que servirá para establecer las conclusiones y recomendaciones.

### 2.6. Desarrollo del proyecto

- Estudio de la situación actual en la seguridad de la institución educativa y las políticas de seguridad que posee.
- Análisis de la metodología que se ocupará (OSSTMM)
- Aplicación de técnicas de recolección en el departamento de sistemas.
- Aspectos organizativos de la seguridad de la información.
- Identificar recursos tecnológicos, aplicaciones y consumo de servicios.
- Análisis de la seguridad de la institución.
- Realización de informes y soluciones prácticas orientadas en resolver los problemas de seguridad informática que se presenten en la unidad educativa.
- Proponer el plan de seguridad informática para la Fundación Cultural y Educativa Ambato (UNIDAD EDUCATIVA ATENAS).

# CAPITULO III

# RESULTADOS Y DISCUSIÓN

## 3.1. Propuesta Solución

Por medio del presente análisis de riesgos aplicando la metodología internacional OSTTMM para la Fundación Cultural y Educativa Ambato (Unidad Educativa Atenas) permitió obtener criterios de la seguridad de la información, con los cuales se generó recomendaciones las cuales serán interpretadas por los encargados del área de sistemas y de esta manera poder aumentar la confidencialidad y la seguridad de los datos, bridando mayor seguridad lógica de la red.

### 3.1.1. Análisis de la situación actual de la Institución Educativa

**Análisis de la situación actual de Fundación Cultural y Educativa Ambato (Unidad Educativa Atenas)**

La Fundación Cultural y Educativa Ambato fue creada en 1976 bajo la denominación de Sociedad, por un grupo de empresarios ambateños encabezados por el señor José Filometor Cuesta Holguín, con el fin de promover actividades culturales y educativas en la ciudad de Ambato, a través de un Centro Educativo que brindara el importante servicio de educar a la juventud ambateña, del Ecuador y el mundo. Desde aquel entonces se iniciaron las labores como "Centro Educativo Atenas" en las instalaciones del Colegio Pío X, donde funcionó hasta 1985

En 1997 el Centro Educativo Atenas pasa a formar parte del proyecto de Reforma Curricular del Bachillerato según Acuerdo Ministerial 1382 con el aval de la Universidad Andina Simón Bolívar. En el año 2005 cambia su denominación de Sociedad a Fundación Cultural y Educativa Ambato. Desde ese momento, y a pedido del señor José Filometor Cuesta Holguín, asume la presidencia de la Fundación, su hijo, licenciado José Filometor Cuesta Vásconez. En el mismo año, se realiza la primera Planificación Estratégica para definir la proyección institucional al 2015.

En el 2007 pasa a ser considerada como **UNIDAD EDUCATIVA** según resolución N° 074-DP-DPET emitido por la Dirección de Educación de Tungurahua. Actualmente la UEA es considerada una de las mejores instituciones del centro del

país, en donde se educan niños y jóvenes que serán los grandes empresarios de nuestra hermosa tierra [12].

#### 3.1.1.1. Misión

Crecemos y aprendamos juntos, fortaleciendo nuestros principios y valores, desarrollando las capacidades y habilidades de nuestra comunidad, de forma crítica y creativa para contribuir a un mundo mejor.

#### 3.1.1.2. Visión

Somos la Organización responsable de la formación de personas felices e íntegras, con conciencia social y capacidades para triunfar

#### 3.1.1.3. Valores Institucionales

- **Respeto:** Es un derecho inalienable de todo ser humano. Reconocemos nuestra individualidad y valoramos la de los demás.

- **Verdad:** Hablamos y actuamos de manera coherente con nuestra conciencia y nuestras convicciones personales, siendo auténticos y valientes.

- **Solidaridad:** Extendemos la mano voluntariamente a quien lo necesita, sintiendo como algo propio el sufrimiento de nuestro prójimo, permitiéndonos crecer como personas íntegras.

- **Responsabilidad:** Hacemos lo que tenemos que hacer en el momento oportuno, sin que nadie nos lo recuerde y se asumió las consecuencias de nuestras decisiones.

#### 3.1.1.4. Políticas de Seguridad y salud ocupacional

La fundación Cultural y Educativa Ambato dedicada a brindar educación, está comprometida con la seguridad y la salud ocupacional en todas las áreas de funcionamiento de la institución, respetando el medio ambiente, el marco legal y normativas establecidas en el país, para lo cual asignaremos los recursos necesarios y promover el mejoramiento continuo.

Educamos y formamos jóvenes competentes, responsables y de servicio.
Trabajamos para la satisfacción de nuestros clientes internos y externos mediante el cumplimiento de requisitos, la innovación de procesos, una organización efectiva, personal especializado y comprometido, una infraestructura adecuada y la participación de la familia.

### 3.1.1.5. Estructura Organizacional Descriptiva

El 19 de octubre de 1976 Creada como Sociedad Cultural y Educativa Ambato por un grupo de ambateños, presidida por el Sr. José Filometor Cuesta Holguín.
Octubre de 1976 inicia sus labores como Centro Educativo Atenas.
Los puestos directivos establecidos en el Organigrama Estructural son: directores, coordinadores de sistema de gestión de calidad, rector, vicerrector, directores de sección, coordinadores de área y docentes de la Fundación Cultural y Educativa Ambato (Unidad Educativa Atenas), mismos que serán reconocidos según políticas internas de la institución. A continuación, en la fig. 1 se muestra el organigrama estructural institucional.

**ORGANIGRAMA FUNDACIÓN CULTURAL Y EDUCATIVA AMBATO**

**UNIDAD EDUCATIVA ATENAS**

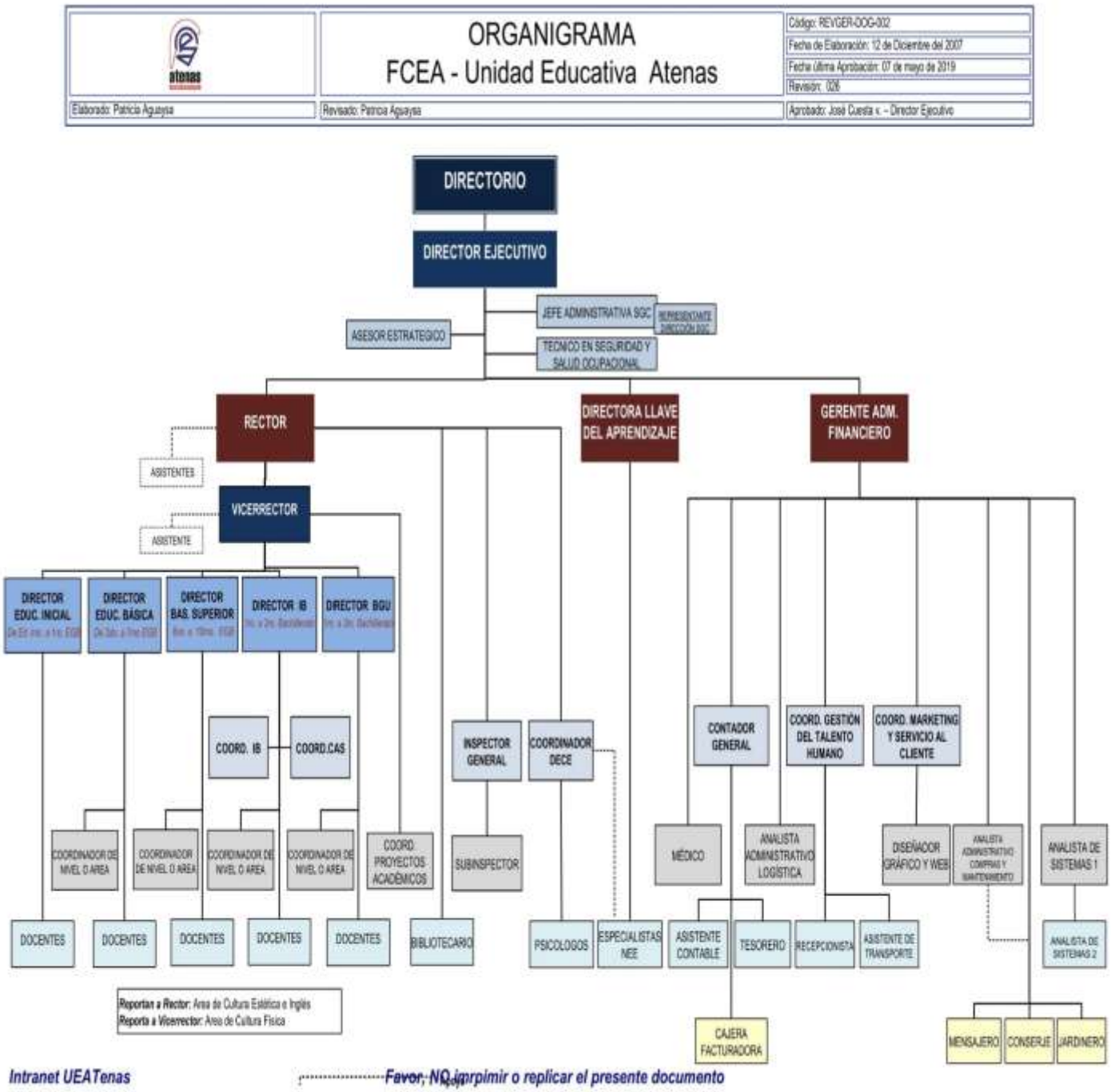



**Fig. 2.** Organigrama FCEA- Unidad Educativa Atenas
**Fuente:** Fundación Cultural y Educativa Ambato (Unidad Educativa Atenas)

### 3.1.2. Seguridad de la información

#### 3.1.2.1. Revisión de la Inteligencia Competitiva

Es la información que se recolecta a través de internet para poder analizarla mediante inteligencia de negocios. Utilizar IC en un Test de Intrusión da valor de negocio a los componentes y puede ayudar a encontrar justificaciones de negocio para implementar distintos servicios.

##### 3.1.2.1.1. Mapa y medida de la estructura de directorio de los servidores.

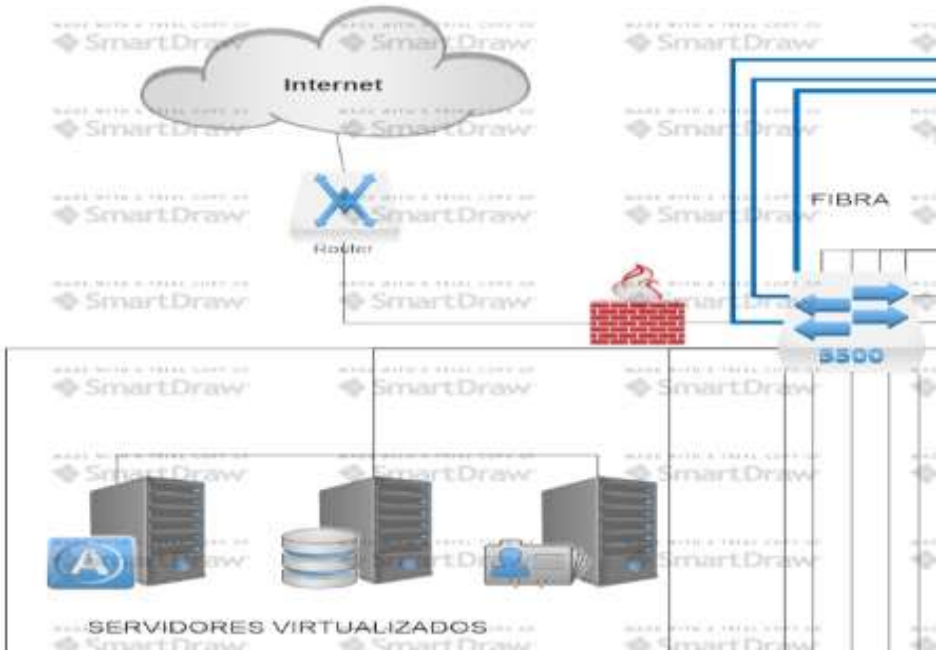



**Fig. 3.** Servidores FCEA- Unidad Educativa Atenas
**Fuente:** Elaborado por el Investigador

**Interpretación**

Al realizar esta investigación obtuvimos que la Unidad Educativa Atenas cuenta con servidores virtualizados los cuales son de: Active Directory, Base de Datos y Aplicaciones. Además, posee servidor de Facturación electrónica y servidor de biblioteca.

**Tabla 1. Descripción de los servidores de la Unidad Educativa Atenas**

| Tipo de servidor | IP | Descripción | Ubicación |
|---|---|---|---|
| VMWARE | [redacted] | Active Directory | Data Center |
| VMWARE | [redacted] | Aplicaciones | Data Center |
| VMWARE | [redacted] | Base de Datos | Data Center |

| | | | |
|---|---|---|---|
| | [redacted] | Facturación Electrónica | Data Center |
| | [redacted] | Biblioteca | Data Center |

**Fuente:** Departamento de Sistemas Unidad Educativa Atenas

#### 3.1.2.1.2. Determinar el costo de TI de la infraestructura de Internet basados en SO, Aplicaciones y Hardware.

**Tabla 2. Costo de TI de la infraestructura**

| Servicio, Aplicaciones o Hardware | Costo | Descripción |
|---|---|---|
| Networking | 1000 | |
| ISP | 3800 | Proveedor Claro |
| Buckup | 150 | Telconet |
| Infraestructura | 30000 | 3 meses atrás compras de parlantes, cables, etc. |

**Fuente:** Departamento de Sistemas Unidad Educativa Atenas, Analista 1.

Cuando se habla sobre el costo de la infraestructura en la parte de sistemas se debe tomar en cuenta los servicios que esta implica, sean físicos, de software y hardware. La Fundación cultural y Educativa Ambato (Unidad Educativa Atenas) han realizado una inversión en la parte de la infraestructura tomando las medidas necesarias especificadas por el departamento de sistemas.

#### 3.1.2.1.3. Determinar el costo de soporte de la infraestructura basado en requerimientos salariales de los profesionales de TI, puestos de trabajo, cantidad de personal, curriculums publicados y responsabilidades.

**Tabla 3. Costo de soporte de la infraestructura**

| Servicio, Aplicaciones o Hardware | Descripción | Costo |
|---|---|---|
| Requerimientos salariales de TI | Presupuesto para Sistemas | |
| Puestos de Trabajo | Analista de Sistemas 1<br>Analista de Sistemas 2 | |
| Cantidad de Personas | 2 | |
| Curriculums publicados | | |
| Responsabilidades<br>Analista de Sistemas 1 | • Actuar en correspondencia con los valores institucionales, promoviendo su aplicación a través del ejemplo.<br>• Planifica, coordina, dirige y elabora estudios sobre funcionamiento y organización del Área de Sistemas.<br>• Determina normas, sistemas y procedimientos necesarios en la Institución.<br>• Estudia sistemas vigentes y los actualiza de acuerdo a las necesidades de la institución.<br>• Propone, elabora, coordina e implanta nuevo software necesario en la institución.<br>• Vela por el cumplimiento de los programas de mantenimiento.<br>• Supervisa el trabajo del analista 2 y determina plazos para el cumplimiento de éste. | |

| | | |
|---|---|---|
| | • Supervisar que se mantenga actualizada la información de WEB E INTRANET de la institución, con apoyo de las diferentes áreas que le proveen, dentro de los tiempos determinados la información que deberá ser publicada.<br>• Coordinar con el área de Gestión de Talento Humano, el proceso de inducción, reinducción y capacitación de los empleados nuevos o antiguos de la institución, logrando tener empleados competentes y en permanente aprendizaje.<br>• Coordinar y/o desarrollar herramientas tecnológicas intermedias que suplan necesidades específicas de la institución, garantizando su funcionamiento y aplicabilidad al proceso en el cual se vayan a utilizar.<br>• Controlar permanentemente las herramientas de seguridad tecnológica de la institución, velando por la confidencialidad de la información y cuidando los equipos de sufrir daños a causa de virus o cualquier otra amenaza del medio.<br>• Verificar el cumplimiento de los requisitos ISO que apliquen al | |

| | | |
|---|---|---|
| | proceso SISTEMAS, velando por el buen desarrollo de las actividades del área y brindando un servicio que se caracterice por su calidad.<br>• Elaborar, entregar y sustentar los informes de su gestión frente a la Gerencia Administrativa Financiera de la institución dentro de los tiempos establecidos, con el fin de verificar el cumplimiento de los indicadores de su área.<br>• Coordinar conjuntamente con el área académica, todo lo relacionado a las certificaciones internacionales y las herramientas necesarias para su realización en todas las Unidades de Negocio.<br>• Recomendar a la Gerencia Administrativa Financiera el equipamiento y/o softwares que se deben adquirir para cubrir las necesidades de la institución.<br>• Mantiene en orden equipo y sitio de trabajo, reportando cualquier anomalía.<br>• Miembro del comité página Institucional.<br>• Apoyo al trabajo y actividades del analista N°2.<br>• Realiza cualquier otra tarea afín que le sea asignada. | |

| | | |
|---|---|---|
| Responsabilidades<br>Analista de Sistemas 2 | • Actuar en correspondencia con los valores institucionales, promoviendo su aplicación a través del ejemplo.<br>• Administrar el correo electrónico de la institución, garantizando su buen funcionamiento y velando por que los usuarios hagan uso correcto de sus servicios.<br>• Mantener en perfecto funcionamiento la red y los servidores de la institución.<br>• Mantener actualizada la información de la WEB E INTRANET.<br>• Realizar el mantenimiento de los equipos de computación y del software de la institución.<br>• Enviar las comunicaciones institucionales a padres de familia y publicarlas en la Web, basado en la información proporcionada por secretaria académica.<br>• Realizar periódicamente el proceso de respaldo de datos, garantizando el cuidado de la información que se maneja en la institución.<br>• Verificar el cumplimiento de los requisitos ISO que apliquen a los procesos en los que interviene.<br>• Elaborar, entregar y sustentar los informes de su gestión frente a la Gerencia Administrativa | |

| | | |
|---|---|---|
| | Financiera, dentro de los tiempos establecidos, con el fin de verificar el cumplimiento de los indicadores de su área.<br>• Entregar de manera inmediata al inspector de nivel, director de Sección o Coordinador de talento Humano según aplique cualquier objeto/ artículo que se identifique como extraviado en aulas, oficinas, áreas recreativas y/o cualquier dependencia de la Fundación Cultural y educativa Ambato - Unidad Educativa Atenas.<br>• Cumplir las otras funciones que le asigne su jefe inmediato.<br>• Promover una cultura de servicio en todas las áreas de la Fundación.<br>• Cumplir con las funciones asignadas en los documentos del sistema de gestión de calidad que le apliquen.<br>• Contribuir a la implementación de un enfoque de procesos y un pensamiento basado en riesgos.<br>• Tomar conciencia de la importancia de cumplir con la política y objetivos de la organización, así como de su contribución a la eficacia, a la satisfacción del cliente y a la mejora. | |

| | | |
|---|---|---|
| | • Asumir la responsabilidad de desarrollar el personal a su cargo, si aplica, de acuerdo al modelo de gestión y liderazgo de la institución, dentro de un adecuado clima laboral.<br>• Promover una cultura de servicio en todas las actividades realizadas en la Fundación Cultural y Educativa Ambato. | |

**Fuente:** Departamento de Sistemas Unidad Educativa Atenas, Analista 1 y Analista 2.

### 3.1.2.2. Revisión de la Privacidad

La revisión de privacidad es el punto de vista legal y ético del almacenamiento, transmisión y control de los datos basados en la privacidad. El uso de estos datos es lo que preocupa a las personas ya que no se tiene reglas de privacidad de datos específicos.

#### 3.1.2.2.1. Comparar las normas y políticas de seguridad

**Normas sobre el uso de correo electrónico**

En el caso de correo electrónico NO está permitido:

- Atentar contra la integridad de la institución
- Divulgar información que incite a la discriminación o a la violencia
- Enviar contenidos con fines publicitarios y comerciales de bienes y servicios en beneficio propio, de familiares o de terceros, salvo en los casos en los cuales el Rectorado en el área académica y Dirección Ejecutiva en Administración lo autorice expresamente
- Enviar correo tipo SPAM, es decir "Correo Basura", relacionado con falsos virus, con publicidad de empresas, cadenas de mensajes, etc.
- Enviar correo masivo de su cuenta personal (usuario@atenas.edu.ec). Esto se gestionara a través de Sistemas previa autorización de Rectorado.
- Usar la cuenta de correo electrónico de otro usuario o entregar a un tercero la contraseña propia
- Falsificar mensajes de correo electrónico.
- Leer, borrar, copiar o modificar mensajes de correo electrónico de otras personas, sin su autorización.
- Enviar mensajes de correo electrónico, alterando la dirección electrónica del remitente para suplantar a terceros, identificarse como una persona ficticia o simplemente no identificarse.
- Iniciar o continuar cadenas de mensajes pues estas tienden a congestionar innecesariamente la red.
- Usar el servidor de correo como medio para archivar los mensajes, los cuales se recomienda borrar una vez leídos. Si hay necesidad de conservarlos, los mensajes se deberían grabar en un sitio destinado para su almacenamiento; esto también se aplica a los correos enviados y en la papelera de reciclaje.
- El usuario debe enviar mails (actas, informes, reportes, etc.) a las personas responsables de esa información y no a todo el personal.

**Fig. 4.** Normas sobre el uso de correo electrónico

**Fuente:** Fundación Cultural y Educativa Ambato (Unidad Educativa Atenas)

## Normas sobre el uso de computadoras e internet

- Los recursos de computación se deben usar exclusivamente para propósitos relacionados con la educación.
- La Fundación Cultural y Educativa Ambato hará la entrega formal del equipo de cómputo en funcionamiento, con el respectivo software instalado, de acuerdo con la actividad del usuario.
- Sólo Sistemas puede llevar a cabo cualquier tipo de mantenimiento tanto de hardware como de software y de la configuración de acceso a la red.
- **El usuario debe reportar cualquier tipo de daño en el equipo a Sistemas por medio de un correo electrónico.**
- Sistemas por autorización de Dirección Ejecutiva, se reserva el derecho de revisar en cualquier computador y sin previo aviso el tráfico de internet, software instalado y la información almacenada en cada uno de ellos, para verificar el cumplimiento de las políticas establecidas y aplicar las consecuencias que corresponda.
- Toda persona a cargo de uno o varios equipos de cómputo es responsable luego de su uso, dejar apagado correctamente cada uno de sus componentes (CPU, Monitor, Parlantes, Impresora, Proyector).
- El uso de impresoras es estrictamente para trabajos relacionados con la institución. El personal de la Fundación Cultural y Educativa Ambato NO debe imprimir archivos personales o que no tengan relación con la actividad institucional.

No se permite a los usuarios

- Retirar el computador o sus accesorios de las instalaciones de la Fundación Cultural y Educativa Ambato
- Comer o ingenir bebidas mientras esté junto al computador.
- Pegar calcomanías, notas, recordatorios o cualquier tipo de adornos a los equipos

**Fig. 5.** Normas sobre el uso de computadoras e internet

**Fuente:** Fundación Cultural y Educativa Ambato (Unidad Educativa Atenas)

## Normas sobre el uso de la infraestructura física de comunicación

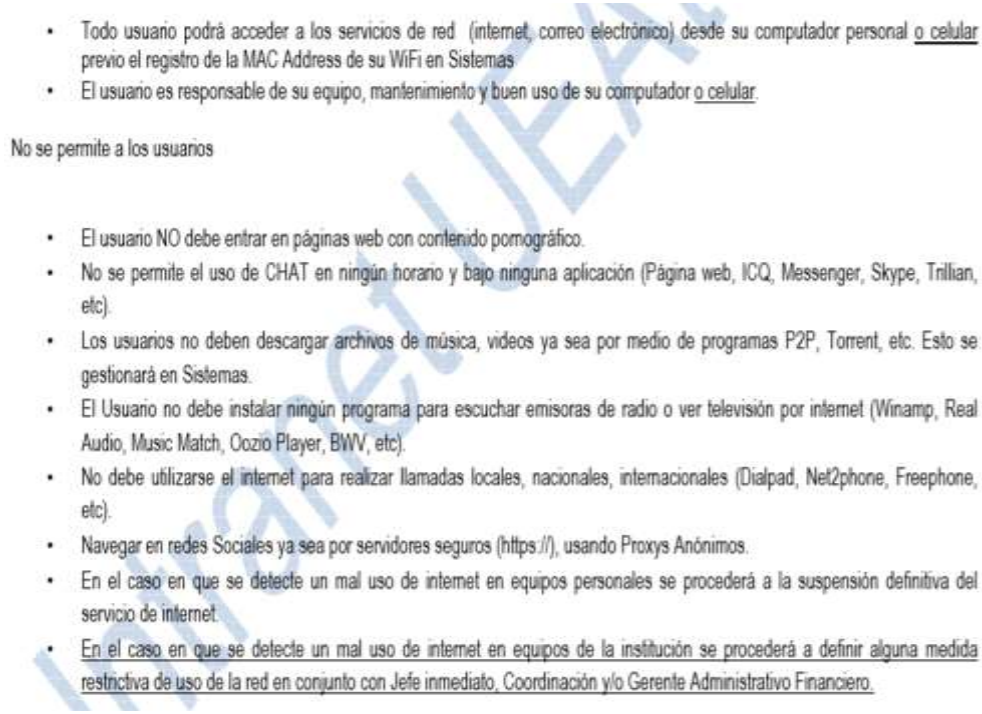
- No está permitido intervenir las redes de cableado, instalando cables no suministrados por Sistemas, cortando o empalmando cables, desprendiendo marcaciones de tomas, puertas o ductos, golpeando o forzando tubos y/o canaletas.
- Tampoco está permitida la instalación de cables, derivaciones a través de conectores en "T" o cualquier tipo de derivación de voz o de datos por parte de los usuarios. Así mismo, no se permite la instalación de ningún servicio que intervenga directamente el cableado que alimenta las tomas. Sin excepción, las conexiones deberán ser realizadas por personal autorizado.

La violación de cualquiera de estas normas podrá causar al usuario la cancelación de la cuenta de correo electrónico, la suspensión indefinida de todos los servicios de red y demás sanciones contempladas en los reglamentos de la Fundación Cultural y Educativa Ambato.

**Fig. 6.** Normas sobre el uso de la infraestructura física de comunicación

**Fuente:** Fundación Cultural y Educativa Ambato (Unidad Educativa Atenas)

## Normas sobre el uso de portátiles y celulares



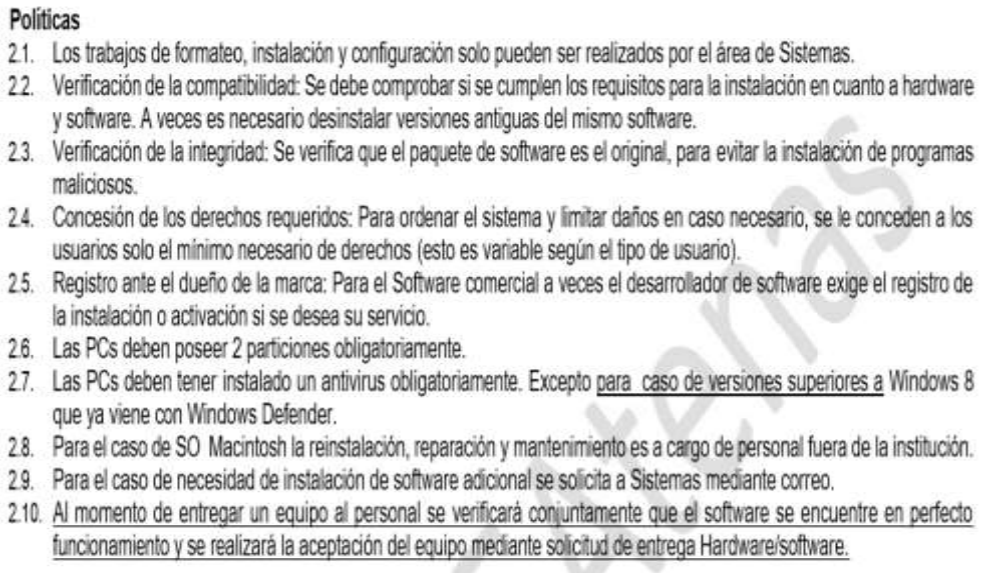
- Todo usuario podrá acceder a los servicios de red (internet, correo electrónico) desde su computador personal o celular previo el registro de la MAC Address de su WiFi en Sistemas
- El usuario es responsable de su equipo, mantenimiento y buen uso de su computador o celular.

No se permite a los usuarios

- El usuario NO debe entrar en páginas web con contenido pornográfico.
- No se permite el uso de CHAT en ningún horario y bajo ninguna aplicación (Página web, ICQ, Messenger, Skype, Trillian, etc).
- Los usuarios no deben descargar archivos de música, videos ya sea por medio de programas P2P, Torrent, etc. Esto se gestionará en Sistemas.
- El Usuario no debe instalar ningún programa para escuchar emisoras de radio o ver televisión por internet (Winamp, Real Audio, Music Match, Oozio Player, BWV, etc).
- No debe utilizarse el internet para realizar llamadas locales, nacionales, internacionales (Dialpad, Net2phone, Freephone, etc).
- Navegar en redes Sociales ya sea por servidores seguros (https://), usando Proxys Anónimos.
- En el caso en que se detecte un mal uso de internet en equipos personales se procederá a la suspensión definitiva del servicio de internet.
- En el caso en que se detecte un mal uso de internet en equipos de la institución se procederá a definir alguna medida restrictiva de uso de la red en conjunto con Jefe inmediato, Coordinación y/o Gerente Administrativo Financiero.

**Fig. 7.** Normas sobre el uso de portátiles y celulares
**Fuente:** Fundación Cultural y Educativa Ambato (Unidad Educativa Atenas)

## Políticas para la instalación y configuración de los equipos informáticos

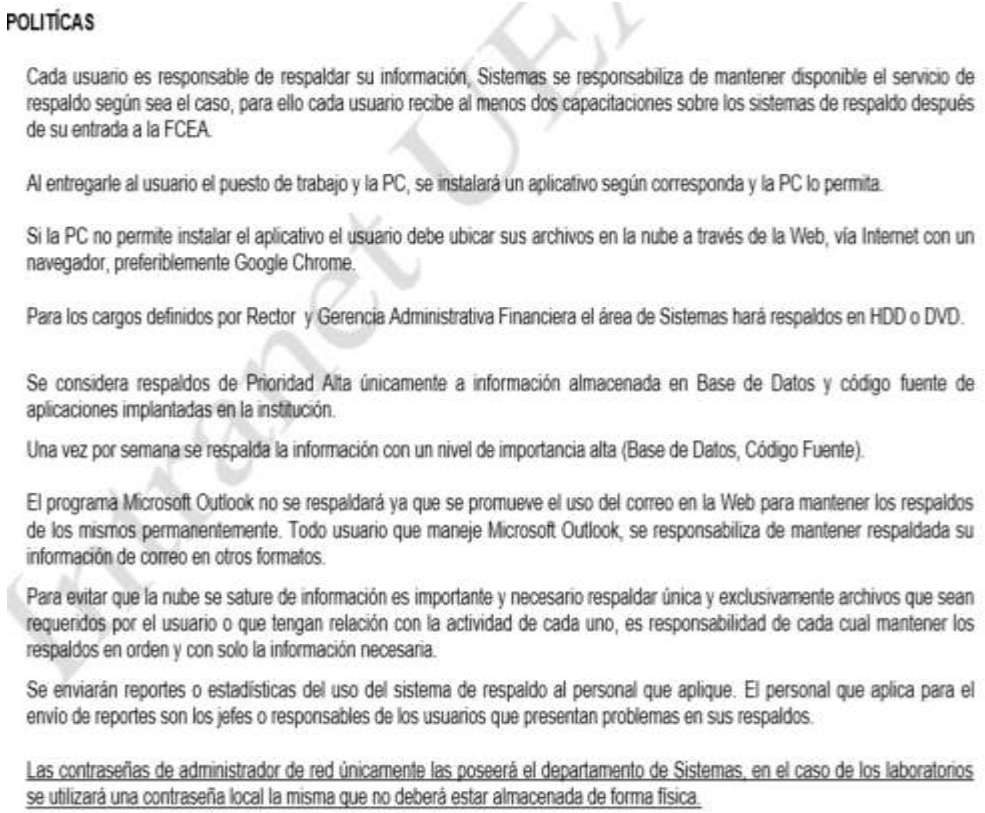


**Políticas**

2.1. Los trabajos de formateo, instalación y configuración solo pueden ser realizados por el área de Sistemas.
2.2. Verificación de la compatibilidad: Se debe comprobar si se cumplen los requisitos para la instalación en cuanto a hardware y software. A veces es necesario desinstalar versiones antiguas del mismo software.
2.3. Verificación de la integridad: Se verifica que el paquete de software es el original, para evitar la instalación de programas maliciosos.
2.4. Concesión de los derechos requeridos: Para ordenar el sistema y limitar daños en caso necesario, se le conceden a los usuarios solo el mínimo necesario de derechos (esto es variable según el tipo de usuario).
2.5. Registro ante el dueño de la marca: Para el Software comercial a veces el desarrollador de software exige el registro de la instalación o activación si se desea su servicio.
2.6. Las PCs deben poseer 2 particiones obligatoriamente.
2.7. Las PCs deben tener instalado un antivirus obligatoriamente. Excepto para caso de versiones superiores a Windows 8 que ya viene con Windows Defender.
2.8. Para el caso de SO Macintosh la reinstalación, reparación y mantenimiento es a cargo de personal fuera de la institución.
2.9. Para el caso de necesidad de instalación de software adicional se solicita a Sistemas mediante correo.
2.10. Al momento de entregar un equipo al personal se verificará conjuntamente que el software se encuentre en perfecto funcionamiento y se realizará la aceptación del equipo mediante solicitud de entrega Hardware/software.

**Fig. 8.** Políticas para la instalación y configuración de los equipos informáticos
**Fuente:** Fundación Cultural y Educativa Ambato (Unidad Educativa Atenas)

## Políticas para el respaldo de la información



**POLITÍCAS**

Cada usuario es responsable de respaldar su información, Sistemas se responsabiliza de mantener disponible el servicio de respaldo según sea el caso, para ello cada usuario recibe al menos dos capacitaciones sobre los sistemas de respaldo después de su entrada a la FCEA.

Al entregarle al usuario el puesto de trabajo y la PC, se instalará un aplicativo según corresponda y la PC lo permita.

Si la PC no permite instalar el aplicativo el usuario debe ubicar sus archivos en la nube a través de la Web, vía Internet con un navegador, preferiblemente Google Chrome.

Para los cargos definidos por Rector y Gerencia Administrativa Financiera el área de Sistemas hará respaldos en HDD o DVD.

Se considera respaldos de Prioridad Alta únicamente a información almacenada en Base de Datos y código fuente de aplicaciones implantadas en la institución.

Una vez por semana se respalda la información con un nivel de importancia alta (Base de Datos, Código Fuente).

El programa Microsoft Outlook no se respaldará ya que se promueve el uso del correo en la Web para mantener los respaldos de los mismos permanentemente. Todo usuario que maneje Microsoft Outlook, se responsabiliza de mantener respaldada su información de correo en otros formatos.

Para evitar que la nube se sature de información es importante y necesario respaldar única y exclusivamente archivos que sean requeridos por el usuario o que tengan relación con la actividad de cada uno, es responsabilidad de cada cual mantener los respaldos en orden y con solo la información necesaria.

Se enviarán reportes o estadísticas del uso del sistema de respaldo al personal que aplique. El personal que aplica para el envío de reportes son los jefes o responsables de los usuarios que presentan problemas en sus respaldos.

Las contraseñas de administrador de red únicamente las poseerá el departamento de Sistemas, en el caso de los laboratorios se utilizará una contraseña local la misma que no deberá estar almacenada de forma física.

**Fig. 9.** Políticas para el respaldo de la información
**Fuente:** Fundación Cultural y Educativa Ambato (Unidad Educativa Atenas)

### 3.1.2.2.2. Comparativa de normas y políticas de seguridad por parte del personal de sistemas de la unidad educativa.

**Tabla 4. Resultado de normas y políticas de seguridad por parte del área de sistemas**

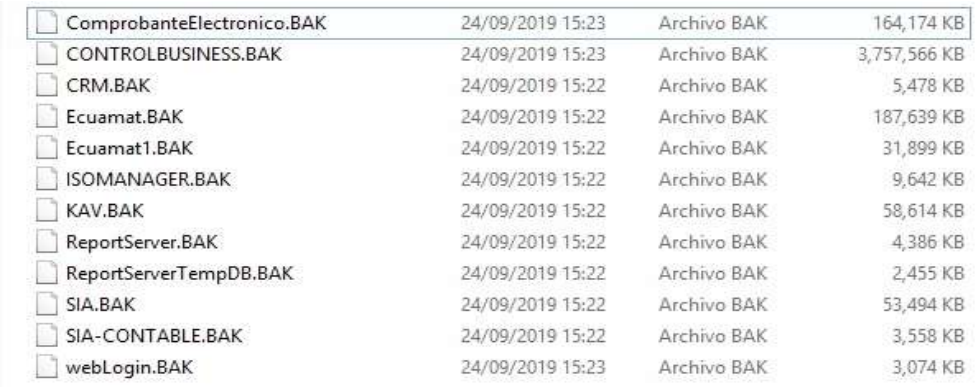
| Norma | Analista 1 | Analista 2 |
|---|---|---|
| **¿El personal de la institución ha intentado atentar a la integridad de la misma por medio del uso indebido del correo electrónico?** | SI | NO |
| **¿El personal divulga información que incite a la discriminación o a la violencia?** | SI | NO |
| **¿Se ha enviado contenido con fines publicitarios y comerciales de bienes y servicios en beneficio propio, sin la autorización pertinente?** | NO | NO |
| **¿Se ha usado el correo institucional para él envió de SPAM, por parte del personal?** | SI | NO |
| **¿Se ha enviado correos masivos de cuentas personales, sin autorización del rectorado?** | SI | NO |
| **¿Se ha registrado casos donde el personal ha utilizado la cuenta de otro usuario o ha facilitado sus contraseñas propias a terceros?** | SI | SI |

| | | |
|---|---|---|
| **¿El personal de la institución ha falsificado mensajes de correo electrónico?** | NO | NO |
| **¿Se ha dado casos donde el personal de la institución lee, copia, borra o modifica mensajes de correo electrónico de otras personas, sin autorización previa?** | NO | NO |
| **¿Ha comprobado que el personal inicia o continua con cadenas de mensajes los cuales congestionan innecesariamente la red?** | SI | SI |
| **¿Los recursos de computación son usados exclusivamente con propósitos educativos?** | NO | SI |
| **¿La unidad educativa entrega un equipo de cómputo en perfecto funcionamiento con lo necesario para la actividad del usuario?** | SI | SI |
| **¿Se reporta a Sistemas por medio correo electrónico cualquier tipo de daño en los equipos?** | SI | SI |
| **¿El departamento de sistemas realiza revisiones sin previo aviso del usuario: el tráfico de internet, software instalado, y la información almacenada en cada una de ellos, verificando el cumplimiento de las políticas de seguridad y aplicando las consecuencias que corresponda?** | SI | SI |
| **¿El personal de la institución cumple con las normas internas establecidas para el correcto uso de las computadoras?** | SI | SI |
| **¿El departamento de sistemas lleva un control de todo el software que está instalado en las computadoras?** | SI | SI |
| **¿Se ha producido alguna intervención en las redes de cableado por parte del personal de la institución?** | NO | NO |
| **¿Existe el previo registro de las direcciones Mac para el uso del internet en pc personales y celulares?** | NO | SI |
| **¿Considera usted que cada usuario es responsable del buen uso de su computador institucional, personal o celular?** | SI | SI |
| **¿Existe el bloque respectivo de páginas con contenido para adultos?** | SI | SI |
| **¿El departamento de sistemas realiza el bloqueo respectivo de las redes sociales para evitar el uso del chat?** | SI | SI |
| **¿El personal de la institución realiza la petición para descargar música?** | SI | SI |
| **¿Sistemas lleva un control para evitar que los usuarios no descarguen aplicaciones que permitan escuchar radio o ver televisión por internet, así como también realizar llamadas nacionales, locales o internacionales por medio del internet?** | SI | SI |
| **¿Sistemas realiza la suspensión de internet de un equipo donde se detecte un mal uso del internet?** | SI | SI |

**Fuente:** Elaborado por el Investigador

Existe un desacuerdo por parte de los analistas de sistemas en el cumplimiento de las normas y políticas de seguridad en lo que se refiere al uso del correo electrónico por lo que se hará un ataque usando este medio el cual será de mucha utilidad al momento de hacer un ataque de ingeniería social.

**Identificar tamaño de la base de datos para el almacenamiento.**



| | | | |
|---|---|---|---|
| ComprobanteElectronico.BAK | 24/09/2019 15:23 | Archivo BAK | 164,174 KB |
| CONTROLBUSINESS.BAK | 24/09/2019 15:23 | Archivo BAK | 3,757,566 KB |
| CRM.BAK | 24/09/2019 15:22 | Archivo BAK | 5,478 KB |
| Ecuamat.BAK | 24/09/2019 15:22 | Archivo BAK | 187,639 KB |
| Ecuamat1.BAK | 24/09/2019 15:22 | Archivo BAK | 31,899 KB |
| ISOMANAGER.BAK | 24/09/2019 15:22 | Archivo BAK | 9,642 KB |
| KAV.BAK | 24/09/2019 15:22 | Archivo BAK | 58,614 KB |
| ReportServer.BAK | 24/09/2019 15:22 | Archivo BAK | 4,386 KB |
| ReportServerTempDB.BAK | 24/09/2019 15:22 | Archivo BAK | 2,455 KB |
| SIA.BAK | 24/09/2019 15:22 | Archivo BAK | 53,494 KB |
| SIA-CONTABLE.BAK | 24/09/2019 15:22 | Archivo BAK | 3,558 KB |
| webLogin.BAK | 24/09/2019 15:23 | Archivo BAK | 3,074 KB |

**Fig. 10.** Tamaño de la base de datos

**Fuente:** Fundación Cultural y Educativa Ambato (Unidad Educativa Atenas)

Según los resultados obtenidos se comprobó que no existía mucha información en la base de datos, donde se podía notar que la información de los datos no superaba los 5gb.

### 3.1.2.2.3. Identificar la ubicación y el almacenamiento de los datos.

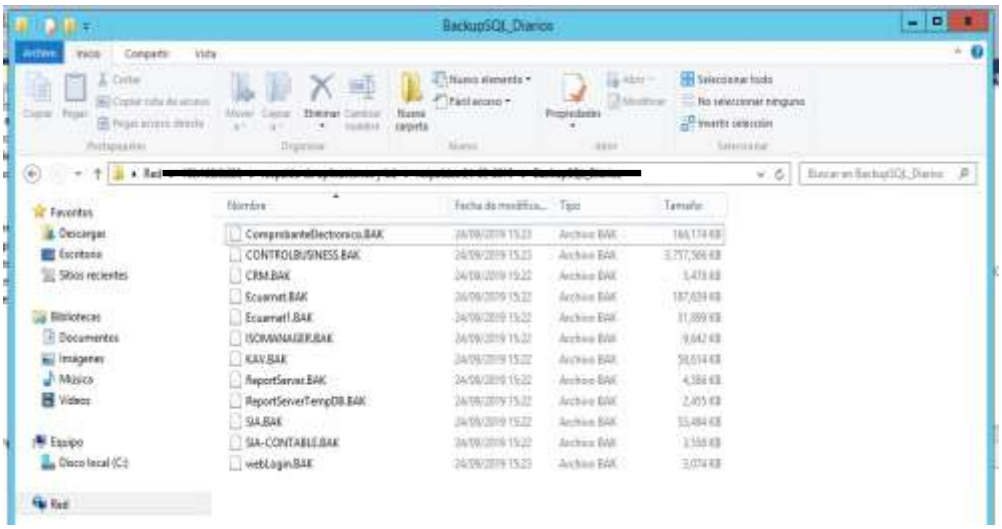



**Fig. 11.** Ubicación y Almacenamiento de la base de datos.

**Fuente:** Elaborado por Analista de sistemas 2

La ubicación y el almacenamiento de la base de datos es especificada por los analistas de sistemas en la cual solo ellos tienen acceso y permisos.

### 3.1.2.2.4. Identificar tipo de cookies.


**Fig. 12.** Tipo de cookies
**Fuente:** Elaborado por Analista de sistemas 1

Al instalar y ocupar Google Chrome esta tiene algunas cookies donde guarda información u otra información importante, la cual si es útil para recordar el sitio o las contraseñas. Pero existe una desventaja la cual es que si se tiene acceso a la información guardada ya que las cookies no es posible ponerlas privadas.

### 3.1.2.2.5. Fechas de expiración y el almacenamiento de cookies.


**Fig. 13.** Expiración y Almacenamiento de cookies
**Fuente:** Elaborado por Analista de sistemas 1

Hay que tener muy claro que la fecha de expiración de las cookies es importante ya que algunas duran 24 horas y otras se quedan varios meses, se debe tener en claro que tipo de cookies tiene activas nuestra máquina y si es posible desactivar las que no crea que son necesarias.

### 3.1.2.3. Recolección de documentos

Es importante la verificación de la información testeada y perteneciente a lo que se considera seguridad de la información. Tomando en cuenta el tiempo otorgado para la búsqueda y extracción de la información.

#### 3.1.2.3.1. Recopilar direcciones de email de la organización y direcciones personales de personas.

**Tabla 5. Datos obtenidos de los docentes de la Unidad Educativa Atenas**


**Fuente:** Elaborado por el Investigador

Los datos que se obtuvieron fueron los siguiente: se pudo obtener 98 correos de los docentes de la institución de un total de 149, para ello se empleó una recolección por medio de comandos de búsqueda de Google.

Dando un porcentaje del 65.77% en la obtención de información contra un 34.23%. Todo depende del almacenamiento de las cookies y los permisos que los usuarios les dan.

**Tabla 6. Datos obtenidos de Administrativos de la Unidad Educativa Atenas**


**Fuente:** Elaborado por el Investigador

Los datos que se obtuvieron fueron los siguiente: se pudo obtener 19 correos de los administrativos de la institución de un total de 25. Estos datos los tenían guardados en un archivo Excel, el mismo que no tenía protección y se encontraba en la maquina principal del analista de sistemas1.

Dando un porcentaje del 76% en la obtención de información contra un 24%.

### 3.1.3. SEGURIDAD DE LOS PROCESOS

#### 3.1.3.1. Testeo de Solicitud

Es la manera de obtener privilegios de acceso a una organización y sus activos por medio de las comunicaciones ya sean teléfono, email, chat, boletines, etc. El personal de entrada es quienes tienen la autoridad para dar privilegios de acceso a otros.

##### 3.1.3.1.1. Prueba de ingeniería social en el personal

La prueba de ingeniería social se realizó a todos los docentes y administrativos en la cual se obtuvo los datos que se presentaran a continuación.

Lo que se realizó en este proyecto es crear un correo electrónico en el cual se pidió datos personales como: Nombre, Apellido, Teléfono, Usuario de IDUKAY, Contraseña de IDUKAY.

## Creación del correo electrónico


**Fig. 14.** Creación del correo electrónico
**Fuente:** Elaborado por el Investigador

## Cuenta de correo electrónico creado


**Fig. 15.** Cuenta de Correo electrónico
**Fuente:** Elaborado por el Investigador

### 3.1.3.1.2. Obtener información acerca de la persona de entrada

**Mensaje para el ataque de ingeniería social**


**Fig. 16.** Mensaje de ataque de ingeniería social
**Fuente:** Elaborado por el Investigador

**Respuesta al ataque de ingeniería social**

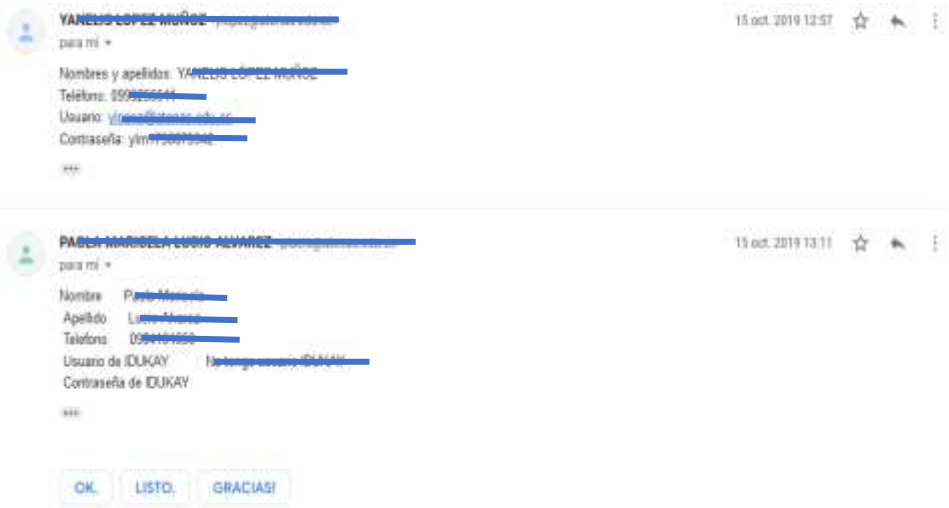



**Fig. 17.** Respuesta al ataque de ingeniería social
**Fuente:** Elaborado por el Investigador

**Descripción:**

A pesar de no tener un dominio parecido al de la institución existieron personas las cuales proporcionaron los datos personales siendo parte del personal administrativo y docentes.

Hay que tomar en cuenta la facilidad con la que se proporcionó los datos, para poder realizar la respectiva inducción sobre los ataques de ingeniería social.

## Detección de phishing por parte de Gmail

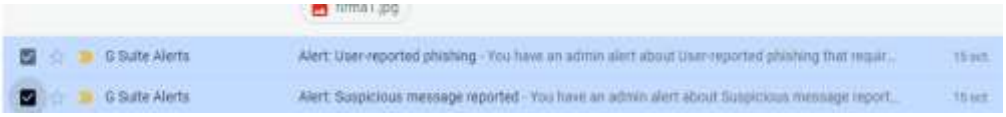



**Fig. 18.** Correo detectado como intento de phishing
**Fuente:** Analista de sistemas 1 Unidad Educativa Atenas

## Mensaje de phishing por parte de Gmail

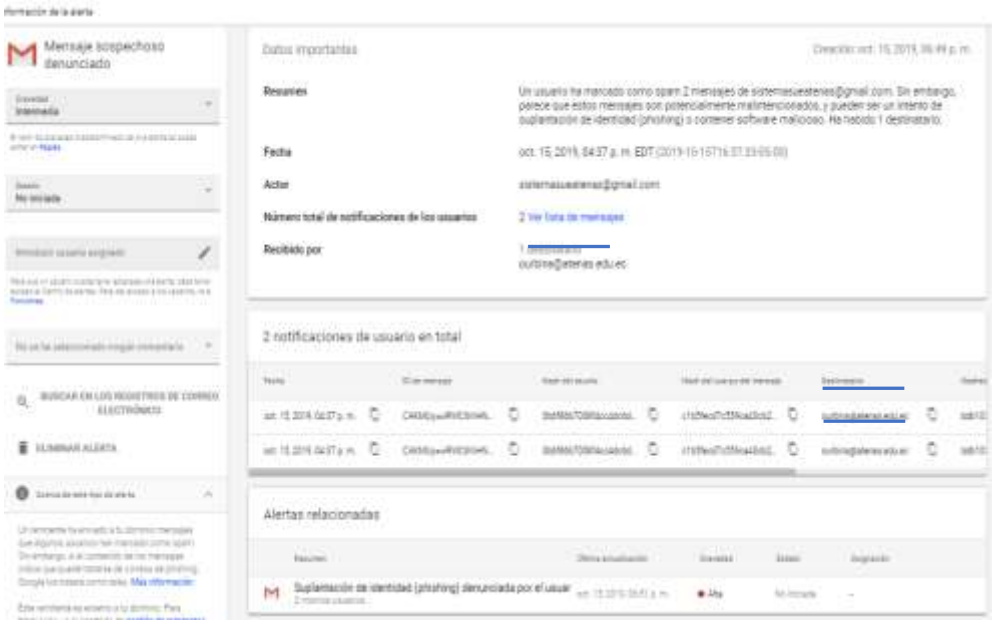



**Fig. 19.** Mensaje intento de phishing
**Fuente:** Analista de sistemas 1 Unidad Educativa Atenas

**Descripción:**

Al realizar él envió del correo electrónico existieron personas las cuales se dieron cuenta de que el correo era un intento de robo de información por lo que hicieron la respectiva denuncia y este inmediatamente envió una alerta a todos los correos que recibieron el mensaje, Gmail al reportar como phishing un correo este manda una advertencia para que las demás personas tomen precaución y eviten enviar datos o responder.

### 3.1.3.1.3. Enumerar cantidad de información privilegiada obtenida

**ATAQUE PERSONAL ADMINISTRATIVO**

**Tabla 7. Datos obtenidos en el ataque a Administrativos de la Unidad Educativa Atenas**

| Nombre | Correo Electrónico | Descripción |
|---|---|---|
| ANDRES MAZON YEPEZ | [redacted] | Sin respuesta |
| CRISTINA ELIZABETH SILVA MERA | [redacted] | Confirmación de Datos con Sistemas |
| DAMNE COTEÑO | [redacted] | Correo suspendido, fuera de la institución |
| MARTHA CECILIA REINOSO NOGALES | [redacted]ec | Facilito sus Datos |

**Fuente:** Elaborado por el Investigador

**Descripción del ataque que se realizó a los Administrativos de la Unidad Educativa Atenas**

| DESCRIPCION | NUMERO |
|---|---|
| Confirmación de Datos con Sistemas | 9 |
| Facilito sus Datos | 3 |
| Sin respuesta | 10 |
| Correo suspendido, fuera de la institución | 3 |
| Total | 25 |

**Fig. 20.** Resultado del ataque de Ingeniería Social realizado Administrativos
**Fuente:** Elaborado por el Investigador

**Grafica del ataque que se realizó a los Administrativos de la Unidad Educativa Atenas**

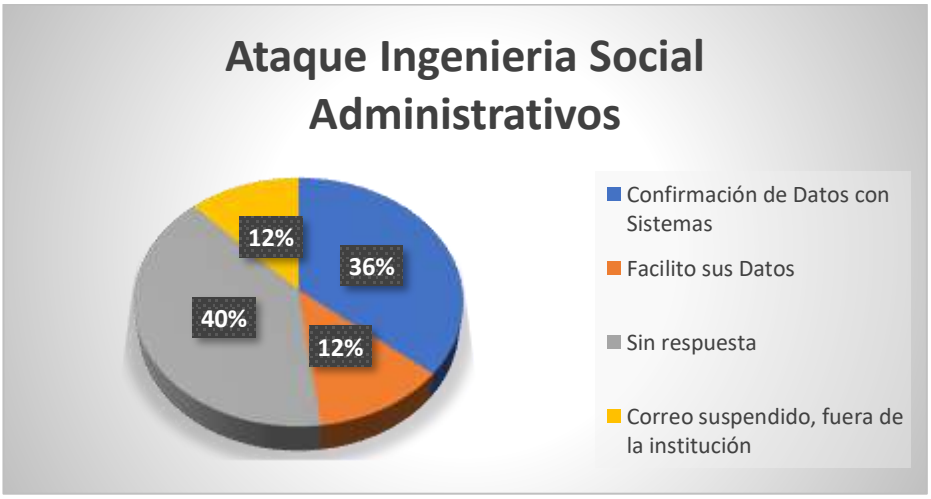



**Fig. 21.** Grafica del ataque de Ingeniería Social realizado Administrativos
**Fuente:** Elaborado por el Investigador

**Interpretación:**

Del personal Administrativo de la institución Educativa Atenas al cual se le realizo el ataque, el 12% fueron empleados los cuales están fuera de la institución, el 36% de los administrativos confirmo los datos con el departamento de sistemas respetando la orientación que se les había brindado, también el 12 % facilito sus datos personales y el 40% no respondió el mensaje solo lo ignoro sin llamar al departamento de sistemas.

**Análisis:**

De los datos se puede deducir que la mayor parte del personal administrativo de la Unidad Educativa Atenas ignora los mensajes, cuando deben preguntar o confirmar con el departamento de sistemas cuando llegan algún correo pidiendo sus datos personales o dar la información pertinente.

**ATAQUE PERSONAL DE DOCENCIA**

**Tabla 8. Datos obtenidos en el ataque a Docentes de la Unidad Educativa Atenas**

| Nombre | Correo Electrónico | Descripción |
|---|---|---|
| ALEIXANDRA HERNANDEZ BLANCO | ahernandez@atenas.edu.ec | Sin respuesta |
| ANA MARIA VELA CALLEJAS | avela@atenas.edu.ec | Confirmación de Datos con Sistemas |
| ANA MARIA PINTO SALAZAR | apinto@atenas.edu.ec | Correo suspendido, fuera de la institución |
| ANDREA LUCIA ROSERO BURBANO | arosero@atenas.edu.ec | Facilito sus Datos |

**Fuente:** Elaborado por el Investigador

**Descripción del ataque que se realizó a los Administrativos de la Unidad Educativa Atenas**

| DESCRIPCION | NUMERO |
|---|---|
| Confirmación de Datos con Sistemas | 17 |
| Facilito sus Datos | 27 |
| Sin respuesta | 72 |
| Correo suspendido, fuera de la institución | 33 |
| Total | 149 |

**Fig. 22.** Resultado del ataque de Ingeniería Social realizado a Docentes

**Fuente:** Elaborado por el Investigador

**Grafica del ataque que se realizó a los Docentes de la Unidad Educativa Atenas**

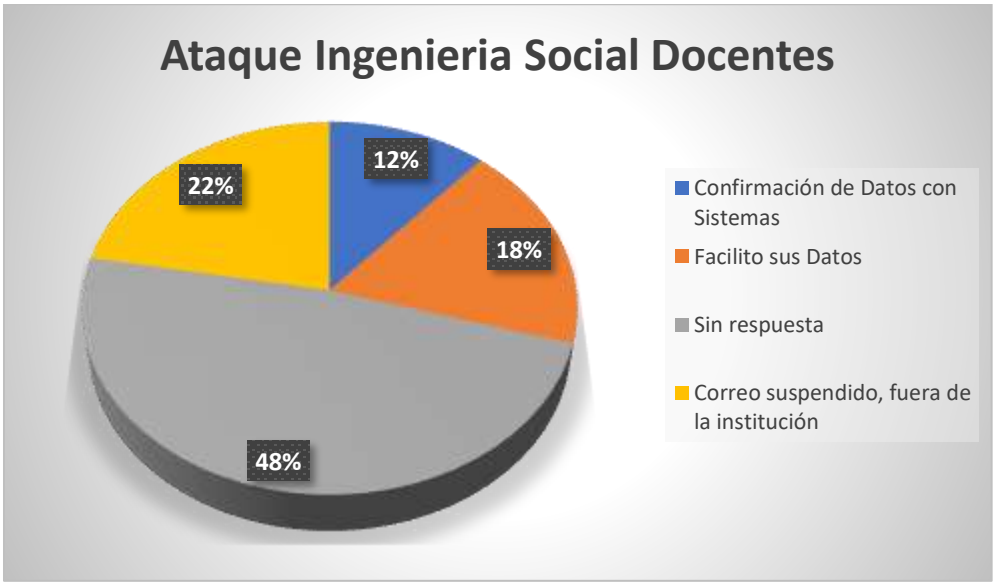



**Fig. 23.** Grafica del ataque de Ingeniería Social realizado Administrativos

**Fuente:** Elaborado por el Investigador

**Interpretación:**

Del personal Educativo de la institución Educativa Atenas al que se le realizo el ataque, el 22% son docentes los cuales están fuera de la institución, el 12% de los docentes confirmo los datos con el departamento de sistemas respetando la orientación que se les había brindado, también el 18% facilito sus datos personales y el 48% no respondió el mensaje solo lo ignoro sin llamar al departamento de sistemas.

**Análisis:**

De los datos se puede deducir que la mayor parte de los docentes de la Unidad Educativa Atenas ignora los mensajes, así también notamos que son pocas personas las que confirman o preguntan al departamento de sistemas el origen del correo o por qué razón piden los datos personales.

### 3.1.3.2.Testeo de Sugerencia Dirigida

Es la manera de obtener privilegios de acceso a una organización y sus activos por medio de las comunicaciones ya sean teléfono, email, chat, boletines, etc. Esta técnica requiere una “ubicación” para la persona a provocar a hablar tal como una página web, una dirección de e-mail, etc.

#### 3.1.3.2.1. Seleccionar una persona o personas a partir de la información ya obtenida sobre el personal

**Tabla 9. Selección de la víctima para el próximo ataque**

| Escenario del ataque | |
|---|---|
| **Correo Electrónico** | **jcalvache@atenas.edu.ec** |
| **Persona** | **JUAN CARLOS CALVACHE** |
| **Descripción** | **Para esta prueba se realizó un njRAT en la cual se puso el nombre Chrome.exe el cual era un ejecutable, con lo cual se buscaba tomar el control de la máquina de la víctima para esto se realizó varias pruebas.** |
| **Resultado** | **La prueba con el njRAT al momento que se envió a la víctima y trato de ejecutar, el antivirus defender lo detectaba como virus en las maquinas.** |

**Fuente:** Elaborado por el Investigador

#### 3.1.3.2.2. Examinar los métodos de contacto a las personas objetivo

Para esta prueba se realizó un njRAT el cual se habilitó en el puerto 443 abierto para poder realizar la prueba pertinente se puso la IP 192.168.X.X y con el nombre de Chrome.exe, el cual se enviará para poder realizar el ataque a la víctima. Para esto primero se eligió a la víctima después ver el puerto que estaba abierto, pero normalmente usamos el 443 que está abierto por defecto para esto se enviara un ejecutable directamente para ser descargado como una actualización de Chrome el cual pedirá que se descargue y lo ejecute.

**Creación del njRAT y selección de puertos**


**Fig. 24.** Creación del njRAT y puerto de ataque
**Fuente:** Elaborado por el Investigador

## Verificación de IP del atacante

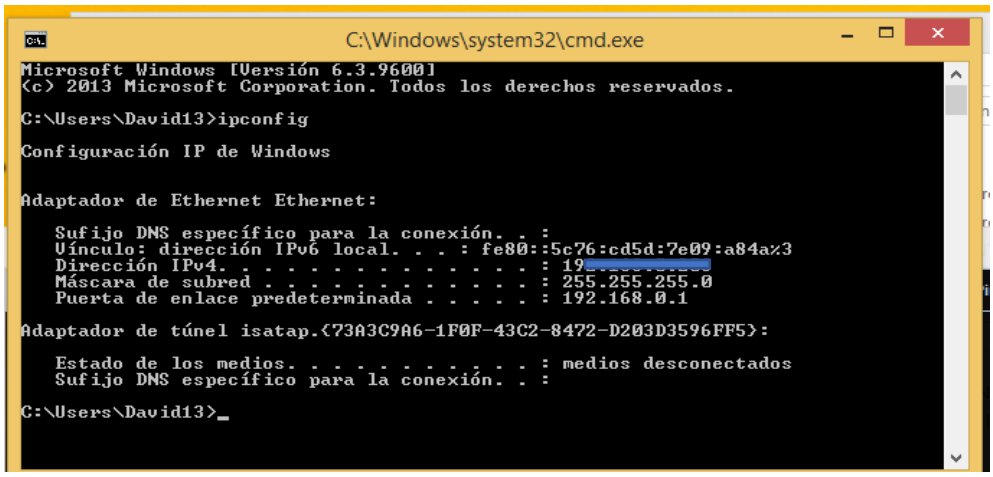



**Fig. 25.** IP de atacante
**Fuente:** Elaborado por el Investigador

## Configuración del njRAT


**Fig. 26.** Configuración de IP, nombre y su ubicación.
**Fuente:** Elaborado por el Investigador

## Ubicación del acceso directo realizo por el njRAT

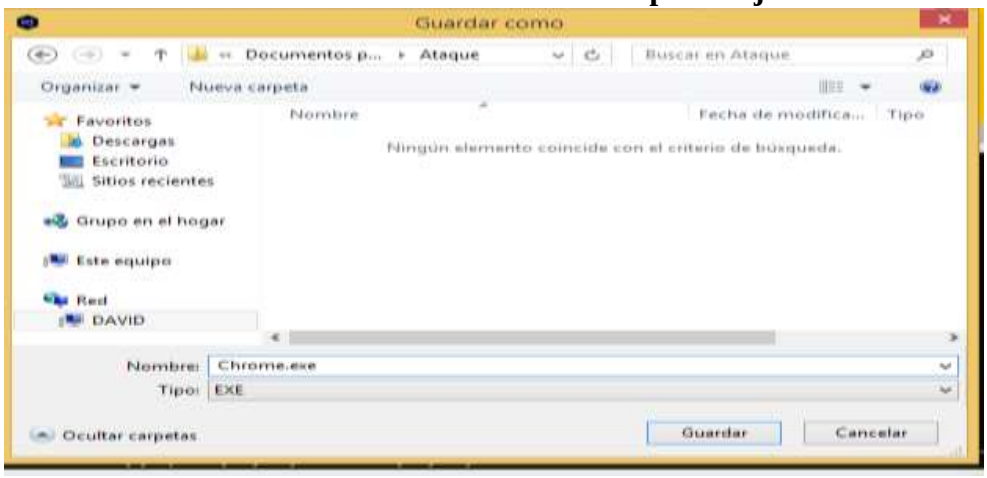



**Fig. 27.** Ubicación del njRAT
**Fuente:** Elaborado por el Investigador

**Finalización de creación del njRAT**


**Fig. 28.** njRAT finalizado
**Fuente:** Elaborado por el Investigador

### 3.1.3.2.3. Ataque con njRat

**Descarga del njRAT desde virtual box**

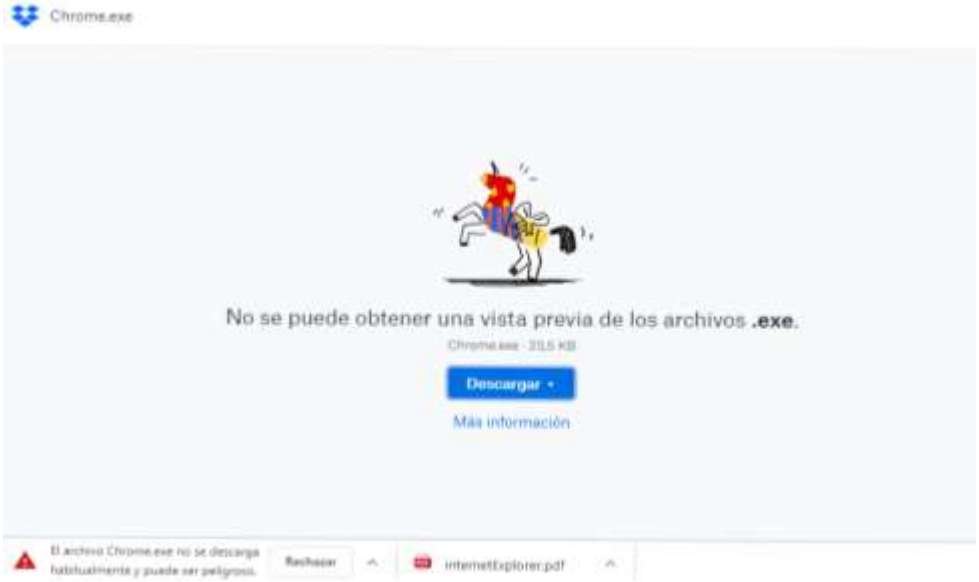



**Fig. 29.** Descarga del njRAT por parte de la víctima
**Fuente:** Elaborado por el Investigador

**Abrir el acceso directo creado**

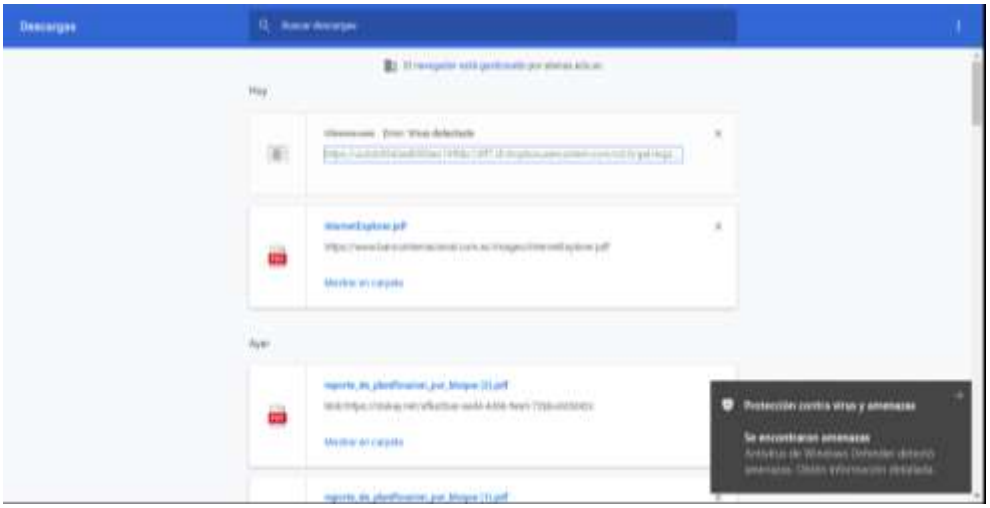


**Fig. 30.** Ejecución del acceso directo creado
**Fuente:** Elaborado por el Investigador

**Resultado:**

Una vez que ya se realizo el njRAT se pocede a realizar la prueba para poder controlar la maquina de la victima. Un inconveniente para enviarlo por gmail fue que el correo no deja subir archivos con la extencion .exe lo que dificulto el envio directo, pero se procedio ha subir en virtual box y enviar por correo el link de descarga directa para evitar que la victima sepa de donde proviene se creo con el nombre Chrome.exe y el correo era una actualizacion. Al descargarse y al ejecutar la aplicación las maquinas de la institucion educativa tenia activado el antivirus defender lo que detecta cualquier archivo.exe como virus y detiene su ejecucuion.

### 3.1.4. SEGURIDAD EN LAS TECNOLOGÍAS DE INTERNET

#### 3.1.4.1. Logística y controles

Reducir falsos positivos y negativos con los ajustes y herramientas necesarias, las mismas que nos ayudaran a tomar decisiones para realizar el respectivo ataque.

#### 3.1.4.2. Sondeo de Red

Para realizar el sondeo de la red se debe especificar la ruta de la red objetivo para que de esta manera apreciar los paquetes TCP, UDP e ICMP.
Primero se debe determinar latencia de la red con la que cuenta la víctima, para y poder tener bien claro el ataque que se piensa realizar.
Medir la cantidad de paquetes perdidos o rechazos de conexión en la red objetivo.

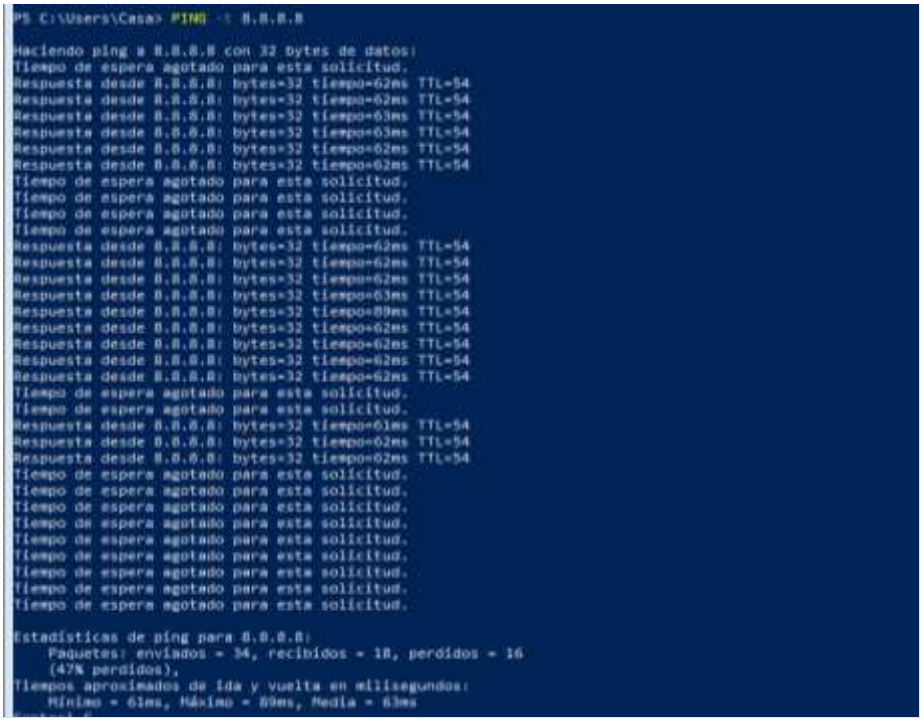



**Fig. 31.** Sondeo de red de paquetes de datos.
**Fuente:** Elaborado por el Investigador

Se debe tener en claro el recorrido que realizan los paquetes desde el origen hasta el destino, se puede realizar un tracert a una IP específica y determinar los saltos que da el paquete hasta llegar a su objetivo.

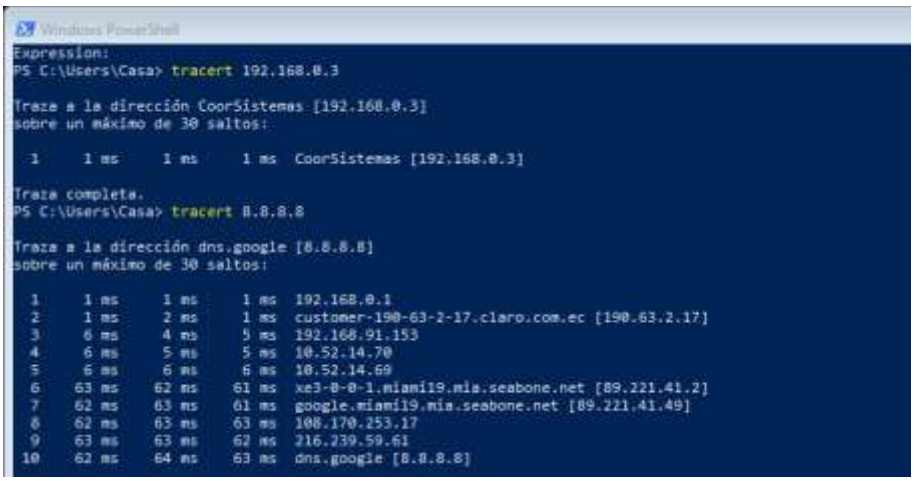



**Fig. 32.** Recorrido de los paquetes TCP perdidos o rechazados
**Fuente:** Elaborado por el Investigador

Se midió la cantidad de paquetes perdidos o rechazos de conexión en la red objetivo de esta manera se puede determinar si tenemos la posibilidad de realizar el ataque analizando los resultados.

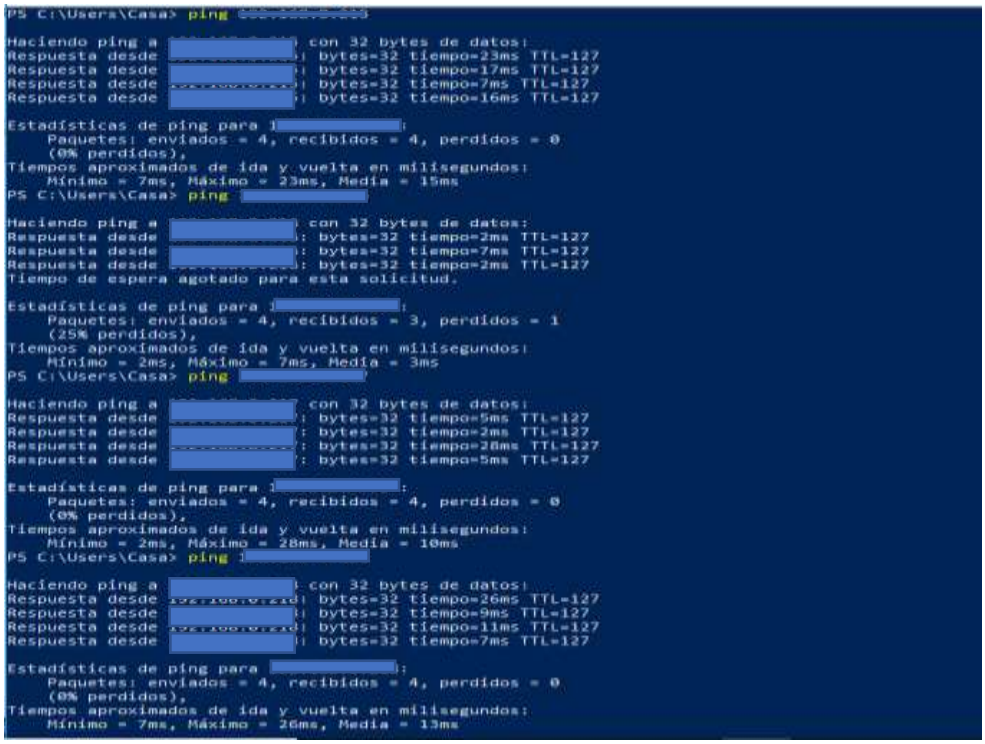



**Fig. 33.** Conexión con los objetivos
**Fuente:** Elaborado por el Investigador

Examinar el camino de enrutamiento al objetivo desde la máquina que realizara el ataque, de esta manera se puede determinar el uso de un firewall el cual puede impedir o dificultar el resultado del mismo.

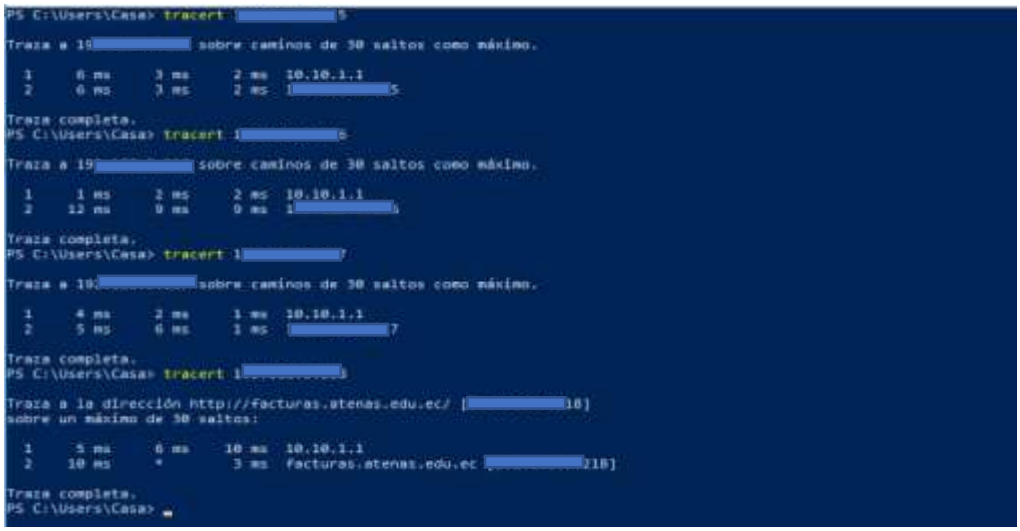



**Fig. 34.** Conexión con los objetivos
**Fuente:** Elaborado por el Investigador

Para examinar el camino de enrutamiento para el ISP del objetivo se utilizó la herramienta Wireshark la cual permite analizar todo el tráfico de red, para esto se debe realizar algunas configuraciones previas.

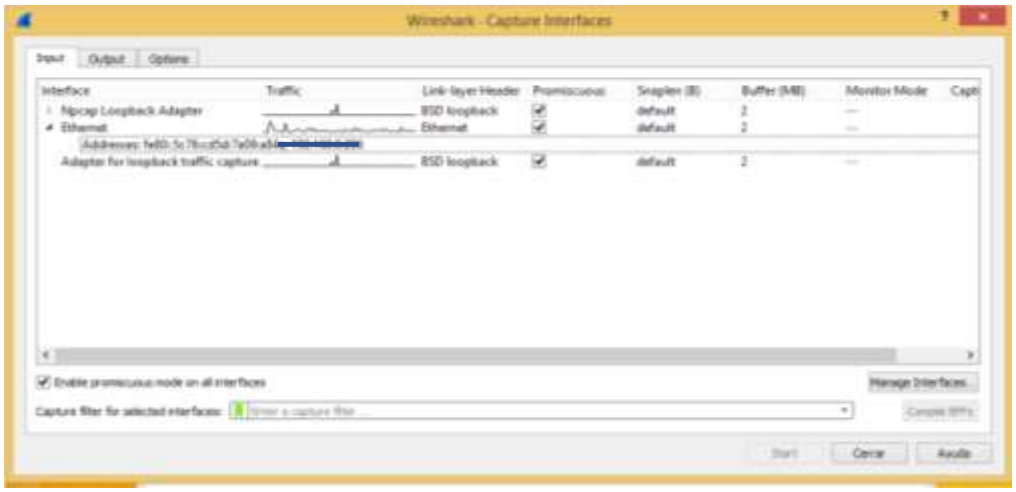



**Fig. 35.** Configuración de wireshark
**Fuente:** Elaborado por el Investigador

Observamos que una vez que nuestra maquina empieza a navegar por internet se puede apreciar cambios los cuales vemos en la imagen (32), algo que es muy importante es el protocolo y el tiempo que se demora en enviar y recibir el paquete de datos.

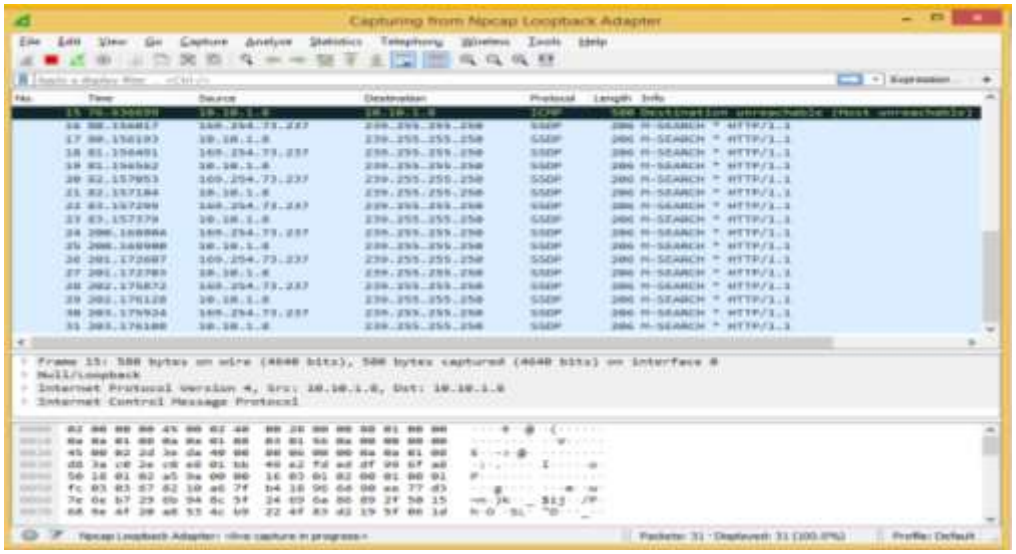



**Fig. 36.** Resultado enrutamiento
**Fuente:** Elaborado por el Investigador

Se puede filtrar para ver el tráfico de red realizado por nuestra IP y de esta manera determinar los diferentes protocolos que tenemos al realizar tareas en nuestra máquina.

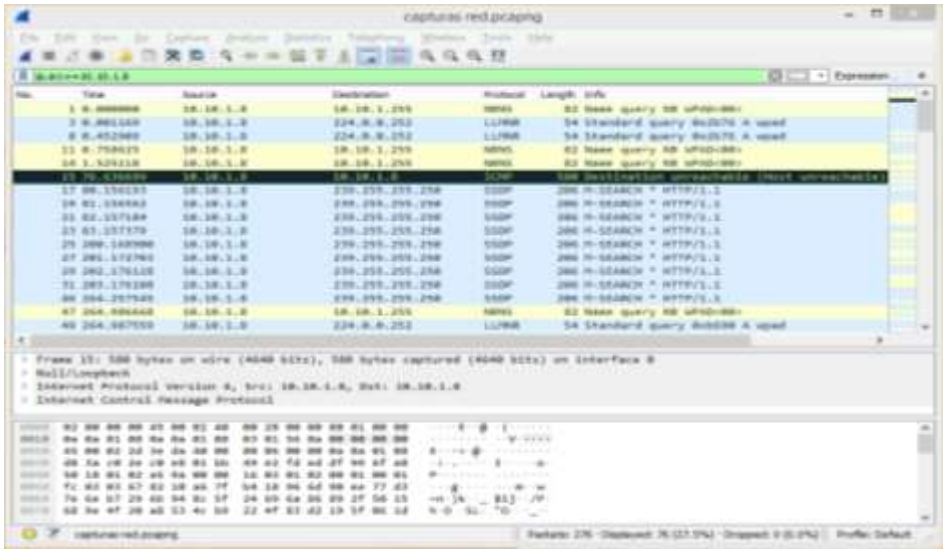


**Fig. 37.** Filtración por IP de enrutamiento
**Fuente:** Elaborado por el Investigador

### 3.1.4.3. Identificación de los Servicios de Sistemas

Es una introducción a los sistemas que van hacer analizados tomando en cuenta la recolección de datos y la obtención de la información. Lo importante es encontrar el número de sistemas a ser alcanzables para ser analizados.

#### 3.1.4.3.1. Respuestas del Servidor de Nombres.

- Examinar la información del registro de dominio en busca de servidores.

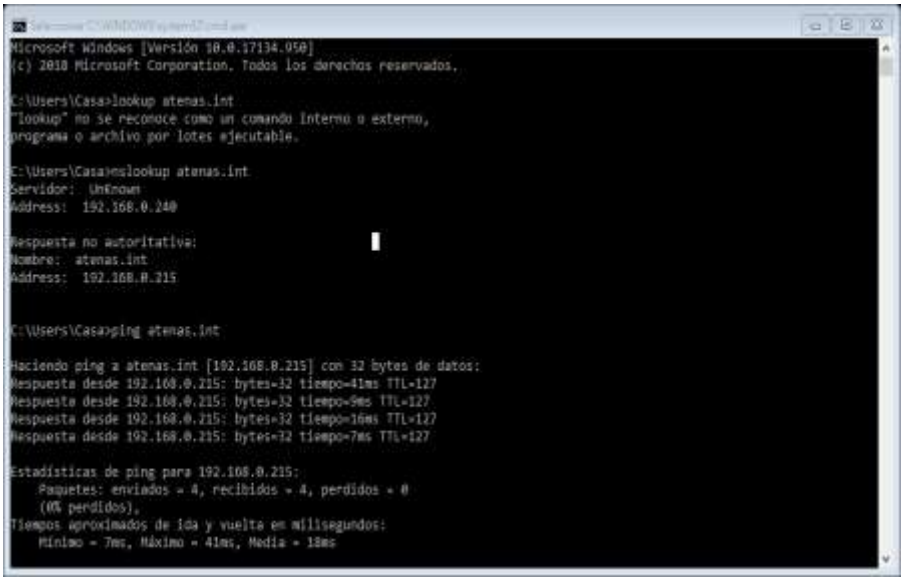



**Fig. 38.** Dominios de la Institución
**Fuente:** Elaborado por el Investigador

- Consultar los servidores de nombres primario, secundario y del ISP en busca de hosts y subdominios.


**Fig. 39.** IP y el ISP de la institución
**Fuente:** Elaborado por el Investigador

### 3.1.4.4. Revisión de la privacidad

#### 3.1.4.4.1. Identificar la localización de los datos almacenados

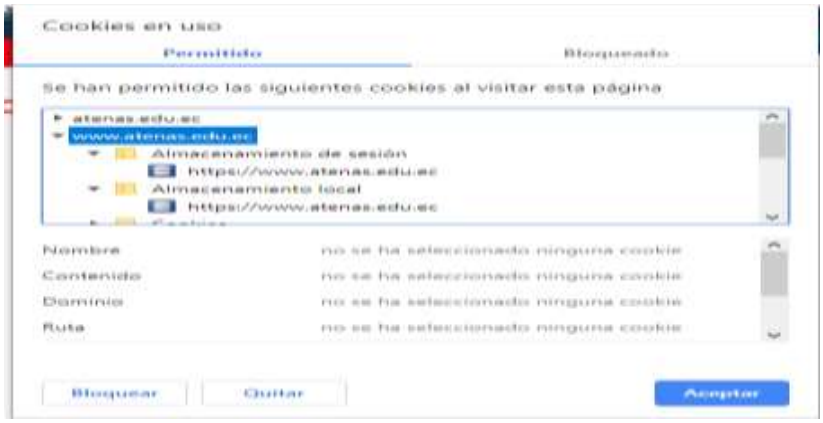



**Fig. 40.** Almacenamiento de cookies
**Fuente:** Elaborado por el Investigador

#### 3.1.4.4.2. Identificar los tipos de cookies


**Fig. 41.** Especificación de cookies
**Fuente:** Elaborado por el Investigador

**Cookies de sesión:** Tiene estas cookies ya que almacenas las contraseñas y la información cuando acceden a la página web de la institución.

**Cookies persistentes:** Se observó este tipo de cookies ya que se borraban estas y después de un tiempo volvían aparecer y guardar la información.

**Cookies publicitarias:** se determinó este uso ya que
Son aquellas que permiten la gestión, de la forma más eficaz posible, de los espacios publicitarios que, en su caso, el editor haya incluido en una página web, aplicación o plataforma desde la que presta el servicio solicitado en base a criterios como el contenido editado o la frecuencia en la que se muestran los anuncios.

**Google Analytics:** Se encontró este tipo de cookies ya que la información que generaba desde su IP era archivada por Google en los servidores de USA.
Al utilizar este website se debe tener en cuenta el uso correcto de este así también con la configuración adecuada.

**Google AdWords:** al verlas configuraciones se observó que se tenía activado el servicio de AdWords en el que se juntaba esta información.
Datos recabados:
Número IP, historial de búsqueda, localización, ID de dispositivo y número de teléfono.
Además de: Visionados de publicidad, analíticos, información del navegador, datos de cookies, fecha y hora, datos demográficos, información del software / hardware, información acerca de interacciones, páginas visitadas, dominios.

### 3.1.4.4.3. Identificar el tiempo de expiración de las cookies


**Fig. 42.** Fecha de expiración de las cookies
**Fuente:** Elaborado por el Investigador

### 3.1.4.5. Búsqueda e identificación de vulnerabilidades

Para esta prueba se ocupó las herramientas nmap en Kali Linux y Nessus para realizar lo que son ataques externos y poder verificar que vulnerabilidades posee la Unidad Educativa Atenas, también usamos lo que es Openvas para realizar ataques internos.

**Tabla 10. Resultados ataques al servidor Facturas**

| Vulnerabilidad | nessus | openvas |
|---|---|---|
| Critica | 1 | - |
| Alta | 2 | 3 |
| Media | 10 | 5 |
| Baja | 2 | 0 |
| Información | 66 | 43 |

**Tabla 11. Resultados ataques al servidor Biblioteca**

| Vulnerabilidad | nessus | openvas |
|---|---|---|
| Critica | 0 | - |
| Alta | 0 | 1 |
| Media | 2 | 1 |
| Baja | 2 | 1 |
| Información | 19 | 11 |

**Tabla 12. Resultados ataques al servidor Active Directory**

| Vulnerabilidad | nessus | openvas |
|---|---|---|
| Critica | 0 | - |
| Alta | 1 | 79 |
| Media | 6 | 120 |
| Baja | 1 | 8 |
| Información | 37 | 75 |

**Tabla 13. Resultados ataques al servidor Base de Datos**

| Vulnerabilidad | nessus | openvas |
|---|---|---|
| Critica | 0 | - |
| Alta | 1 | 0 |
| Media | 7 | 4 |
| Baja | 2 | 0 |
| Información | 33 | 20 |

**Tabla 14. Resultados ataques al servidor Aplicaciones**

| Vulnerabilidad | nessus | openvas |
|---|---|---|
| Critica | 18 | - |
| Alta | 41 | 44 |
| Media | 72 | 71 |
| Baja | 5 | 3 |
| Información | 126 | 39 |

#### 3.1.4.5.1. Búsqueda de vulnerabilidades con Nmap

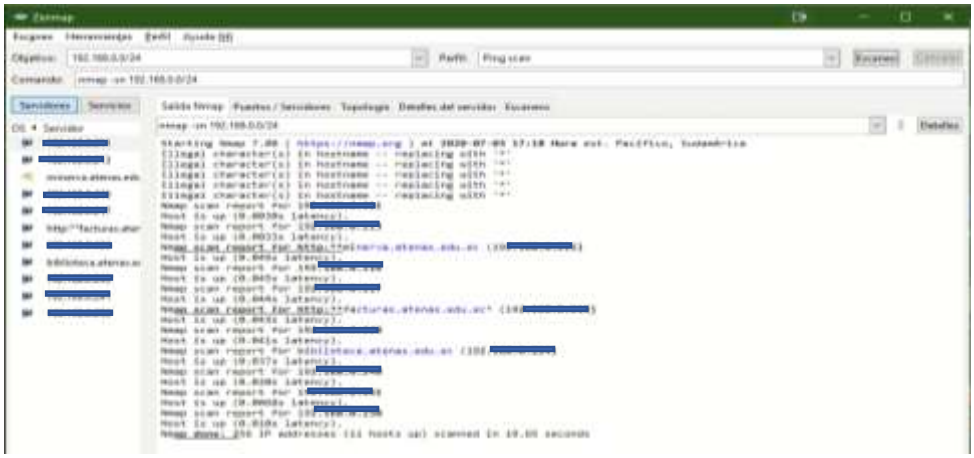


**Fig. 43.** Análisis de red con Zenmap
**Fuente:** Elaborado por el Investigador

Se realizó un análisis de red para ver los dispositvos que estan conectados y poder descubrir las ip de los servidores y si estan conectados a la red por medio de un ping de la aplicación.

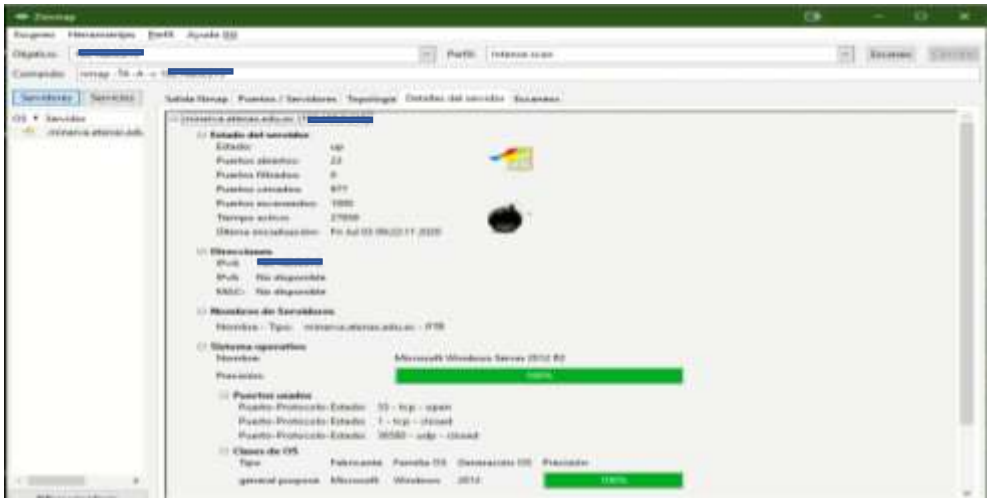


**Fig. 44.** Detalle de servidor de Active Directory
**Fuente:** Elaborado por el Investigador

**Interpretación**:

Se realizó un análisis al servidor Active directory en el cual el resultado fue 23 puertos abiertos tambien se pudo determinar el sistema operativo el cual tenía instalado era un Microsoft Windows Server 2012 R2, además tenía abierto el puerto 53 que es usado por el DNS.

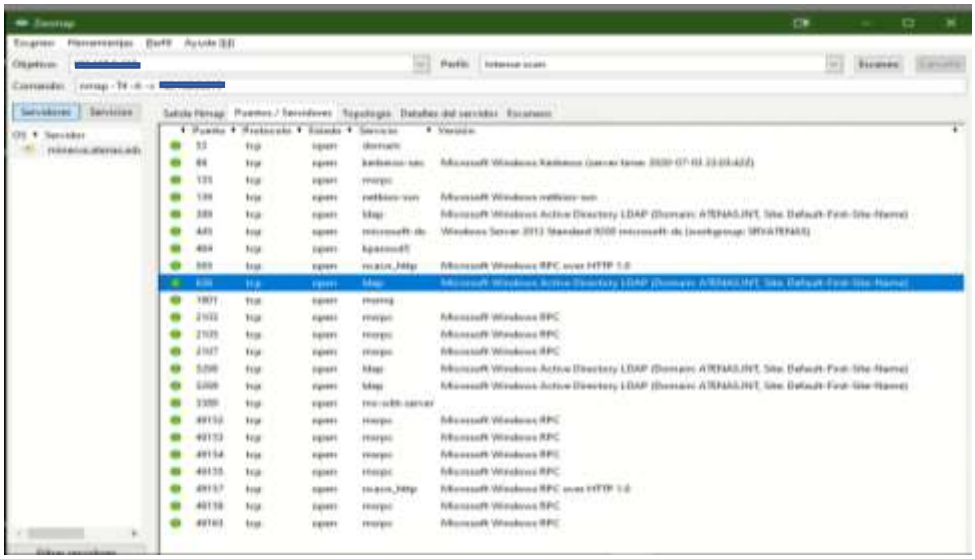


**Fig. 45.** Detalle de servidor de Active Directory
**Fuente:** Elaborado por el Investigador

**Interpretación**:

Se realizó un análisis de los puertos que estaban abiertos, para su posterior ataque. Se debe tener muy en cuenta los puertos y el protocolo que usan así determinar cómo pueden ser vulnerados.

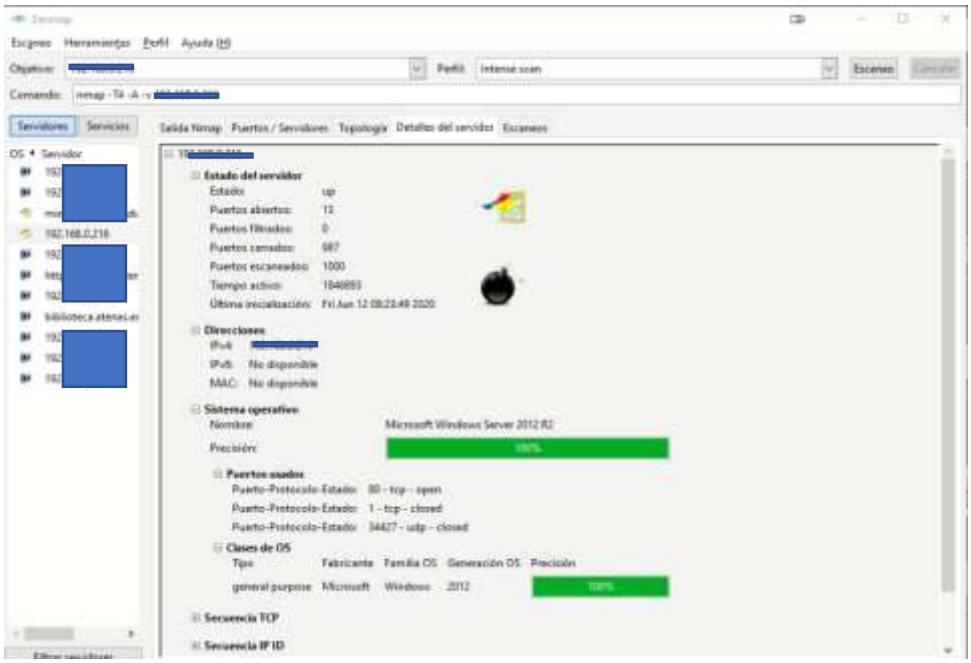


**Fig. 46.** Detalle de servidor de Aplicaciones
**Fuente:** Elaborado por el Investigador

**Interpretación**:

Se realizó un análisis al servidor Aplicaciones en el cual se encontró 13 puertos abiertos también se pudo determinar el sistema operativo el cual tenía

instalado era un Microsoft Windows Server 2012 R2, además tenía abierto el puerto 80 que es usado para conexión a internet.

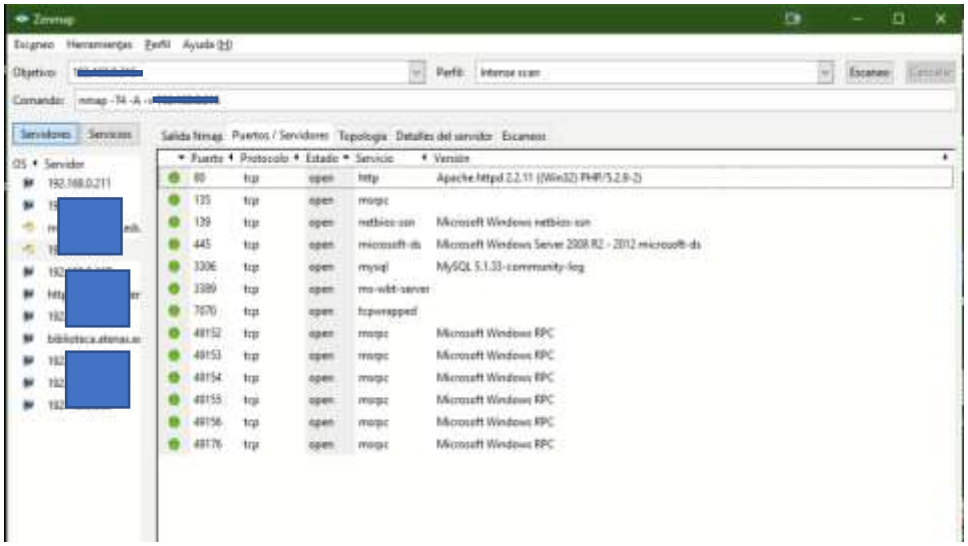


**Fig. 47.** Puertos abiertos servidor de Aplicaciones
**Fuente:** Elaborado por el Investigador

**Interpretación**:

Se realizó un análisis de los puertos abiertos y se vi mayor vulnerabilidad en el puerto 80 HTTP, la solución para esto sería ver que no existan reglas NAT sobre este puerto de ser el caso ver que en ninguna maquina exista alguna configuración como DMZ.

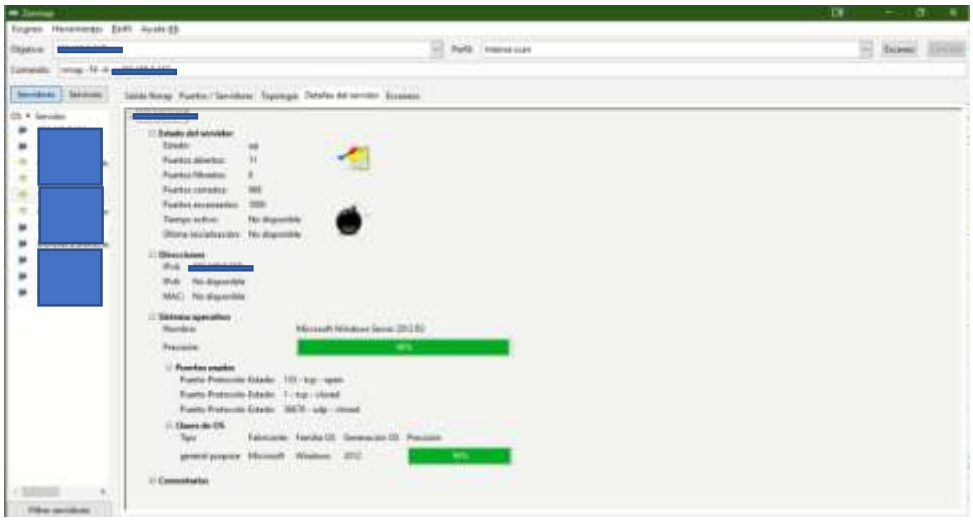


**Fig. 48.** Detalle de servidor de Base de Datos
**Fuente:** Elaborado por el Investigador

**Interpretación**:

Se realizó un análisis al servidor Aplicaciones en el cual se encontró 11 puertos abiertos, el mismo sistema operativo de Windows server 2012 y el puerto más vulnerable era el 135 tcp que usado por el protocolo msrpc.

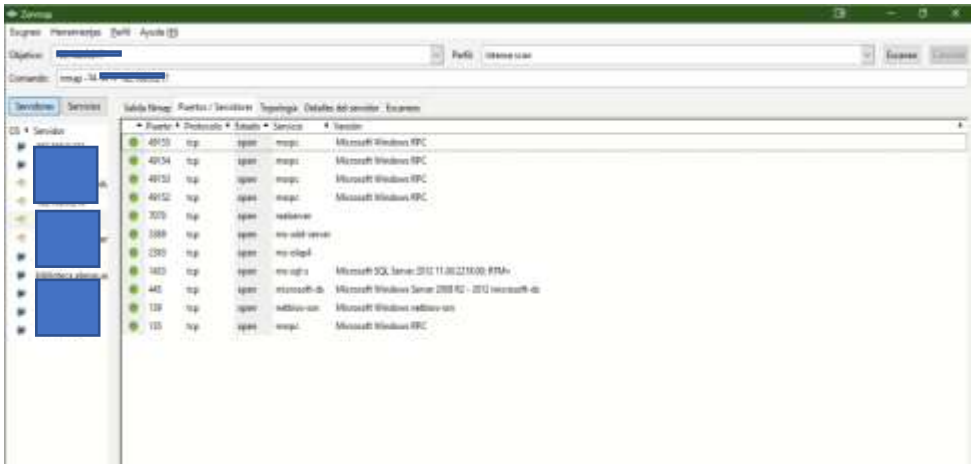


**Fig. 49.** Puertos abiertos servidor de Base de Datos
**Fuente:** Elaborado por el Investigador

**Interpretación**:

Se realizó un análisis de los puertos abiertos, donde se detectó una vulnerabilidad mayor fue en el puerto 135 tcp con su servicio msrcp que es la llamada de protección remota de Microsoft. Para esto Microsoft ha lanzado una serie de parches desde el 2003, muchas personas no tienen conocimiento de este servicio, pero puede ser afectado por virus existentes hay que tomar en cuenta los puertos TCP: 135, 139, 445, así como los inmediatamente superiores al 1024 (como el 1025 y el 1026) son objeto de ataque de código malicioso.

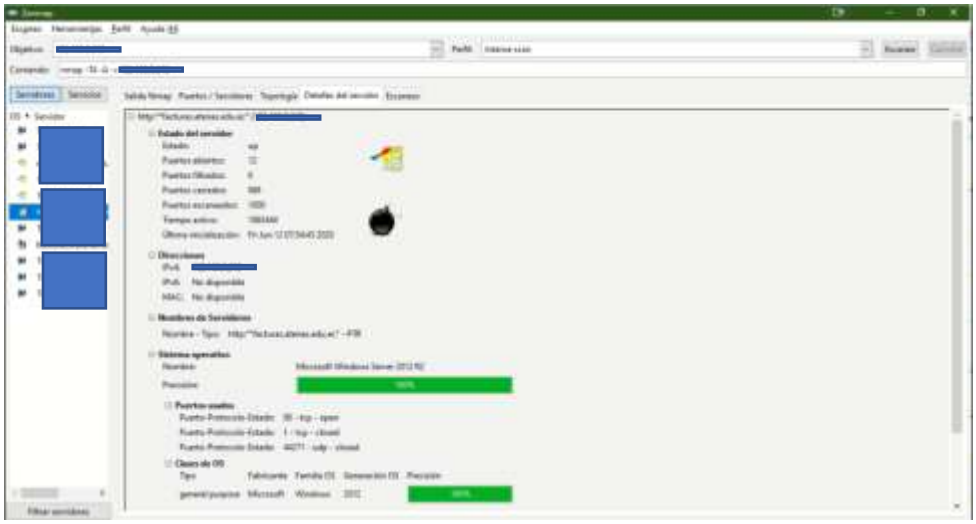


**Fig. 50.** Detalle de servidor de Facturación
**Fuente:** Elaborado por el Investigador

**Interpretación**:

Se realizó un análisis al servidor Aplicaciones en el cual se encontró 12 puertos abiertos, el mismo sistema operativo de Windows server 2012 y el puerto más vulnerable era el 80 HTTP de conexión de internet.

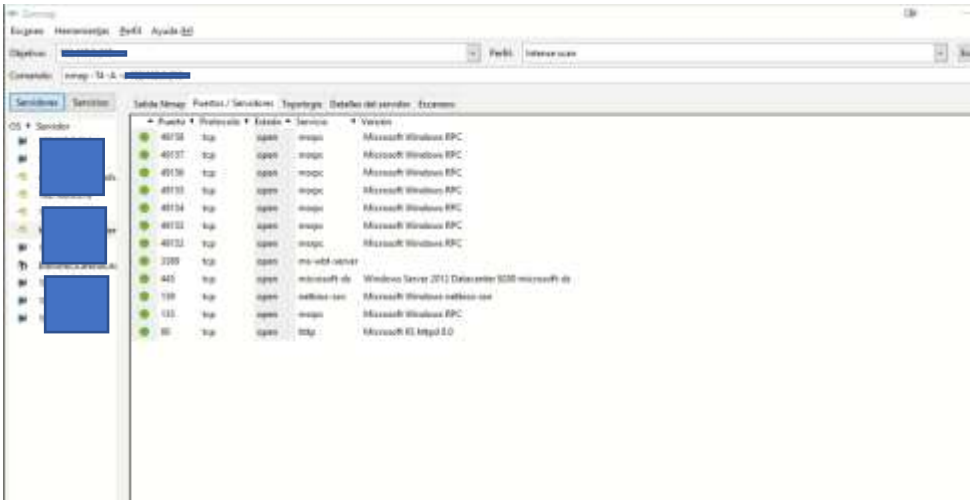


**Fig. 51.** Puertos abiertos servidor de Facturación
**Fuente:** Elaborado por el Investigador

**Interpretación**:

Se realizo un analisis de los puertos abiertos y se vi mayor vulnerabilidad en el puerto 80 HTTP, la solucion para esto seria ver que no existan reglas NAT sobre este puerto de ser el caso ver que en ninguna maquina exista alguna configuarcion como DMZ.

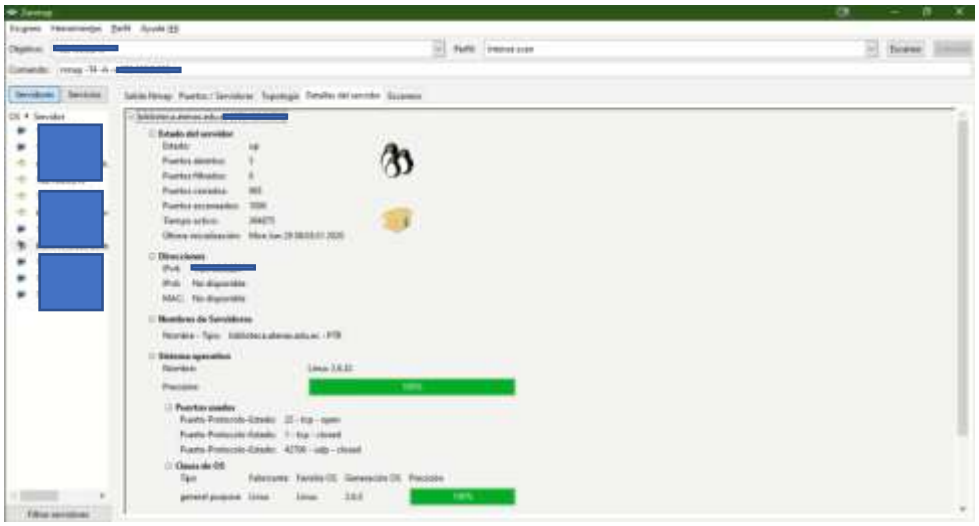


**Fig. 52.** Detalle de servidor de Biblioteca
**Fuente:** Elaborado por el Investigador

**Interpretación**:

Se realizó un análisis al servidor Aplicaciones en el cual se encontró 5 puertos abiertos, el mismo sistema operativo de Linux 2.6 32bits y el puerto más vulnerable era el 22 tcp que es el protocolo SSH.

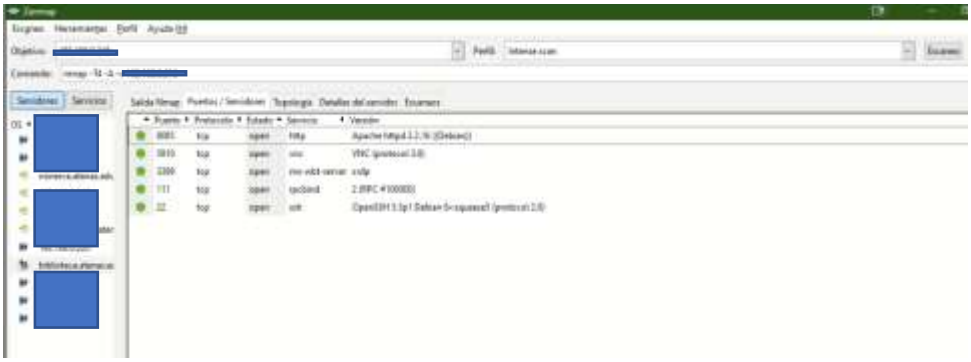


**Fig. 53.** Puertos abiertos servidor de Biblioteca
**Fuente:** Elaborado por el Investigador

**Interpretación**:

Se realizó un análisis de los puertos abiertos, donde se detectó una vulnerabilidad mayor fue en el puerto 22 y el 111. La solución sería deshabilitar los indicios de sesión del root ya que existen inicios de sesión de claves débiles los cuales pueden ser un factor de riesgo mayor, cambiar el SSH a un puerto mayor se debe dejar de usar Telnet y cerrar el puerto 23. Para el caso del puerto 111 que es el servicio de llamadas a procedimientos remotos, se recomienda desactivar el Portmapper junto con los servicios RPC que se estén ejecutando. Es necesario una configuración en el firewall que limite las solicitudes entrantes al servidor, configurando las direcciones IP para que los usuarios remotos accedan a los servicios del servidor.

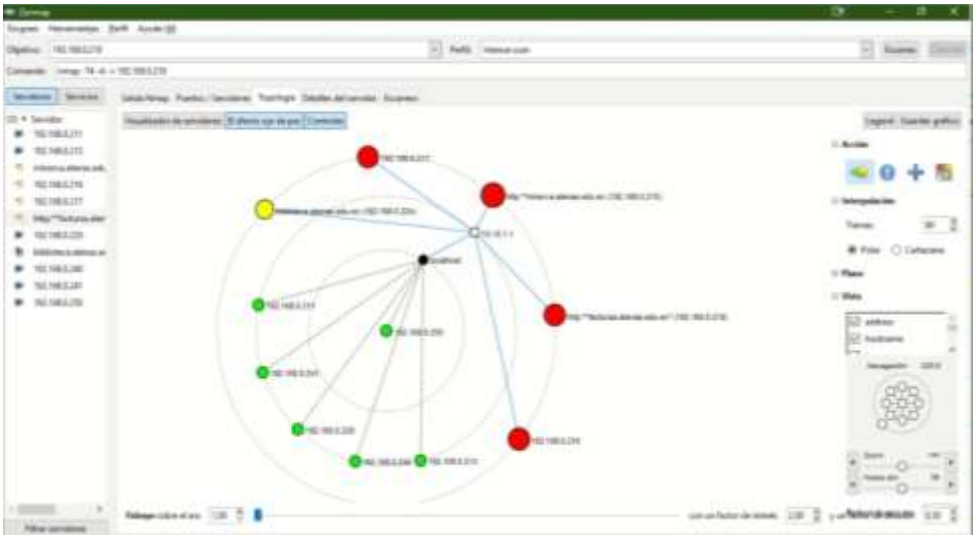


**Fig. 54.** Mapa de escaneo de vulnerabilidades
**Fuente:** Elaborado por el Investigador

Se puede apreciar en un mapa como se realizó el escaneo de vulnerabilidades a los servidores de la unidad educativa Atenas.

### 3.1.4.5.2. Búsqueda de vulnerabilidades con Nessus

Ataque al servidor de Facturas

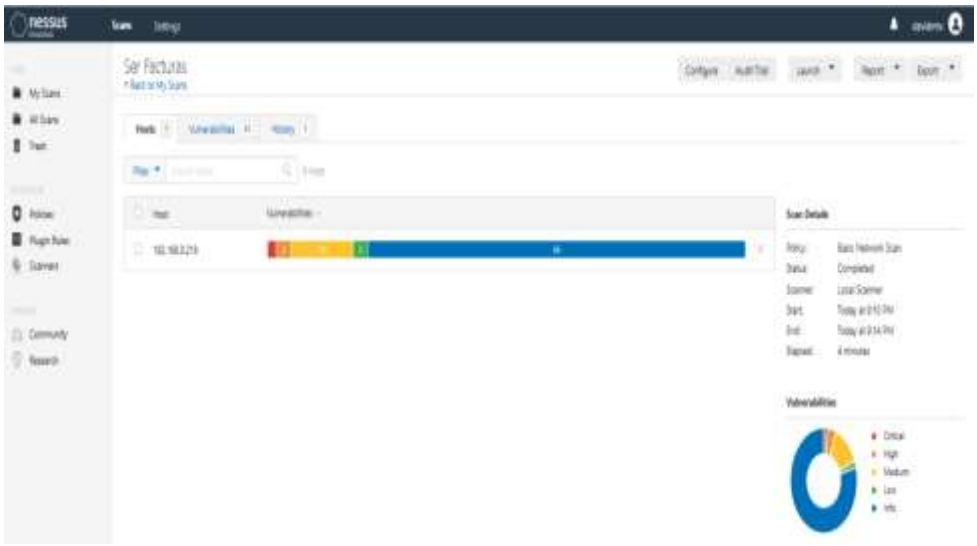


**Fig. 55.** Ataque al servidor de Facturación con nessus
**Fuente:** Elaborado por Nessus

Los resultados obtenidos en el escaneo de vulnerabilidades con Nessus al servidor de facturación fueron los siguientes:

1 vulnerabilidad critica, 2 altas, 10 medias, 2 bajas y 66 de información, entre las que se puede poner a conocimiento son las siguientes.

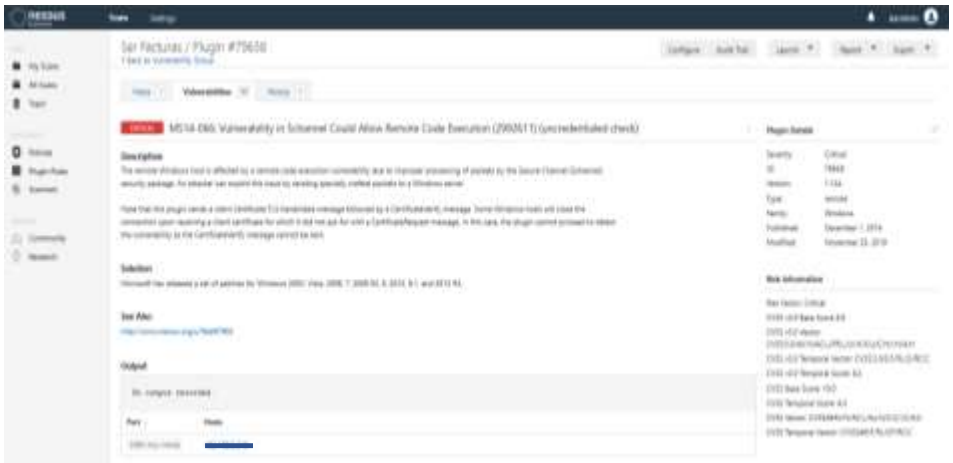


**Fig. 56.** Vulnerabilidad de ejecución remota de código
**Fuente:** Elaborado por Nessus

**Descripción**

El host remoto de Windows se ve afectado por una vulnerabilidad de ejecución remota de código debido al procesamiento incorrecto de los paquetes por el paquete de seguridad Secure Channel (Schannel). Un atacante puede explotar este problema enviando paquetes especialmente diseñados a un servidor de Windows.

Tenga en cuenta que este complemento envía un mensaje de protocolo de enlace de TLS de cliente seguido de un mensaje de verificación de certificado. Algunos hosts de Windows cerrarán la conexión al recibir un certificado de cliente para el que no solicitó con un mensaje CertificateRequest. En este caso, el complemento no puede detectar la vulnerabilidad ya que no se puede enviar el mensaje CertificateVerify.

**Solución**

Microsoft ha lanzado un conjunto de parches para Windows 2003, Vista, 2008, 7, 2008 R2, 8, 2012, 8.1 y 2012 R2.

También se puede ocupar lo que es cripto canal, canal seguro o un cripto sistema dependiendo el uso que se vaya a dar.

**Fig. 57.** Bloque de mensajes de servidor Microsoft 1.0 (SMBv1)
**Fuente:** Elaborado por Nessus

**Descripción**

El host remoto de Windows tiene habilitado el Bloque de mensajes de servidor Microsoft 1.0 (SMBv1). Por lo tanto, se ve afectado por múltiples vulnerabilidades:

Existen múltiples vulnerabilidades de divulgación de información en Microsoft Server Message Block 1.0 (SMBv1) debido a un manejo inadecuado de los paquetes SMBv1. Un atacante remoto no autenticado puede explotar estas vulnerabilidades, a través de un paquete SMBv1 especialmente diseñado, para revelar información confidencial. (CVE-2017-0267, CVE-2017-0268, CVE-2017-0270, CVE-2017-0271, CVE-2017-0274, CVE-2017-0275, CVE-2017-0276)

- Existen múltiples vulnerabilidades de denegación de servicio en Microsoft Server Message Block 1.0 (SMBv1) debido al manejo inadecuado de las solicitudes. Un atacante remoto no autenticado puede explotar estas vulnerabilidades, a través de una solicitud SMB especialmente diseñada, para que el sistema deje de responder. (CVE-2017-0269, CVE-2017-0273, CVE-2017-0280)

- Existen múltiples vulnerabilidades de ejecución remota de código en Microsoft Server Message Block 1.0 (SMBv1) debido al manejo inadecuado de los paquetes SMBv1. Un atacante remoto no autenticado puede explotar estas vulnerabilidades, a través de un paquete SMBv1 especialmente diseñado, para ejecutar código arbitrario. (CVE-2017-0272, CVE-2017-0277, CVE-2017-0278, CVE-2017-0279)

Dependiendo de la configuración de la política de seguridad del host, este complemento no siempre puede determinar correctamente si el host de Windows es vulnerable si el host está ejecutando una versión posterior de Windows (es decir, Windows 8.1, 10, 2012, 2012 R2 y 2016) específicamente las tuberías con nombre y Se puede acceder a los recursos compartidos de forma remota y anónima. Tenable no recomienda esta configuración, y los hosts deben verificarse localmente en busca de parches con uno de los siguientes complementos, según la versión de Windows: 100054, 100055, 100057, 100059, 100060 o 100061.

**Solución**

Aplique la actualización de seguridad aplicable para su versión de Windows:

- Windows Server 2008: KB4018466

- Windows 7: KB4019264

- Windows Server 2008 R2: KB4019264

- Windows Server 2012: KB4019216

- Windows 8.1 / RT 8.1. : KB4019215

- Windows Server 2012 R2: KB4019215

- Windows 10: KB4019474

- Windows 10 versión 1511: KB4019473

- Windows 10 versión 1607: KB4019472

- Windows 10 versión 1703: KB4016871

- Windows Server 2016: KB4019472

Es recomendado para las empresas que deshabiliten el acceso de SMBv1 para evitar el fallo de Microsoft porque es un protocolo ya poco usado.

**Fig. 58.** Bloque de mensajes de servidor Microsoft 1.0 (SMB SERVER)
**Fuente:** Elaborado por Nessus

## Descripción

El host remoto de Windows se ve afectado por las siguientes vulnerabilidades:

Existen múltiples vulnerabilidades de ejecución remota de código en Microsoft Server Message Block 1.0 (SMBv1) debido al manejo inadecuado de ciertas solicitudes. Un atacante remoto no autenticado puede explotar estas vulnerabilidades, a través de un paquete especialmente diseñado, para ejecutar código arbitrario. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)

Existe una vulnerabilidad de divulgación de información en Microsoft Server Message Block 1.0 (SMBv1) debido al manejo inadecuado de ciertas solicitudes. Un atacante remoto no autenticado puede explotar esto, a través de un paquete especialmente diseñado, para revelar información confidencial. (CVE-2017-0147)

ETERNALBLUE, ETERNALCHAMPION, ETERNALSANCE y ETERNALSYNERGY son cuatro de las múltiples vulnerabilidades y

exploits del Grupo de ecuaciones reveladas en 2017/04/14 por un grupo conocido como Shadow Brokers. WannaCry / WannaCrypt es un programa de ransomware que utiliza el exploit ETERNALBLUE, y EternalRocks es un gusano que utiliza siete vulnerabilidades de Equation Group. Petya es un programa de ransomware que primero utiliza CVE-2017-0199, una vulnerabilidad en Microsoft Office, y luego se propaga a través de ETERNALBLUE.

**Solución**

Microsoft lanzó un conjunto de parches para Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10 y 2016. Microsoft también lanzó parches de emergencia para sistemas operativos Windows que ya no son compatibles, incluidos Windows XP, 2003 y 8.

Para sistemas operativos Windows no compatibles, p. Windows XP, Microsoft recomienda que los usuarios suspendan el uso de SMBv1. SMBv1 carece de características de seguridad que se incluyeron en versiones posteriores de SMB. SMBv1 puede deshabilitarse siguiendo las instrucciones del proveedor proporcionadas en Microsoft KB2696547. Además, US-CERT recomienda que los usuarios bloqueen SMB directamente bloqueando el puerto TCP 445 en todos los dispositivos de límite de red. Para SMB sobre la API NetBIOS, bloquee los puertos TCP 137/139 y los puertos UDP 137/138 en todos los dispositivos de límite de red.

**Fig. 59.** Vulnerabilidad de elevación de privilegios en los protocolos del Administrador de cuentas de seguridad (SAM)
**Fuente:** Elaborado por Nessus

**Descripción**

El host remoto de Windows se ve afectado por una vulnerabilidad de elevación de privilegios en los protocolos del Administrador de cuentas de

seguridad (SAM) y de la Autoridad de seguridad local (Política de dominio) (LSAD) debido a una negociación inadecuada del nivel de autenticación sobre los canales de Llamada a procedimiento remoto (RPC). Un atacante man-in-the-middle capaz de interceptar las comunicaciones entre un cliente y un servidor que aloja una base de datos SAM puede explotar esto para forzar la disminución del nivel de autenticación, permitiendo que el atacante se haga pasar por un usuario autenticado y acceda a la base de datos SAM.

### Solución

Microsoft ha lanzado un conjunto de parches para Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2 y 10.

Esta actualización se la realiza por Windows Update automáticamente lo que hay que tener en cuenta es ver la versión y la compatibilidad.

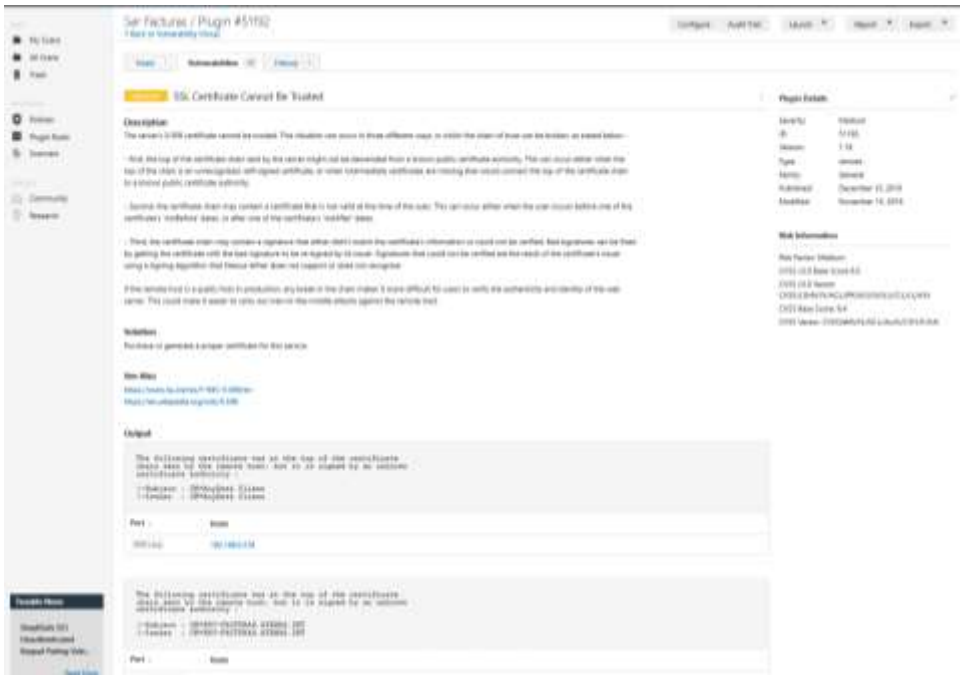


**Fig. 60.** El certificado SSL no se puede traspasar
**Fuente:** Elaborado por Nessus

### Descripción

No se puede confiar en el certificado X.509 del servidor. Esta situación puede ocurrir de tres maneras diferentes, en las cuales se puede romper la cadena de confianza, como se indica a continuación:

Primero, la parte superior de la cadena de certificados enviada por el servidor podría no descender de una autoridad de certificación pública conocida. Esto

puede ocurrir cuando la parte superior de la cadena es un certificado autofirmado no reconocido o cuando faltan certificados intermedios que conectarían la parte superior de la cadena de certificados a una autoridad de certificación pública conocida.

Segundo, la cadena de certificados puede contener un certificado que no es válido en el momento del escaneo. Esto puede ocurrir cuando el escaneo ocurre antes de una de las fechas 'no antes' del certificado, o después de una de las fechas 'no después' del certificado.

Tercero, la cadena de certificados puede contener una firma que no coincide con la información del certificado o que no se pudo verificar. Las firmas incorrectas se pueden corregir haciendo que el emisor vuelva a firmar el certificado con la firma incorrecta. Las firmas que no se pudieron verificar son el resultado de que el emisor del certificado utiliza un algoritmo de firma que Nessus no admite o no reconoce.

Si el host remoto es un host público en producción, cualquier interrupción en la cadena hace que sea más difícil para los usuarios verificar la autenticidad e identidad del servidor web. Esto podría facilitar la realización de ataques de hombre en el medio contra el host remoto.

**Solución**

Compre o genere un certificado adecuado para este servicio. Se podría importar el certificado PEM en formato (.crt)

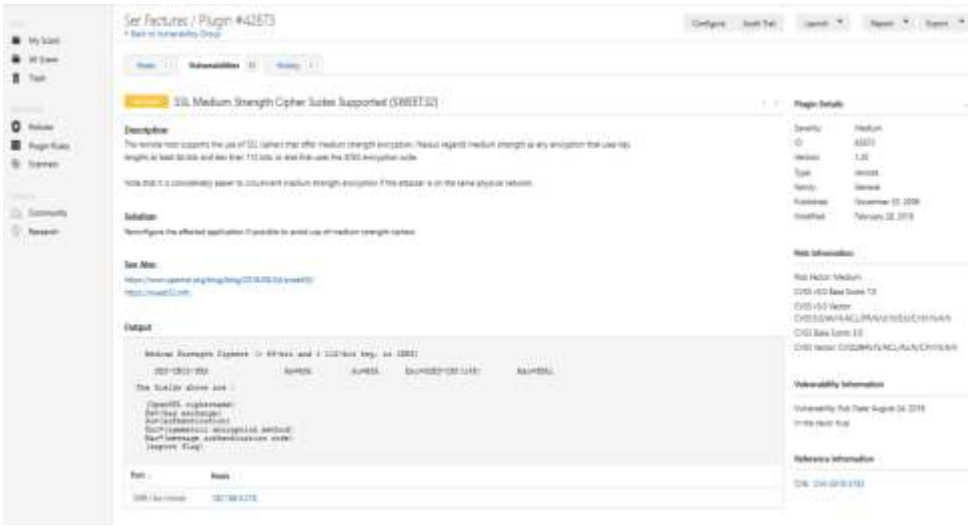


**Fig. 61.** SSL ofrecen cifrado de fuerza media
**Fuente:** Elaborado por Nessus

**Descripción**

El host remoto admite el uso de cifrados SSL que ofrecen cifrado de fuerza media. Nessus considera la fuerza media como cualquier encriptación que usa longitudes de clave de al menos 64 bits y menos de 112 bits, o que usa el conjunto de encriptación 3DES.

Tenga en cuenta que es considerablemente más fácil eludir el cifrado de potencia media si el atacante está en la misma red física.

**Solución**

Vuelva a configurar la aplicación afectada si es posible para evitar el uso de cifrados de fuerza media.

Tomando en cuenta que el servidor no posee una encriptacion se recomienda el algoritmo AES (Advanced Encrytion Standar) que usa varias sustituciones y transformaciones lineales ejecutandose en bloques de 16 bytes. Por lo que es mas rapido que 3DES.

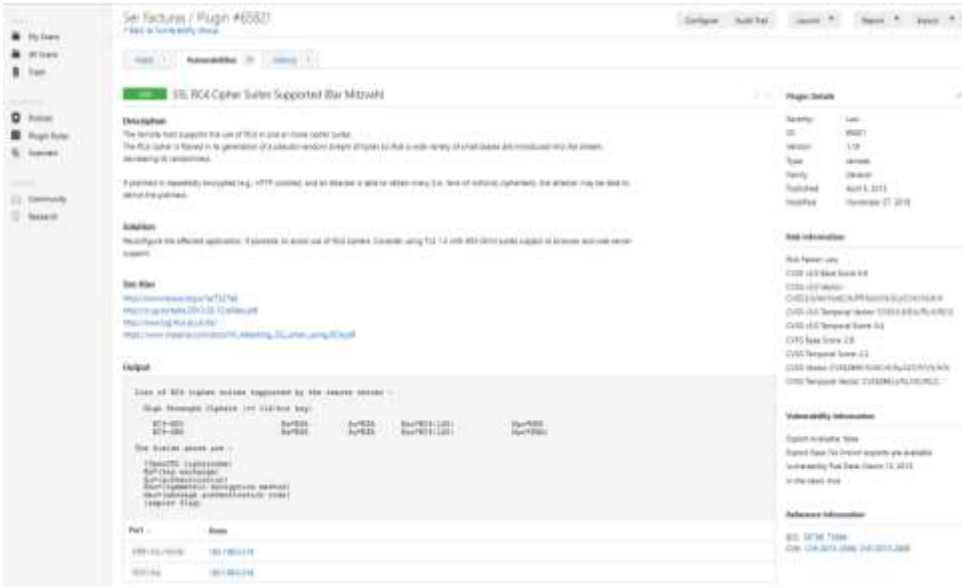


**Fig. 62.** Uso de RC4 en uno o más conjuntos de cifrado
**Fuente:** Elaborado por Nessus

**Descripción**

El host remoto admite el uso de RC4 en uno o más conjuntos de cifrado.

El cifrado RC4 tiene fallas en su generación de una secuencia de bytes pseudoaleatoria, por lo que se introduce una gran variedad de pequeños sesgos en la secuencia, lo que disminuye su aleatoriedad.

Si el texto sin formato se cifra varias veces (por ejemplo, cookies HTTP) y un atacante puede obtener muchos (por ejemplo, decenas de millones) de textos cifrados, el atacante puede obtener el texto sin formato.

## Solución

Vuelva a configurar la aplicación afectada, si es posible, para evitar el uso de cifrados RC4. Este algoritmo de cifrado tenía un problema el cual en claves débiles proporcionaba información acerca de la clave para lo cual se debe descartar la parte inicial de los bytes y se corrige el problema. Considere usar TLS 1.2 con las suites AES-GCM sujetas a la compatibilidad con el navegador y el servidor web.

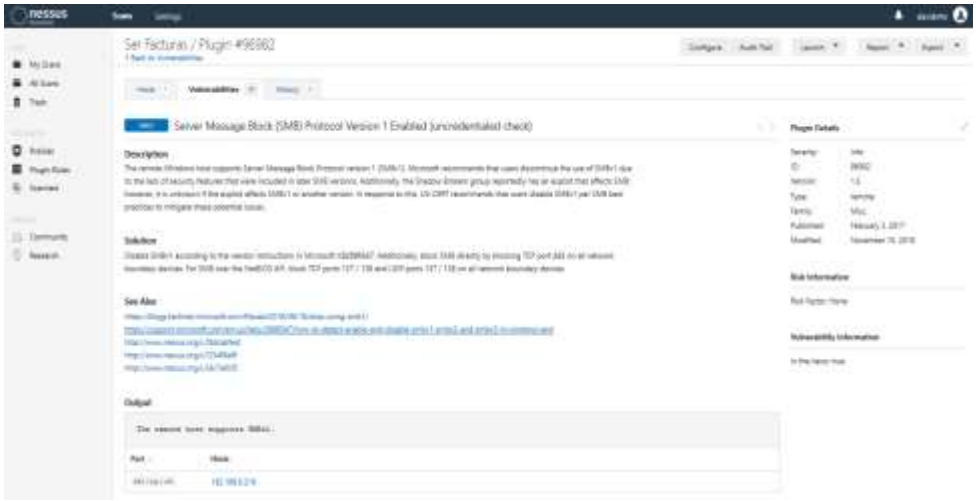


**Fig. 63.** Windows es compatible con el Protocolo de bloqueo de mensajes del servidor versión 1 (SMBv1)
**Fuente:** Elaborado por Nessus

## Descripción

El host remoto de Windows es compatible con el Protocolo de bloqueo de mensajes del servidor versión 1 (SMBv1). Microsoft recomienda que los usuarios suspendan el uso de SMBv1 debido a la falta de características de seguridad que se incluyeron en versiones posteriores de SMB. Además, el grupo Shadow Brokers, según los informes, tiene una vulnerabilidad que afecta a SMB; sin embargo, se desconoce si el exploit afecta a SMBv1 u otra versión. En respuesta a esto, US-CERT recomienda que los usuarios deshabiliten SMBv1 según las mejores prácticas de SMB para mitigar estos posibles problemas.

## Solución

Deshabilite SMBv1 de acuerdo con las instrucciones del proveedor en Microsoft KB2696547. Además, bloquee SMB directamente bloqueando el puerto TCP 445 en todos los dispositivos de límite de red. Para SMB sobre la API NetBIOS, bloquee los puertos TCP 137/139 y los puertos UDP 137/138 en todos los dispositivos de límite de red.

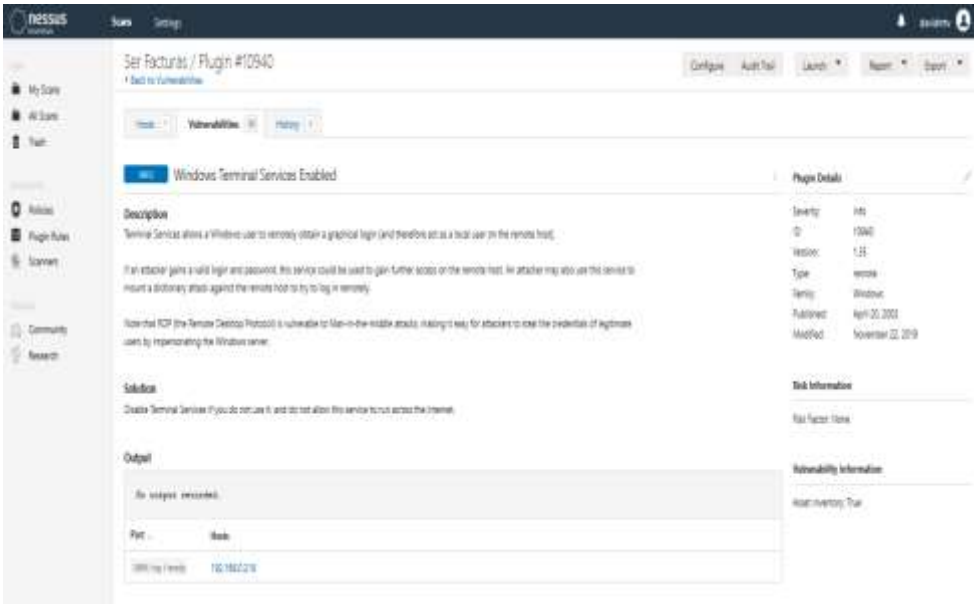



**Fig. 64.** Servicio terminal permite a un usuario de Windows
**Fuente:** Elaborado por Nessus

## Descripción

Terminal Services permite a un usuario de Windows obtener de forma remota un inicio de sesión gráfico (y, por lo tanto, actuar como un usuario local en el host remoto).

Si un atacante obtiene un inicio de sesión y una contraseña válidos, este servicio podría utilizarse para obtener más acceso en el host remoto. Un atacante también puede usar este servicio para montar un ataque de diccionario contra el host remoto para intentar iniciar sesión de forma remota.

Tenga en cuenta que RDP (el Protocolo de escritorio remoto) es vulnerable a los ataques Man-in-the-middle, lo que facilita a los atacantes robar las credenciales de los usuarios legítimos al hacerse pasar por el servidor de Windows.

## Solución

Deshabilite los Servicios de Terminal Server si no lo usa, y no permita que este servicio se ejecute a través de Internet.

Además, se puede usar credencial de Guard remoto de Windows defender la cual redirige las solicitudes de kerberos del dispositivo que pide la conexión, es muy útil ya que si esta se ve comprometida sus credenciales no serán expuestas ya nunca pasan atreves de la red y al dispositivo destino.

**SERVIDOR DE BIBLIOTECA**

Los resultados obtenidos en el escaneo de vulnerabilidades con nessus al servidor de biblioteca fueron los siguientes:

2 vulnerabilidades medias, 2 bajas y 24 de información, entre las que se poner a conocimiento son las siguientes.

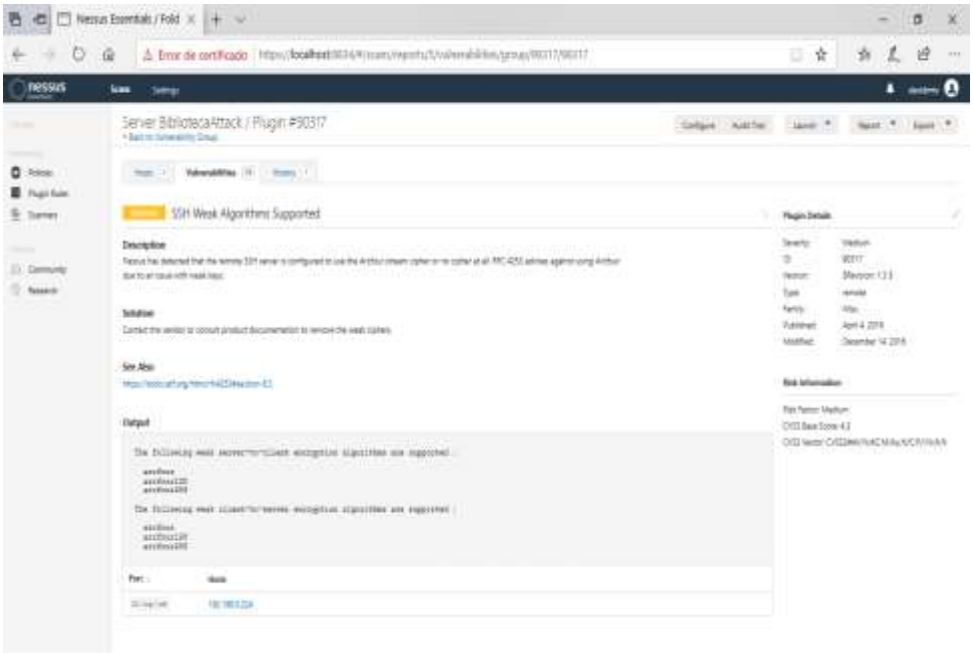



**Fig. 65.** Ataque al servidor de Base de Datos con cifrado de flujo
**Fuente:** Elaborado por Nessus

**Descripción**

Nessus ha detectado que el servidor SSH remoto está configurado para usar el cifrado de flujo Arcfour o ningún cifrado. RFC 4253 desaconseja el uso de Arcfour debido a un problema con claves débiles.

**Solución**

Usar claves efectivas de longitudes de 128 bits o más, tomando en cuenta la encriptación del algoritmo dado usándolo en ambas direcciones independientemente uno del otro. También podemos incluir el cifrado hash o SHA-1 el cual nos ayuda en claves débiles.

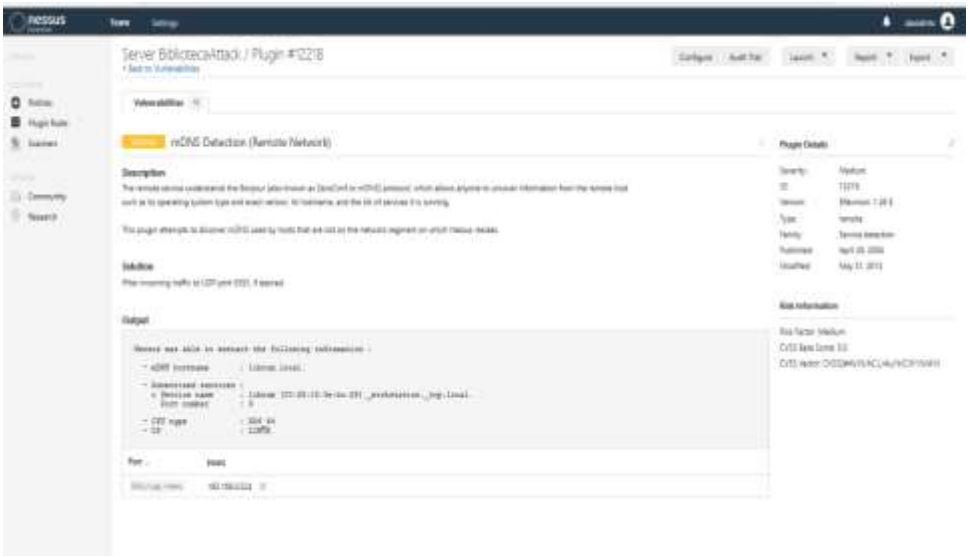


**Fig. 66.** Protocolo Bonjour
**Fuente:** Elaborado por Nessus

### Descripción

El servicio remoto comprende el protocolo Bonjour (también conocido como ZeroConf o mDNS), que permite a cualquier persona descubrir información del host remoto, como el tipo de sistema operativo y la versión exacta, su nombre de host y la lista de servicios que está ejecutando.

Este complemento intenta descubrir los mDNS utilizados por los hosts que no están en el segmento de red en el que reside Nessus.

### Solución

Filtre el tráfico entrante al puerto UDP 5353, permitiendo conexión de direcciones IP o host confiables debido a que no realiza la verificación y corrección de errores. Es recomendable desactivar el servicio si no es utilizado.

**Fig. 67.** SSH admite el cifrado Cipher Block Chaining (CBC)
**Fuente:** Elaborado por Nessus

**Descripción**

El servidor SSH está configurado para admitir el cifrado Cipher Block Chaining (CBC). Esto puede permitir que un atacante recupere el mensaje de texto sin formato del texto cifrado.

Tenga en cuenta que este complemento solo busca las opciones del servidor SSH y no busca versiones de software vulnerables.

**Solución**

Deshabilitar el cifrado en modo CBC y habilitar el cifrado en modo de cifrado CTR o GCM ya que estos son cifrados de bloques en cifrados de flujos.

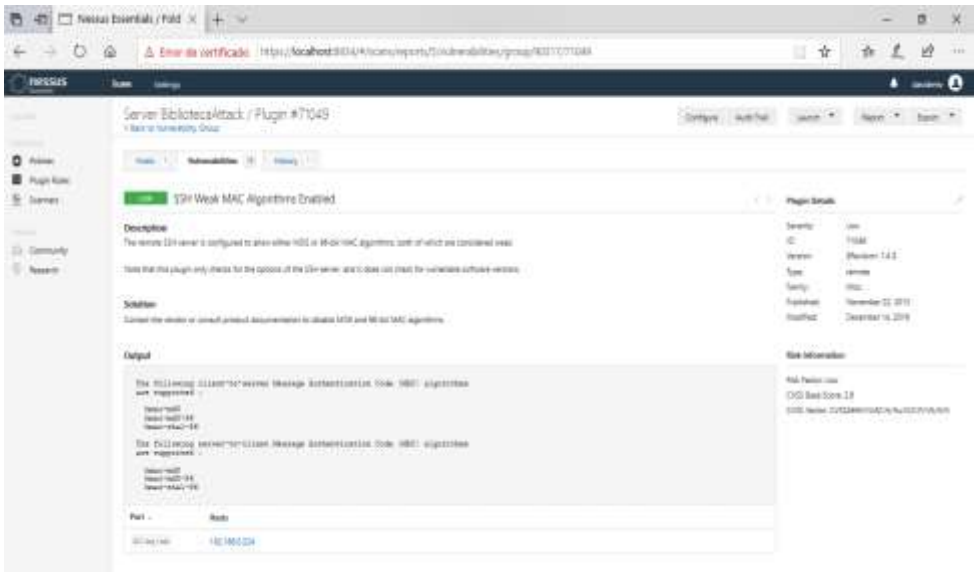


**Fig. 68.** SSH remoto permite algoritmos MAC MD5 o de 96 bits
**Fuente:** Elaborado por Nessus

**Descripción**

El servidor SSH remoto está configurado para permitir algoritmos MAC MD5 o de 96 bits, los cuales se consideran débiles.

Tenga en cuenta que este complemento solo busca las opciones del servidor SSH y no busca versiones de software vulnerables.

**Solución**

Desactivar los algoritmos MD5 y MAC de 96 bits y añadir algoritmos criptográficos a la selección VPN para atributos de asociaciones de seguridad de Política de intercambio de datos usando cifrado, Hash/PRF, Diffie-Hellman y para políticas de datos usar validaciones de autenticación.

**SERVIDOR DE BASE DE DATOS**


**Fig. 69.** Ataque al servidor de Base de Datos con nessus
**Fuente:** Elaborado por Nessus

Los resultados obtenidos en el escaneo de vulnerabilidades con nessus al servidor de biblioteca fueron los siguientes:

2 vulnerabilidades medias, 2 bajas y 24 de información, entre las que se puede poner a conocimiento son las siguientes.


**Fig. 70.** Detección de protocolo SSL

**Fuente:** Elaborado por Nessus

**Solución**:

Al usar SSL son susceptibles a ataques de hombre en medio que puede capturar la comunicación y romper el cifrado del lado del cliente, se puede utilizar protocolo TSL con seguridad en la capa de transporte lo que proporciona una conexión segura.


**Fig. 71.** Vulnerabilidad en el certificado SSL
**Fuente:** Elaborado por Nessus

**Solución**:

Al usar certificados SSL hay que realizar una configuración para evitar vulnerabilidades, primero el DNS debe tener un registro CAA el cual incluye Digicert que presenta una alerta, una etiqueta y un valor.


**Fig. 72.** Vulnerabilidad en firma SMB
**Fuente:** Elaborado por Nessus

**Solución**:

Se puede aplicar parches de seguridad de Windows según la versión para su respectiva actualización estando disponible en Microsoft Windows update, además se puede configurar el firewall deshabilitan el puerto 445 al menos que sea necesario.


**Fig. 73.** Certificados SSL contiene claves RSA
**Fuente:** Elaborado por Nessus

**SERVIDOR DE ACTIVE**


**Fig. 74.** Ataque al servidor Active Directory con Nessus
**Fuente:** Elaborado por Nessus

Los resultados obtenidos en el escaneo de vulnerabilidades con nessus al servidor de biblioteca fueron los siguientes:

1 vulnerabilidad alta, 1 bajas y 37 de información, entre las que se puede poner a conocimiento son las siguientes.


**Fig. 75.** Protocolo SSL en Active Directory
**Fuente:** Elaborado por Nessus


**Fig. 76.** Servidor DNS Snooping
**Fuente:** Elaborado por Nessus

**Solución**:

Se puede deshabilitar la recursividad si el servidor DNS se encuentra en una red corporativa donde clientes externos pueden ingresar, limitando el acceso a clientes públicos.


**Fig. 77.** SSL firmado con algoritmo hash débil
**Fuente:** Elaborado por Nessus

**Solución**:

Renovar el certificado usando un algoritmo hash compatible, SHA-2 es un algoritmo un poco más seguro anteriormente MD5 se pensó que era segura y poco descifrable.

## Suites de cifrado SSL de resistencia media compatibles (SWEET32)

ID de complemento Nessus 42873

### Sinopsis

El servicio remoto admite el uso de cifrados SSL de potencia media.

### Descripción

El host remoto admite el uso de cifrados SSL que ofrecen cifrado de fuerza media. Nessus considera la fuerza media como cualquier encriptación que usa longitudes de clave de al menos 64 bits y menos de 112 bits, o que usa el conjunto de encriptación 3DES.
Tenga en cuenta que es considerablemente más fácil eludir el cifrado de potencia media si el atacante está en la misma red física.

### Solución

Vuelva a configurar la aplicación afectada si es posible para evitar el uso de cifrados de fuerza media.

### Detalles del complemento

**Severidad :** media
**ID :** 42873
**Nombre de archivo :** ssl_medium_supported_ciphers.nasl
**Versión :** 1.20
**Tipo :** remoto
**Familia :** general
**Publicado :** 23/11/2009
**Actualizado :** 28/02/2019
**Dependencias :** 21643

**Fig. 78.** SSL (SWEET32)
**Fuente:** Elaborado por Nessus

## SSLv3 Padding Oracle en la vulnerabilidad de cifrado heredado degradado (POODLE)

ID del complemento Nessus 78479

### Sinopsis

Es posible obtener información confidencial del host remoto con servicios habilitados para SSL / TLS.

### Descripción

El host remoto se ve afectado por una vulnerabilidad de divulgación de información man-in-the-middle (MitM) conocida como POODLE. La vulnerabilidad se debe a la forma en que SSL 3.0 maneja los bytes de relleno al descifrar mensajes cifrados usando cifrados de bloque en modo de encadenamiento de bloque de cifrado (CBC).
Los atacantes MitM pueden descifrar un byte seleccionado de un texto cifrado en tan solo 256 intentos si pueden forzar a una aplicación víctima a enviar repetidamente los mismos datos a través de conexiones SSL 3.0 recién creadas.
Mientras un cliente y un servicio sean compatibles con SSLv3, una conexión se puede 'revertir' a SSLv3, incluso si el cliente y el servicio admiten TLSv1 o más reciente.

El mecanismo TLS Fallback SCSV evita los ataques de 'reversión de versiones' sin afectar a los clientes heredados; sin embargo, solo puede proteger las conexiones cuando el cliente y el servicio admiten el mecanismo. Los sitios que no pueden deshabilitar SSLv3 de inmediato deben habilitar este mecanismo.
Esta es una vulnerabilidad en la especificación SSLv3, no en ninguna implementación de SSL en particular. Deshabilitar SSLv3 es la única forma de mitigar por completo la vulnerabilidad.

### Solución

Deshabilitar SSLv3.
Los servicios que deben ser compatibles con SSLv3 deben habilitar el mecanismo TLS Fallback SCSV hasta que SSLv3 se pueda deshabilitar.

### Detalles del complemento

**Severidad :** media
**ID :** 78479
**Nombre de archivo :** ssl_poodle.nasl
**Versión :** 1.22
**Tipo :** remoto
**Familia :** general
**Publicado :** 15/10/2014
**Actualizado :** 2019/11/25
**Dependencias :** 56984 , 21643

### Información de riesgo

**Factor de riesgo :** medio
**Fuente de puntaje CVSS :** CVE-2014-3566

**CVSS v2.0**

**Puntaje base :** 4.3
**Puntuación temporal :** 3.2
**Vector :** CVSS2 # AV: N / AC: M / Au: N / C
**Vector temporal :** CVSS2 # E: U / RL: OF /

**Fig. 79.** SSLv3 vulnerabilidad de cifrado heredado (POODLE)
**Fuente:** Elaborado por Nessus

**Solución**:

Actualizar el SSL 3.0 o sus versiones anteriores en el servidor, ya que aún se usan en los navegadores de manera sencilla pero esto se solucionan usando un cifrado TSL1.0.

**SERVIDOR DE APLICACIONES**


**Fig. 80.** Ataque servidor Aplicaciones con nessus
**Fuente:** Elaborado por Nessus

Los resultados obtenidos en el escaneo de vulnerabilidades con nessus al servidor de biblioteca fueron los siguientes:

18 vulnerabilidades críticas, 41 altas, 72 medias, 5 bajas y 126 de información, entre las que se puede poner a conocimiento son las siguientes.


**Fig. 81.** RCE(Ejecución de Código Remoto)
**Fuente:** Elaborado por Nessus

**Solución**:

La ejecución de código remoto nos puede permitir acceder a una red pasando los firewalls en el cual el atacante puede inyectar comandos http.log, leer archivos de extensión .doc .txt e incluso obtener tokens de inicio de sesión.

Se debe deshabilitar los servicios http y https cuando no estén en uso.

89081 - OpenSSL 1.0.1 <1.0.1s Múltiples vulnerabilidades (DROWN)

**Sinopsis**

El servicio remoto se ve afectado por múltiples vulnerabilidades.

**Descripción**

Según su banner, el host remoto está ejecutando una versión de OpenSSL 1.0.1 anterior a 1.0.1s. Por lo tanto, se ve afectado por las siguientes vulnerabilidades:

- Existe una vulnerabilidad de divulgación clave debido al manejo inadecuado de los conflictos de bancos de caché en la microarquitectura Intel Sandy-bridge. Un atacante puede explotar esto para obtener acceso a la información clave de RSA.
(CVE-2016-0702)

: existe un error de doble libre debido a una validación incorrecta de la entrada proporcionada por el usuario al analizar las claves privadas DSA con formato incorrecto. Un atacante remoto puede explotar esto para dañar la memoria, lo que resulta en una condición de denegación de servicio o la ejecución de código arbitrario. (CVE-2016-0705)

- Existe un defecto de desreferencia de puntero NULL en las funciones BN_hex2bn () y BN_dec2bn (). Un atacante remoto puede explotar esto para desencadenar una corrupción del montón, lo que resulta en la ejecución de código arbitrario. (CVE-2016-0797)

: existe una vulnerabilidad de denegación de servicio debido al manejo inadecuado de nombres de usuario no válidos. Un atacante remoto puede explotar esto, a través de un nombre de usuario especialmente diseñado, para perder 300 bytes de memoria por conexión, agotando los recursos de memoria disponibles. (CVE-2016-0798)

- Existen múltiples problemas de corrupción de memoria que permiten que un atacante remoto cause una condición de denegación de servicio o la ejecución de código arbitrario. (CVE-2016-0799)

- Existe una falla que permite un ataque de oráculo de relleno Bleichenbacher de protocolo cruzado conocido como DROWN (descifrar RSA con cifrado obsoleto y debilitado).
Esta vulnerabilidad existe debido a una falla en la implementación de Secure Sockets Layer Versión 2 (SSLv2), y permite descifrar el tráfico TLS capturado. Un atacante man-in-the-middle puede explotar esto para descifrar la conexión TLS utilizando tráfico previamente capturado y criptografía débil junto con una serie de conexiones especialmente diseñadas a un servidor SSLv2 que usa la misma clave privada. (CVE-2016-0800)

**Ver también**

https://www.openssl.org/news/secadv/20160301.txt
https://www.openssl.org/news/cl101.txt
https://drownattack.com/

**Solución**

Actualice a OpenSSL versión 1.0.1s o posterior.

**Fig. 82.** Múltiples vulnerabilidades (DROWN)
**Fuente:** Elaborado por Nessus

## **Solución**:

Al usar SSLv2 o su llave privada un servidor de las mismas características puede tener acceso a la información por lo que es necesario actualizar las versiones de OpenSSL.

78555 - OpenSSL no compatible

**Sinopsis**

Se está ejecutando un servicio no compatible en el host remoto.

**Descripción**

Según su banner, el servidor web remoto está ejecutando una versión de OpenSSL que ya no es compatible.

La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, es probable que contenga vulnerabilidades de seguridad.

**Ver también**

https://www.openssl.org/policies/releasestrat.html
http://www.nessus.org/u?4d55548d

**Solución**

Actualice a una versión de OpenSSL que sea compatible actualmente.

**Fig. 83.** OpenSSL no compatible
**Fuente:** Elaborado por Nessus

**Solución**:

Actualizar la versión de OpenSSL a una que sea compatible tomando en cuenta los enlaces de las páginas del fabricante.

**81511 - PHP 5.5.x <5.5.22 Vulnerabilidades múltiples (GHOST)**

**Sinopsis**

El servidor web remoto utiliza una versión de PHP que se ve afectada por múltiples vulnerabilidades.

**Descripción**

Según su banner, la versión de PHP 5.5.x instalada en el host remoto es anterior a 5.5.22. Por lo tanto, se ve afectado por múltiples vulnerabilidades

- Un defecto de desbordamiento del búfer basado en el montón en la función enchant_broker_request_dict en ext / enchant / enchant.c podría permitir que un atacante remoto provoque un desbordamiento del búfer, resultando en una condición de denegación de servicio o la ejecución de código arbitrario. (CVE-2014-9705)

- Un defecto de desbordamiento del búfer basado en el montón en la Biblioteca GNU C (glibc) debido a una validación incorrecta de la entrada suministrada por el usuario en las funciones glibc __nss_hostname_digits_dots (), gethostbyname () y gethostbyname2 (). Esto permite que un atacante remoto provoque un desbordamiento del búfer, lo que da como resultado una condición de denegación de servicio o la ejecución de código arbitrario. (CVE-2015-0235)

- Existe una falla de uso libre después en la función php_date_timezone_initialize_from_hash () dentro del script 'ext / date / php_date.c'. Un atacante puede explotar esto para acceder a información confidencial o bloquear aplicaciones vinculadas a PHP. (CVE-2015-0273)

- Una vulnerabilidad de uso libre después de la función phar_rename_archive en phar_object.c podría permitir que un atacante remoto cause una denegación de servicio. (CVE-2015-2301)

- Existe una falla de entidad externa XML (XXE) en el componente PHP-FPM debido al análisis incorrecto de datos XML. Un atacante remoto puede explotar esto, a través de datos XML especialmente diseñados, para revelar información confidencial o causar una denegación de servicio. (CVE-2015-8866) Tenga en cuenta que Nessus no ha intentado explotar estos problemas, sino que se ha basado únicamente en el número de versión autoinformado de la aplicación.

**Ver también**

http://php.net/ChangeLog-5.php#5.5.22
https://bugs.php.net/bug.php?id=68925
https://bugs.php.net/bug.php?id=68942
http://www.nessus.org/u?c7afddbd

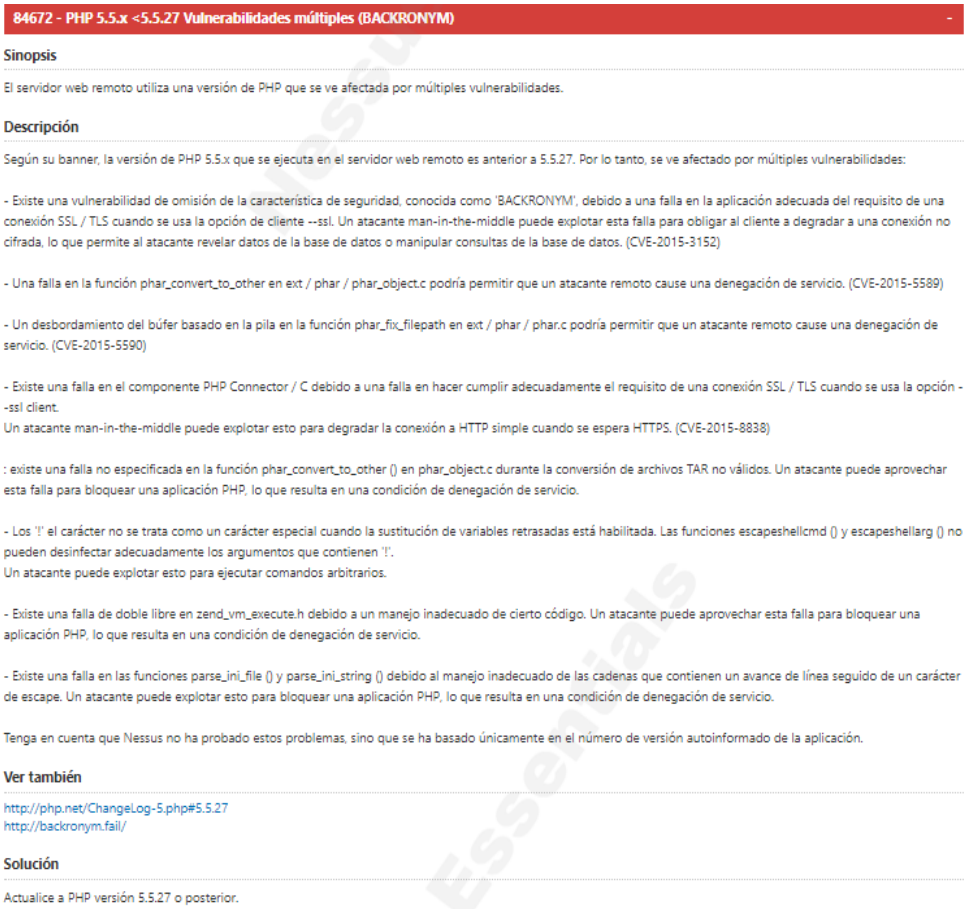
**Solución**

Actualice a PHP versión 5.5.22 o posterior.

**Fig. 84.** Vulnerabilidades múltiples (Ghost)
**Fuente:** Elaborado por Nessus

**Solución**:

Esta es una de las vulnerabilidades mas severas ya que emplea la biblioteca glibc, lo que provoca que servidores que soportan gran cantidad de sistemas. Se puede corregir el esta vulnerabilidad aplicando el parche que el proveedor de Linux proporciona desde los enlaces permitidos.



84672 - PHP 5.5.x <5.5.27 Vulnerabilidades múltiples (BACKRONYM)

Sinopsis

El servidor web remoto utiliza una versión de PHP que se ve afectada por múltiples vulnerabilidades.

Descripción

Según su banner, la versión de PHP 5.5.x que se ejecuta en el servidor web remoto es anterior a 5.5.27. Por lo tanto, se ve afectado por múltiples vulnerabilidades:

- Existe una vulnerabilidad de omisión de la característica de seguridad, conocida como 'BACKRONYM', debido a una falla en la aplicación adecuada del requisito de una conexión SSL / TLS cuando se usa la opción de cliente --ssl. Un atacante man-in-the-middle puede explotar esta falla para obligar al cliente a degradar a una conexión no cifrada, lo que permite al atacante revelar datos de la base de datos o manipular consultas de la base de datos. (CVE-2015-3152)

- Una falla en la función phar_convert_to_other en ext / phar / phar_object.c podría permitir que un atacante remoto cause una denegación de servicio. (CVE-2015-5589)

- Un desbordamiento del búfer basado en la pila en la función phar_fix_filepath en ext / phar / phar.c podría permitir que un atacante remoto cause una denegación de servicio. (CVE-2015-5590)

- Existe una falla en el componente PHP Connector / C debido a una falla en hacer cumplir adecuadamente el requisito de una conexión SSL / TLS cuando se usa la opción --ssl client.
Un atacante man-in-the-middle puede explotar esto para degradar la conexión a HTTP simple cuando se espera HTTPS. (CVE-2015-8838)

: existe una falla no especificada en la función phar_convert_to_other () en phar_object.c durante la conversión de archivos TAR no válidos. Un atacante puede aprovechar esta falla para bloquear una aplicación PHP, lo que resulta en una condición de denegación de servicio.

- Los '!' el carácter no se trata como un carácter especial cuando la sustitución de variables retrasadas está habilitada. Las funciones escapeshellcmd () y escapeshellarg () no pueden desinfectar adecuadamente los argumentos que contienen '!'.
Un atacante puede explotar esto para ejecutar comandos arbitrarios.

- Existe una falla de doble libre en zend_vm_execute.h debido a un manejo inadecuado de cierto código. Un atacante puede aprovechar esta falla para bloquear una aplicación PHP, lo que resulta en una condición de denegación de servicio.

- Existe una falla en las funciones parse_ini_file () y parse_ini_string () debido al manejo inadecuado de las cadenas que contienen un avance de línea seguido de un carácter de escape. Un atacante puede explotar esto para bloquear una aplicación PHP, lo que resulta en una condición de denegación de servicio.

Tenga en cuenta que Nessus no ha probado estos problemas, sino que se ha basado únicamente en el número de versión autoinformado de la aplicación.

Ver también

http://php.net/ChangeLog-5.php#5.5.27
http://backronym.fail/

Solución

Actualice a PHP versión 5.5.27 o posterior.

**Fig. 85.** Vulnerabilidades múltiples (BACKRONYM)
**Fuente:** Elaborado por Nessus

## **Solución**:

Esta es una de las vulnerabilidades considerada de explotación fácil ya que se lo puede hacer a través de la red, esta no necesita ninguna autenticación y no se determinó si existe un exploit. Para eliminar esta vulnerabilidad es necesario actualizar la versión de PHP que tiene parches ya específicos en puntos vulnerables.

58987 - Detección de versión PHP no compatible

Sinopsis

El host remoto contiene una versión no compatible de un lenguaje de script de aplicación web.

Descripción

Según su versión, la instalación de PHP en el host remoto ya no es compatible.

La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, es probable que contenga vulnerabilidades de seguridad.

Ver también

http://php.net/eol.php
https://wiki.php.net/rfc/releaseprocess

Solución

Actualice a una versión de PHP que sea actualmente compatible.

**Fig. 86.** PHP no compatible
**Fuente:** Elaborado por Nessus

77088 - OpenSSL 1.0.1 <1.0.1i Vulnerabilidades múltiples

**Sinopsis**

El servicio remoto se ve afectado por múltiples vulnerabilidades.

**Descripción**

Según su banner, el servidor web remoto utiliza una versión de OpenSSL 1.0.1 anterior a 1.0.1i. La biblioteca OpenSSL, por lo tanto, se ve afectada por las siguientes vulnerabilidades:

- Existe un error de memoria doble libre relacionado con el manejo de paquetes DTLS que permite ataques de denegación de servicio. (CVE-2014-3505)

: existe un error no especificado relacionado con el manejo de mensajes de protocolo de enlace DTLS que permite ataques de denegación de servicio debido al consumo de grandes cantidades de memoria. (CVE-2014-3506)

: existe un error de pérdida de memoria relacionado con el manejo de paquetes DTLS especialmente diseñados que permiten ataques de denegación de servicio. (CVE-2014-3507)

- Existe un error relacionado con 'OBJ_obj2txt' y la bonita impresión 'X509_name_*' que filtra datos de la pila, lo que resulta en una divulgación de información. (CVE-2014-3508)

: existe un error relacionado con el manejo de 'extensión de formato de punto ec' y los clientes multiproceso que permiten sobrescribir la memoria liberada durante una sesión reanudada. (CVE-2014-3509)

: existe un error de desreferencia de puntero NULL relacionado con el manejo de conjuntos de cifrado de ECDH anónimos y mensajes de saludo creados que permiten ataques de denegación de servicio contra clientes. (CVE-2014-3510)

- Existe un error relacionado con el manejo de mensajes fragmentados de 'ClientHello' que podrían permitir que un atacante man-in-the-middle fuerce el uso de TLS 1.0 independientemente de que el servidor y el cliente admitan niveles de protocolo más altos. (CVE-2014-3511)

: existe un error de desbordamiento del búfer relacionado con el manejo de los parámetros del Protocolo de contraseña remota segura (SRP) que tienen un impacto no especificado. (CVE-2014-3512)

: existe un error de desreferencia de puntero NULL relacionado con el manejo del Protocolo de contraseña remota segura (SRP) que permite que un servidor malintencionado bloquee a un cliente, lo que resulta en una denegación de servicio. (CVE-2014-5139)

**Ver también**

https://www.openssl.org/news/openssl-1.0.1-notes.html
https://www.openssl.org/news/secadv/20140806.txt
https://www.openssl.org/news/vulnerabilities.html

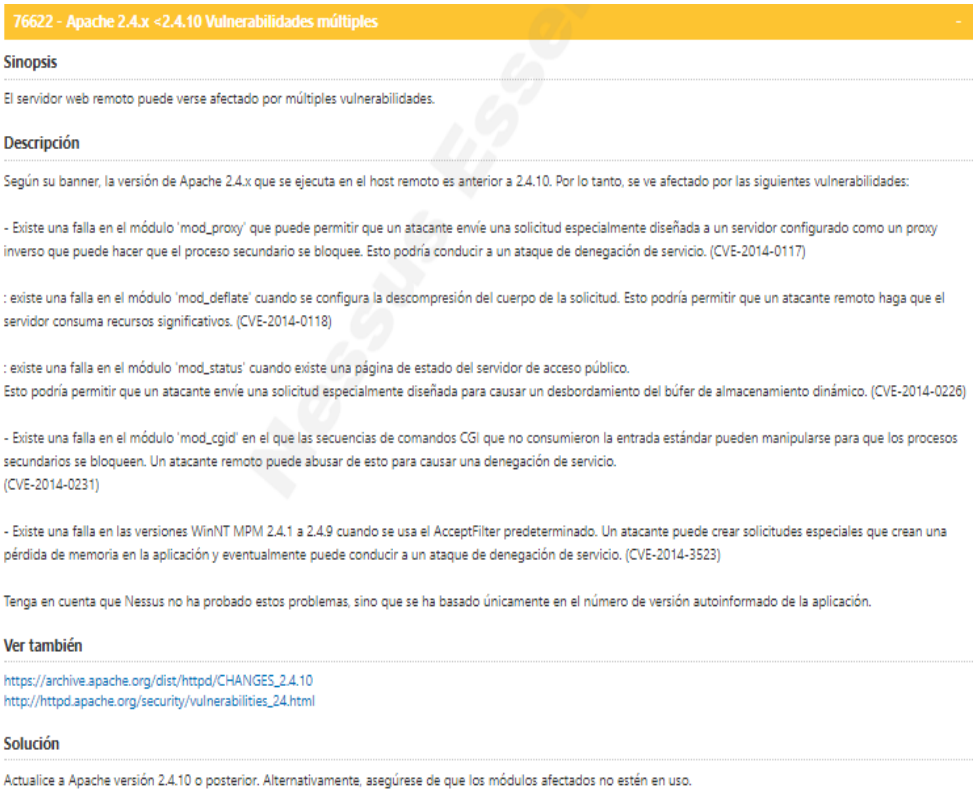
**Solución**

Actualice a OpenSSL 1.0.1i o posterior.

**Fig. 87.** Vulnerabilidades múltiples en memoria
**Fuente:** Elaborado por Nessus

## **Solución**:

Esta es una de las vulnerabilidad provoca que al enviar y manejar paquetes DTLS un atacante puede hacer que el sistema falle, consumir gran cantidad de memoria y denegación de servicios. No existe alguna protección específica pero lo que se podría hacer es OpenSSL a su versión actual pero tomando en cuenta que no afecte a la compatibilidad del sistema.



76622 - Apache 2.4.x <2.4.10 Vulnerabilidades múltiples

**Sinopsis**

El servidor web remoto puede verse afectado por múltiples vulnerabilidades.

**Descripción**

Según su banner, la versión de Apache 2.4.x que se ejecuta en el host remoto es anterior a 2.4.10. Por lo tanto, se ve afectado por las siguientes vulnerabilidades:

- Existe una falla en el módulo 'mod_proxy' que puede permitir que un atacante envíe una solicitud especialmente diseñada a un servidor configurado como un proxy inverso que puede hacer que el proceso secundario se bloquee. Esto podría conducir a un ataque de denegación de servicio. (CVE-2014-0117)

: existe una falla en el módulo 'mod_deflate' cuando se configura la descompresión del cuerpo de la solicitud. Esto podría permitir que un atacante remoto haga que el servidor consuma recursos significativos. (CVE-2014-0118)

: existe una falla en el módulo 'mod_status' cuando existe una página de estado del servidor de acceso público.
Esto podría permitir que un atacante envíe una solicitud especialmente diseñada para causar un desbordamiento del búfer de almacenamiento dinámico. (CVE-2014-0226)

- Existe una falla en el módulo 'mod_cgid' en el que las secuencias de comandos CGI que no consumieron la entrada estándar pueden manipularse para que los procesos secundarios se bloqueen. Un atacante remoto puede abusar de esto para causar una denegación de servicio.
(CVE-2014-0231)

- Existe una falla en las versiones WinNT MPM 2.4.1 a 2.4.9 cuando se usa el AcceptFilter predeterminado. Un atacante puede crear solicitudes especiales que crean una pérdida de memoria en la aplicación y eventualmente puede conducir a un ataque de denegación de servicio. (CVE-2014-3523)

Tenga en cuenta que Nessus no ha probado estos problemas, sino que se ha basado únicamente en el número de versión autoinformado de la aplicación.

**Ver también**

https://archive.apache.org/dist/httpd/CHANGES_2.4.10
http://httpd.apache.org/security/vulnerabilities_24.html

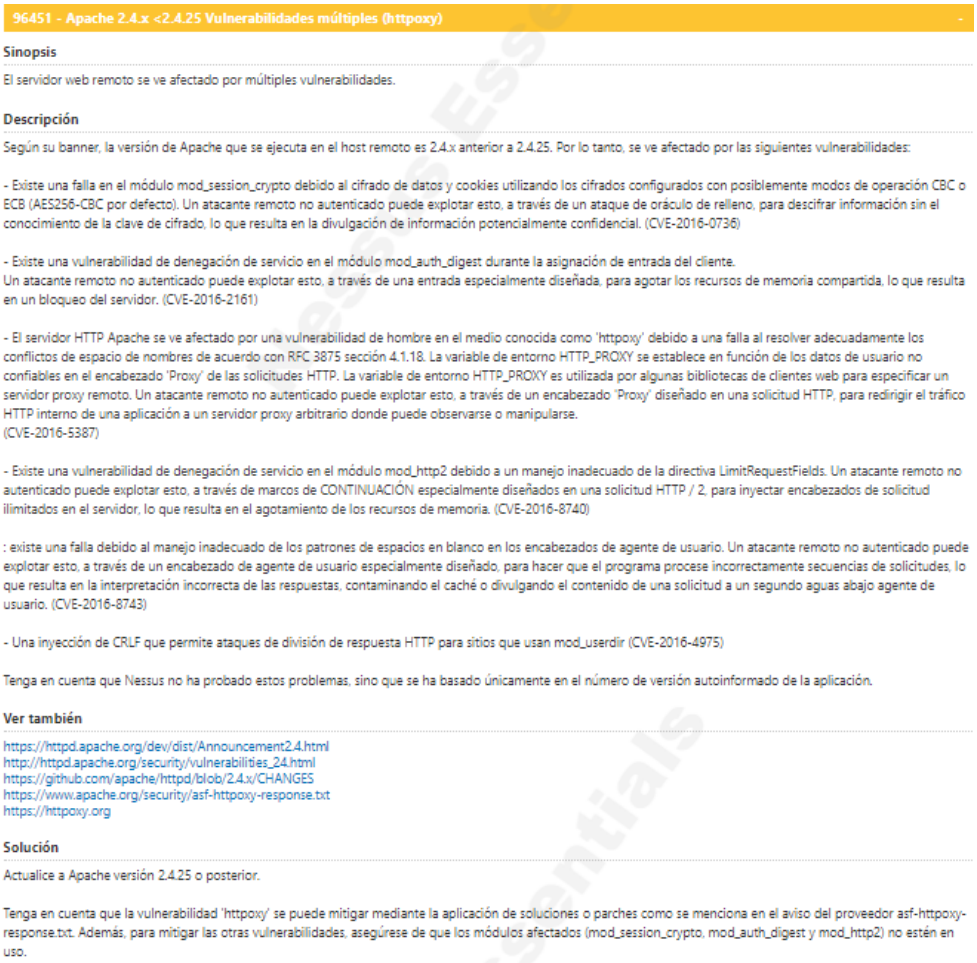
**Solución**

Actualice a Apache versión 2.4.10 o posterior. Alternativamente, asegúrese de que los módulos afectados no estén en uso.

**Fig. 88.** Vulnerabilidades múltiples en módulos
**Fuente:** Elaborado por Nessus

## **Solución**:

Actualizar la versión de OpenSSL a una que sea compatible tomando en cuenta los enlaces de las páginas del fabricante. Tomando en cuenta que los módulos que se vieron infectados estén deshabilitados.



**96451 - Apache 2.4.x <2.4.25 Vulnerabilidades múltiples (httpoxy)**

**Sinopsis**

El servidor web remoto se ve afectado por múltiples vulnerabilidades.

**Descripción**

Según su banner, la versión de Apache que se ejecuta en el host remoto es 2.4.x anterior a 2.4.25. Por lo tanto, se ve afectado por las siguientes vulnerabilidades:

- Existe una falla en el módulo mod_session_crypto debido al cifrado de datos y cookies utilizando los cifrados configurados con posiblemente modos de operación CBC o ECB (AES256-CBC por defecto). Un atacante remoto no autenticado puede explotar esto, a través de un ataque de oráculo de relleno, para descifrar información sin el conocimiento de la clave de cifrado, lo que resulta en la divulgación de información potencialmente confidencial. (CVE-2016-0736)

- Existe una vulnerabilidad de denegación de servicio en el módulo mod_auth_digest durante la asignación de entrada del cliente.
Un atacante remoto no autenticado puede explotar esto, a través de una entrada especialmente diseñada, para agotar los recursos de memoria compartida, lo que resulta en un bloqueo del servidor. (CVE-2016-2161)

- El servidor HTTP Apache se ve afectado por una vulnerabilidad de hombre en el medio conocida como 'httpoxy' debido a una falla al resolver adecuadamente los conflictos de espacio de nombres de acuerdo con RFC 3875 sección 4.1.18. La variable de entorno HTTP_PROXY se establece en función de los datos de usuario no confiables en el encabezado 'Proxy' de las solicitudes HTTP. La variable de entorno HTTP_PROXY es utilizada por algunas bibliotecas de clientes web para especificar un servidor proxy remoto. Un atacante remoto no autenticado puede explotar esto, a través de un encabezado 'Proxy' diseñado en una solicitud HTTP, para redirigir el tráfico HTTP interno de una aplicación a un servidor proxy arbitrario donde puede observarse o manipularse.
(CVE-2016-5387)

- Existe una vulnerabilidad de denegación de servicio en el módulo mod_http2 debido a un manejo inadecuado de la directiva LimitRequestFields. Un atacante remoto no autenticado puede explotar esto, a través de marcos de CONTINUACIÓN especialmente diseñados en una solicitud HTTP / 2, para inyectar encabezados de solicitud ilimitados en el servidor, lo que resulta en el agotamiento de los recursos de memoria. (CVE-2016-8740)

: existe una falla debido al manejo inadecuado de los patrones de espacios en blanco en los encabezados de agente de usuario. Un atacante remoto no autenticado puede explotar esto, a través de un encabezado de agente de usuario especialmente diseñado, para hacer que el programa procese incorrectamente secuencias de solicitudes, lo que resulta en la interpretación incorrecta de las respuestas, contaminando el caché o divulgando el contenido de una solicitud a un segundo aguas abajo agente de usuario. (CVE-2016-8743)

- Una inyección de CRLF que permite ataques de división de respuesta HTTP para sitios que usan mod_userdir (CVE-2016-4975)

Tenga en cuenta que Nessus no ha probado estos problemas, sino que se ha basado únicamente en el número de versión autoinformado de la aplicación.

**Ver también**

https://httpd.apache.org/dev/dist/Announcement2.4.html
http://httpd.apache.org/security/vulnerabilities_24.html
https://github.com/apache/httpd/blob/2.4.x/CHANGES
https://www.apache.org/security/asf-httpoxy-response.txt
https://httpoxy.org

**Solución**

Actualice a Apache versión 2.4.25 o posterior.

Tenga en cuenta que la vulnerabilidad 'httpoxy' se puede mitigar mediante la aplicación de soluciones o parches como se menciona en el aviso del proveedor asf-httpoxy-response.txt. Además, para mitigar las otras vulnerabilidades, asegúrese de que los módulos afectados (mod_session_crypto, mod_auth_digest y mod_http2) no estén en uso.

**Fig. 89.** Vulnerabilidades múltiples (httpoxy)
**Fuente:** Elaborado por Nessus

## **Solución**:

Actualizar la versión de HTTPOXY a una versión de soluciones con parches hay que asegurarse que os módulos vulnerados mod_session_crypto y mod_auth_digest se encuentren desactivados.

**11213 - Métodos HTTP TRACE / TRACK permitidos**

**Sinopsis**

Las funciones de depuración están habilitadas en el servidor web remoto.

**Descripción**

El servidor web remoto admite los métodos TRACE y / o TRACK. TRACE y TRACK son métodos HTTP que se utilizan para depurar las conexiones del servidor web.

**Ver también**

https://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf
http://www.apacheweek.com/issues/03-01-24
https://download.oracle.com/sunalerts/1000718.1.html

**Solución**

Deshabilita estos métodos. Consulte la salida del complemento para obtener más información.

**Fig. 90.** Métodos HTTP TRACE/TRACK
**Fuente:** Elaborado por Nessus

### 3.1.4.5.3. Búsqueda de vulnerabilidades con OPENVAS (Ataque interno)


**Fig. 91.** Resultado de los Ataques Internos con Openvas
**Fuente:** Elaborado por Nessus

Los resultados obtenidos en el escaneo de vulnerabilidades con Openvas a los servidores fueron los siguientes:

Vemos de manera general en los gráficos donde se especifican la gravedad de las vulnerabilidades para su análisis posterior.

**Fig. 92.** Grafica especifica de ataques internos
**Fuente:** Elaborado por Nessus

Observamos en los gráficos de manera detallada el número de vulnerabilidades obtenidas en el ataque a los servidores de esta manera tenemos muy claro donde es más vulnerable el servidor y así poder realizar la respectiva protección.

## SERVIDORES

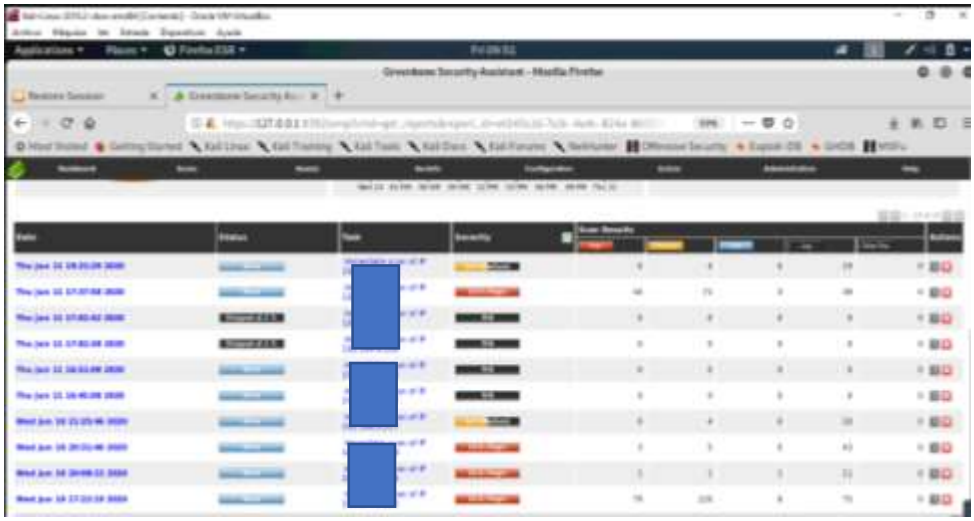


**Fig. 93.** Resultado individual de ataques a los servidores
**Fuente:** Elaborado por Nessus

## SERVIDOR ACTIVE DIRECTORY

**Fig. 94.** Detección de fin de vida de PHP
**Fuente:** Realizado por Openvas

**Solución**:

Debido a que PHP es compatible con cada versión solo por 2 años si no se actualice puede tener vulnerabilidades normalmente la vida útil se determina por los 3 años de soporte que dan al final ese periodo se termina la vida útil y se debe actualizar a una versión compatible.

**Fig. 95.** Detección de fin de vida de OpenSSL
**Fuente:** Realizado por Openvas

**Solución**:

Comprobar si existe una versión vulnerable en el servidor dado que un atacante puede aprovechar estas falencias de seguridad para infiltrarse comprometiendo la seguridad, por lo que es necesario actualizar la versión de openssl a una actual y compatible.

**Fig. 96.** Vulnerabilidades en OpenSSL
**Fuente:** Realizado por Openvas

**Solución**:

Comprobar si existe una versión vulnerable en el servidor dado que un atacante puede aprovechar estas falencias de seguridad para infiltrarse comprometiendo la seguridad, por lo que es necesario actualizar la versión de Openssl a una actual y compatible.

**Fig. 97.** PHP denegación de servicios
**Fuente:** Realizado por Openvas

**Solución**:

Una de las vulnerabilidades en PHP es la denegación de servicios el cual genera fallas en php_handle_iff() y php_handle_jpeg() de algunas funciones la cual consume los recursos de la maquina y consigue la denegación de servicios, para evitar eso se puede actualizar la versión de PHP a la 5.6.7 o superior.

**Fig. 98.** PHP denegación de servicios al correr OpenSSL
**Fuente:** Realizado por Openvas

**Solución**:

Una vulnerabilidad es la que emplea el mecanismo de cacheo interno de OpenSSL y si no se tiene configurado el protocolo TSL como una librería criptográfica general expuesta a que puedan realizar denegaciones de servicio al llenar nuestra memoria, para evitar se debe actualizar las versiones de OpenSSL de 0.9.8(f,o,p) a 1.0.0(a,b) según su versión.

**Fig. 99.** Vulnerabilidad de extensión de memoria no enlazada
**Fuente:** Realizado por Openvas

**Solución**:

Una vulnerabilidad de memoria es similar a la denegación de servicios solo que esta se enfoca en llenar la memoria con levantamiento de los servicios, la solución es actualizar la versión de OpenSSl.

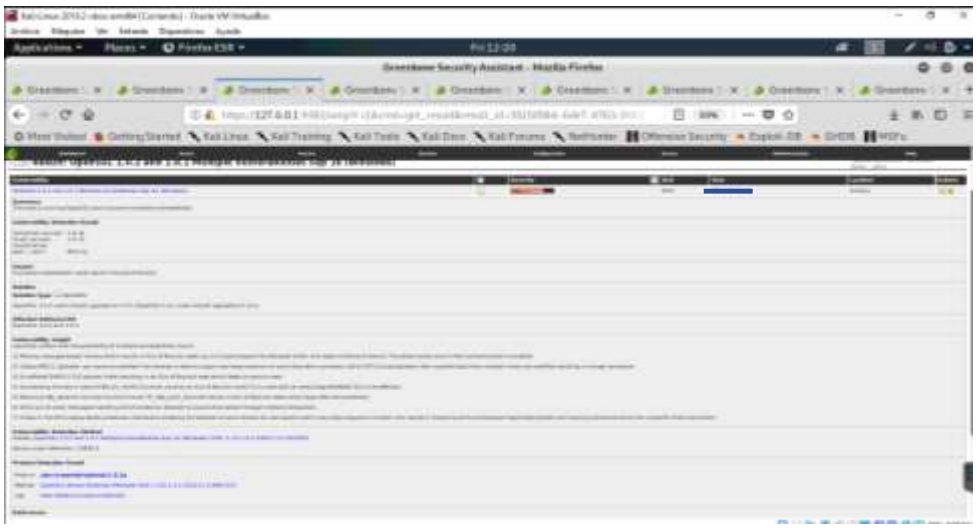


**Fig. 100.** Vulnerabilidades multiples OpenSSL
**Fuente:** Realizado por Openvas

**Solución**:

Una vulnerabilidad es la que emplea el mecanismo de cacheo interno de OpenSSL y si no se tiene configurado el protocolo TSL como una librería criptográfica general expuesta a que puedan realizar ataques por lo que para evitar esto es necesario actualizar la versión de OpenSSL y deshabilitar las anteriores.

**Fig. 101.** Vulnerabilidades ejecución de código arbitrario
**Fuente:** Realizado por Openvas

**Solución**:

Cuando existen vulnerabilidades de código arbitrario de php es necesario actualizar a la versión 7.3.10 la cual evita estos ataques, tomar en cuenta las actualizaciones del sistema operativo y las aplicaciones que se ejecutan en el mismo, llevar un control de donde se valide y confirme los cambios.

**Fig. 102.** Vulnerabilidades de PHP en recorrido de directorio
**Fuente:** Realizado por Openvas

**Solución**:

Cuando existen vulnerabilidades de código arbitrario de PHP es necesario actualizar a la versión 7.3.10 la cual evita estos ataques, tomar en cuenta las actualizaciones del sistema operativo y las aplicaciones que se ejecutan en el mismo, llevar un control de donde se valide y confirme los cambios.

**Fig. 103.** Vulnerabilidad denegación de servicio “libgd”
**Fuente:** Realizado por Openvas

**Solución**:

Cuando se encuentre una vulnerabilidad LIBGD que es en la librería grafica se la realiza por medio de input lo que provocaría una denegación de servicios, se la realiza por la red sin ninguna autenticación. Por lo que la solución seria actualizar PHP a su versión 7 o superior.

**Fig. 104.** Vulnerabilidad Apache http server
**Fuente:** Realizado por Openvas

**Solución**:

Cuando se produce la vulnerabilidad de Apache http server es porque se ejecuta código en procesos que corren en segundo plano, de esta manera pueden determinar las credenciales de usuarios y usar en otra autenticación. Actualizar la versión de PHP 2.4.38 o 2.4.39 respectivamente.

**Fig. 105.** Vulnerabilidad no especificada y PHP denegación de servicio
**Fuente:** Realizado por Openvas

**Solución**:

Cuando se produce las vulnerabilidades no especificadas lo que puede realizar es una actualización de PHP tomando en cuenta la compatibilidad de los servicios y aplicaciones instalados.

SERVIDOR FACTURACION

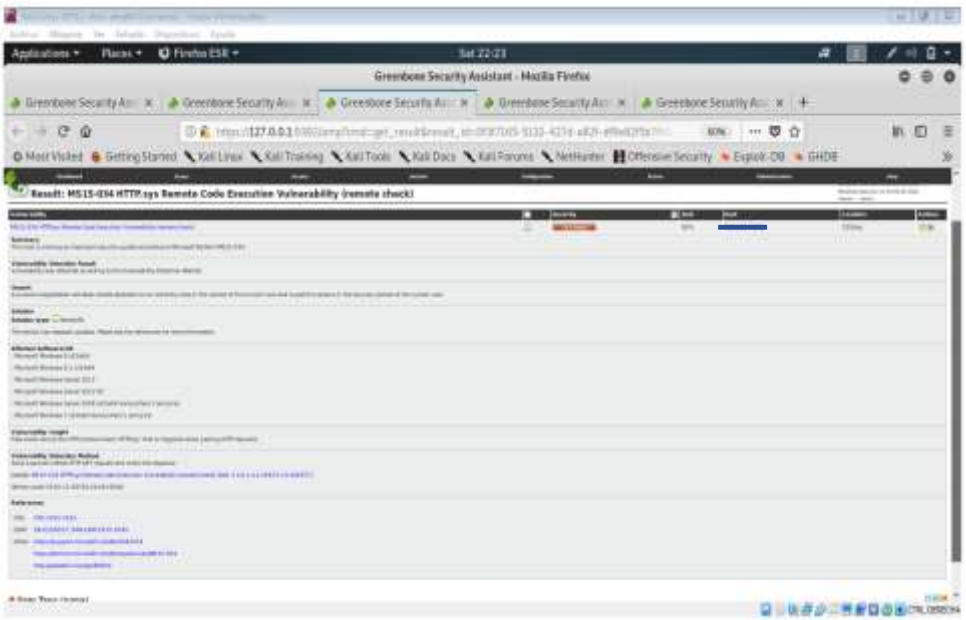


**Fig. 106.** Vulnerabilidad de ejecución de código remoto
**Fuente:** Realizado por Openvas

**Solución**:

Cuando se produce las vulnerabilidades no especificadas lo que puede realizar es una actualización teniendo más información de los problemas encontrados.

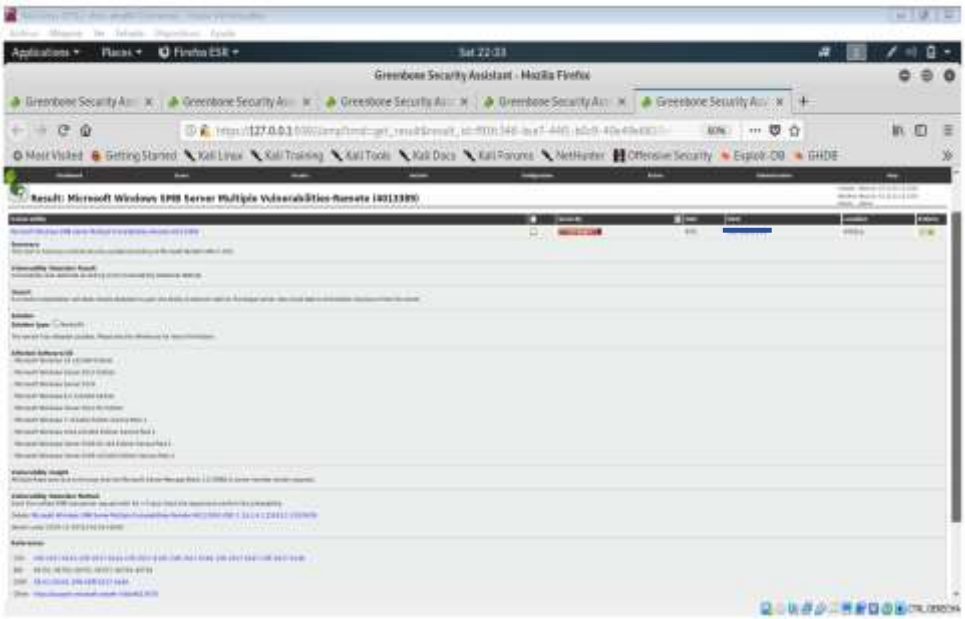


**Fig. 107.** Vulnerabilidad server SMB
**Fuente:** Realizado por Openvas

**Solución**:

Cuando se presenta esta vulnerabilidad se debe tener en claro si hay que proteger servidores o clientes SMB, en un servidor desde Powershell se ejecutara un parche (“HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters”) pero en el cliente se debe bloquear el puerto 445 TCP en el firewall.

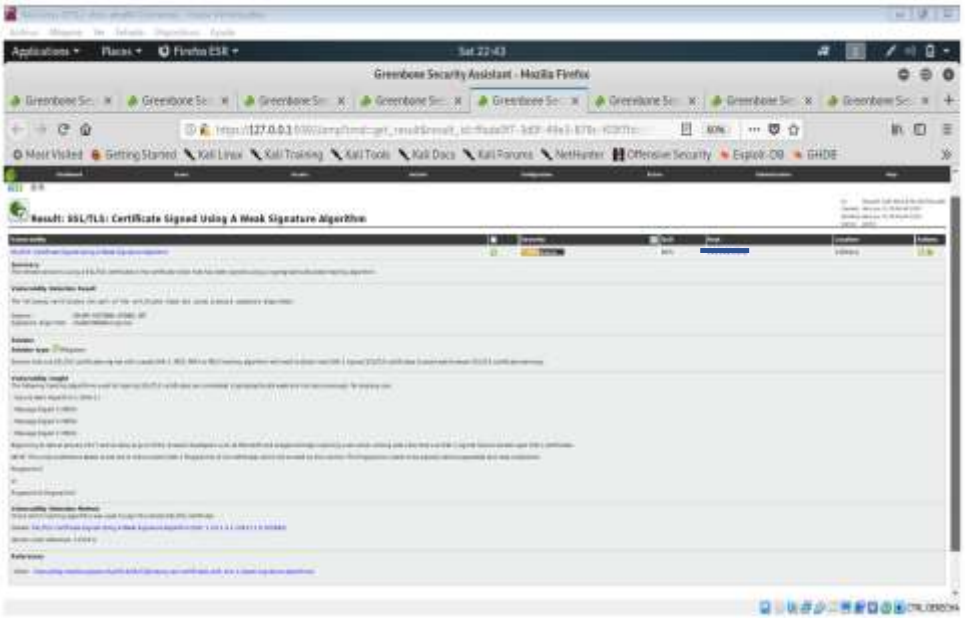


**Fig. 108.** Algoritmo de certificado de firma débil
**Fuente:** Realizado por Openvas

**Solución**:

Cuando encontramos algoritmos de firma débil lo que demos hacer es ver la cadena de certificado SSL que está usando un algoritmo hash de cifrado y actualizarlo por un certificado donde la CA use algoritmos seguros.

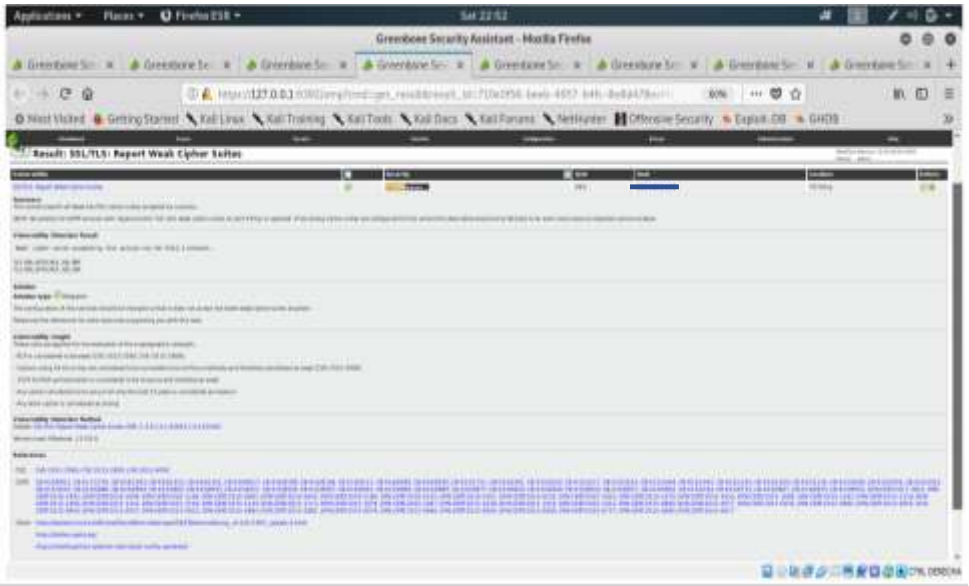



**Fig. 109.** Vulnerabilidad de cifrado débil
**Fuente:** Realizado por Openvas

**Solución**:

Cuando tenemos cifrado débil se debe realizar lo siguiente: en servidores desactivar las versiones de TLS inferiores a 1.2 y las SSL lo que provocará que el servidor use mejores algoritmos de cifrados, en el caso del cliente mantener actualizado los navegadores.

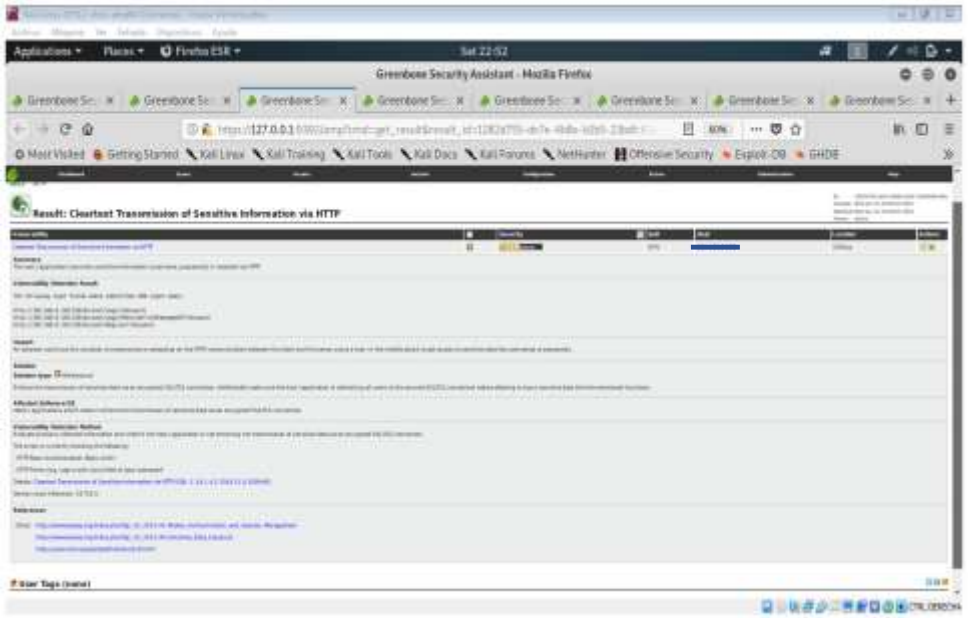



**Fig. 110.** Transmisión de información delicada vía HTTP
**Fuente:** Realizado por Openvas

**Solución**:

Cuando existen vulnerabilidades de este tipo se debe crear un archivo de configuración de seguridad de red en XML, se puede personalizar la CA de confianza autoafirmada o emitirlo a nivel interno.

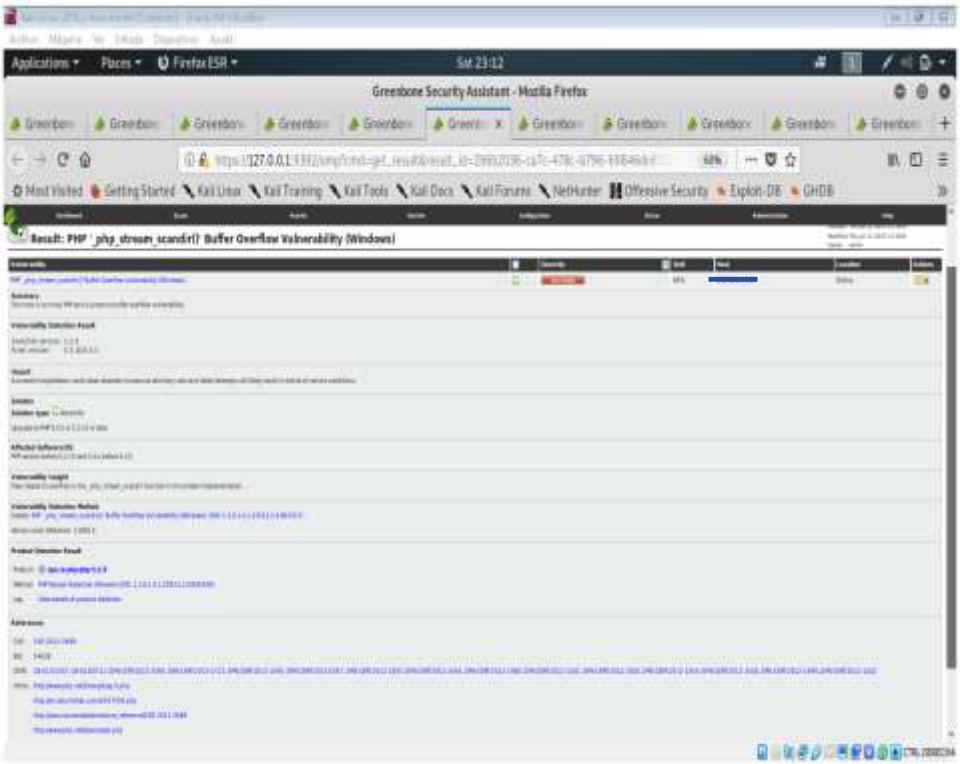



**Fig. 111.** Vulnerabilidad desbordamiento de buffer
**Fuente:** Realizado por Openvas

**Solución**:

Cuando existen vulnerabilidad de desbordamiento de buffer esta puede producir que sea posible introducir código arbitrario y escalada de privilegios lo que puede ocasionar denegación de servicios. Para prevenir se puede realizar una redirección de espacios aleatorios ya que para realizar un ataque se debe conocer las direcciones exactas, también realizar una prevención de ejecución de datos.

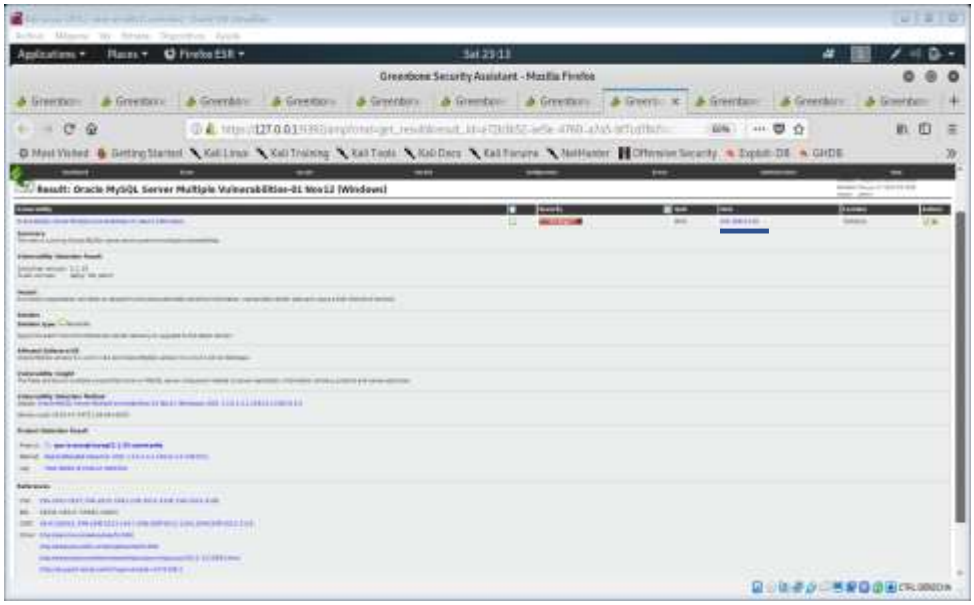


**Fig. 112.** Vulnerabilidad en Mysql server
**Fuente:** Realizado por Openvas

**Solución**:

Cuando existen vulnerabilidades en MySQL lo más recomendado es actualizar a la última versión y aplicar los parches de seguridad.

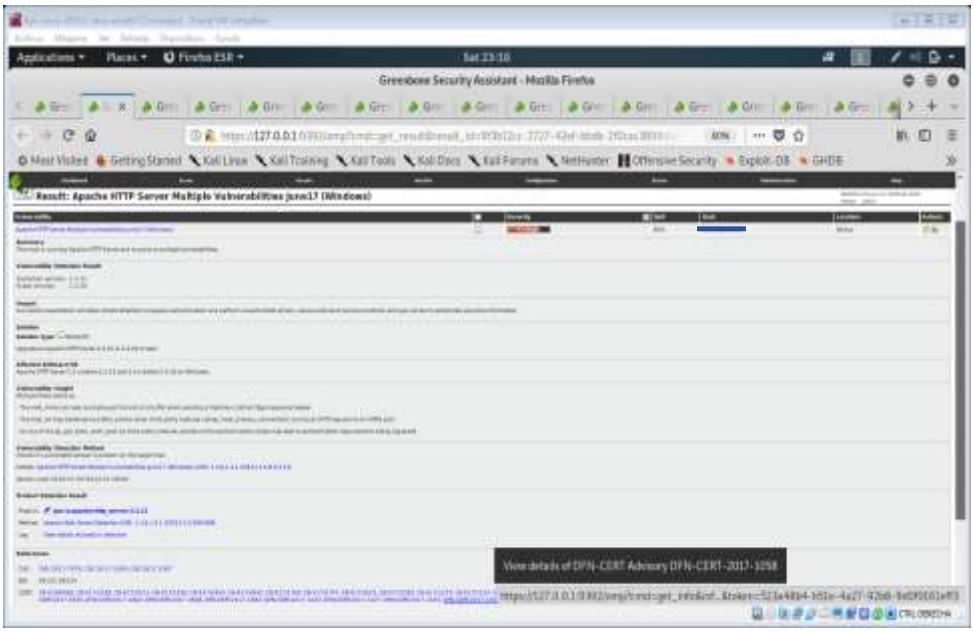


**Fig. 113.** Vulnerabilidad Apache HTTP server
**Fuente:** Realizado por Openvas

**Solución**:

Cuando tenemos estas vulnerabilidades son consideradas de alto impacto ya que puede permitir a un atacante ejecutar código arbitrario. Para evitar se debe actualizar Apache HTTP server 2.2.33 o 2.4.26 según su necesidad.

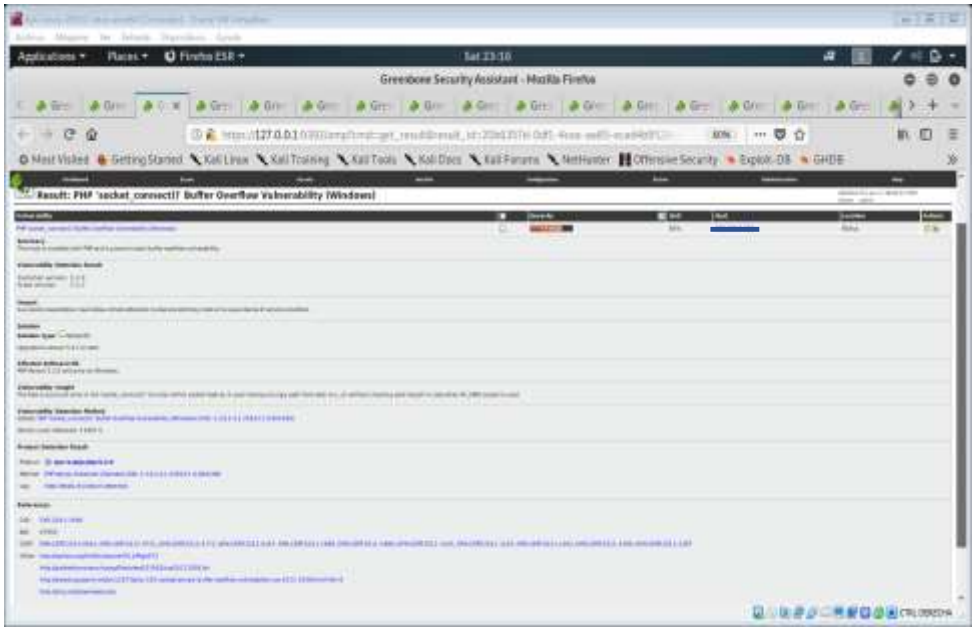


**Fig. 114.** Vulnerabilidad desbordamiento de buffer
**Fuente:** Realizado por Openvas

**Solución**:

Se debe actualizar la versión de PHP 5.3.5

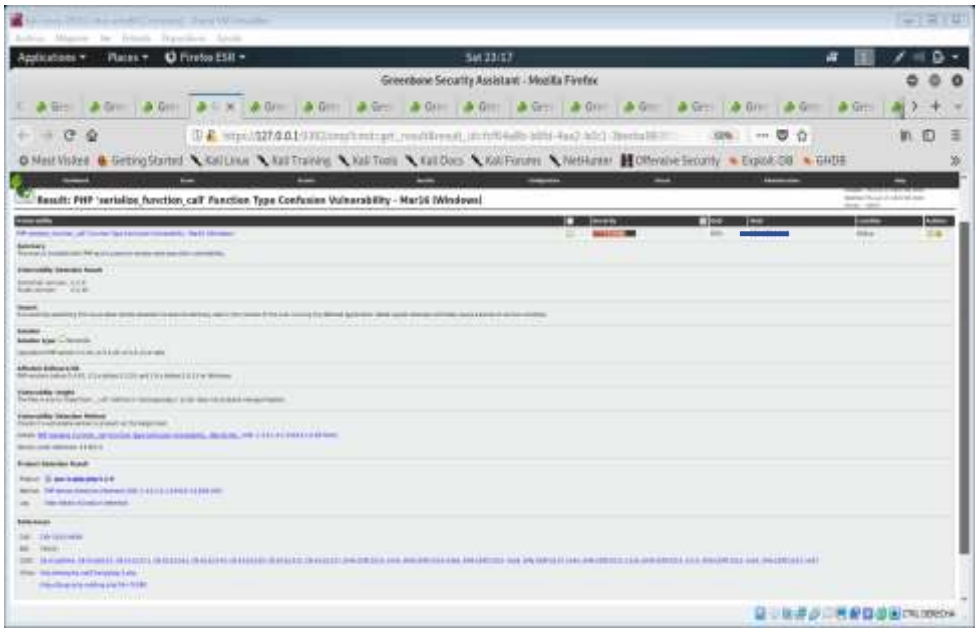


**Fig. 115.** Vulnerabilidad en tipo de función
**Fuente:** Realizado por Openvas

**Solución**:

Para esta vulnerabilidad se debe tener en claro cómo funciona PHP unserialize(), ya que si se logra infiltrar se puede realizar ataques maliciosos, para lo que no es recomendable usar dichas funciones y en su lugar usar funciones JSON.

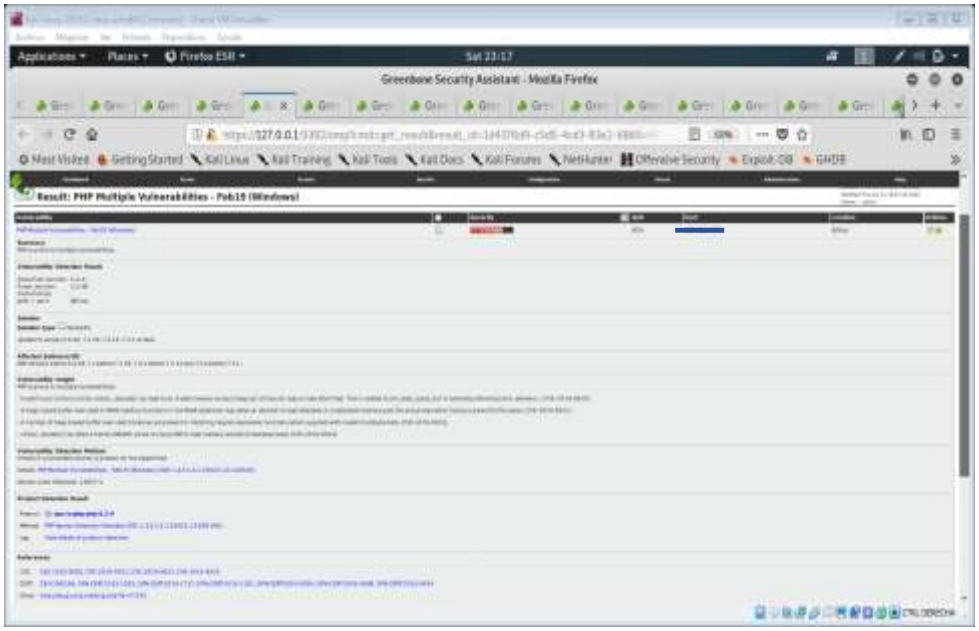


**Fig. 116.** Vulnerabilidades múltiples en PHP
**Fuente:** Realizado por Openvas

**Solución**:

Se debe actualizar la versión de PHP 5.6.40 o a una superior pero que sea compatible.

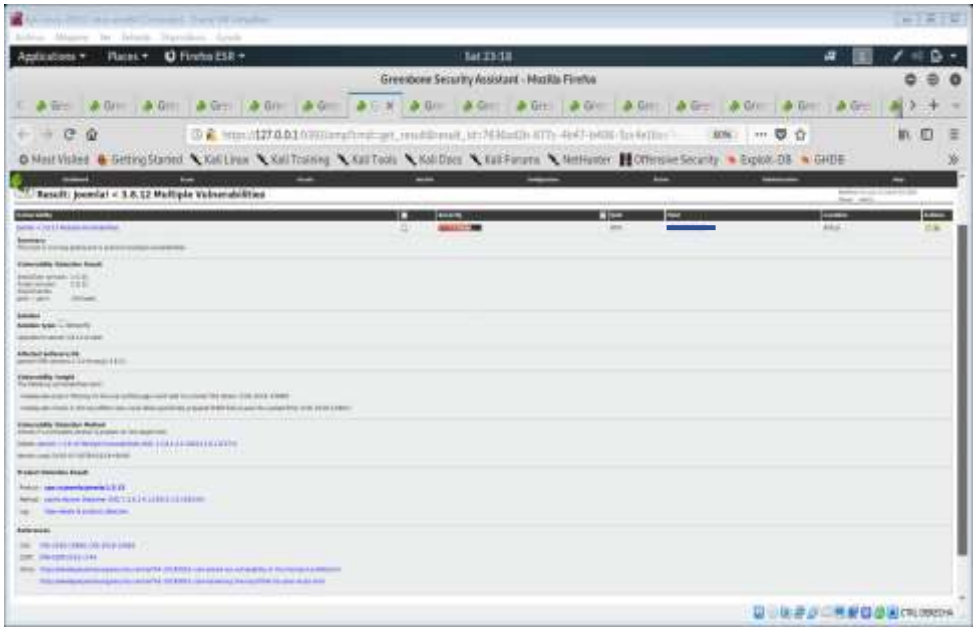


**Fig. 117.** Vulnerabilidades en Joomla
**Fuente:** Realizado por Openvas

**Solución**:

Cambiar de versión actualizándola de la 3.8.11 a la versión 3.8.12

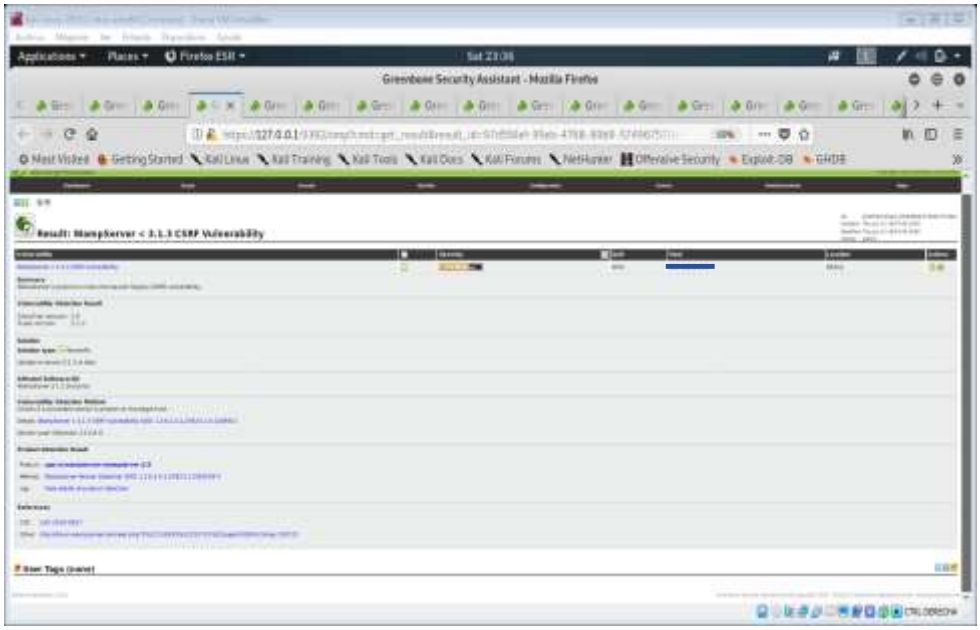



**Fig. 118.** Vulnerabilidad WampServer
**Fuente:** Realizado por Openvas

**Solución**:

Esta vulnerabilidad contiene un xss en index.php en su versión 3.1.4 este ataque no necesita autenticación y ataca a la integridad del sistema, por lo que se debe actualizar la versión de php 3.1.5 y solucionar las seguridades xss en index.php.

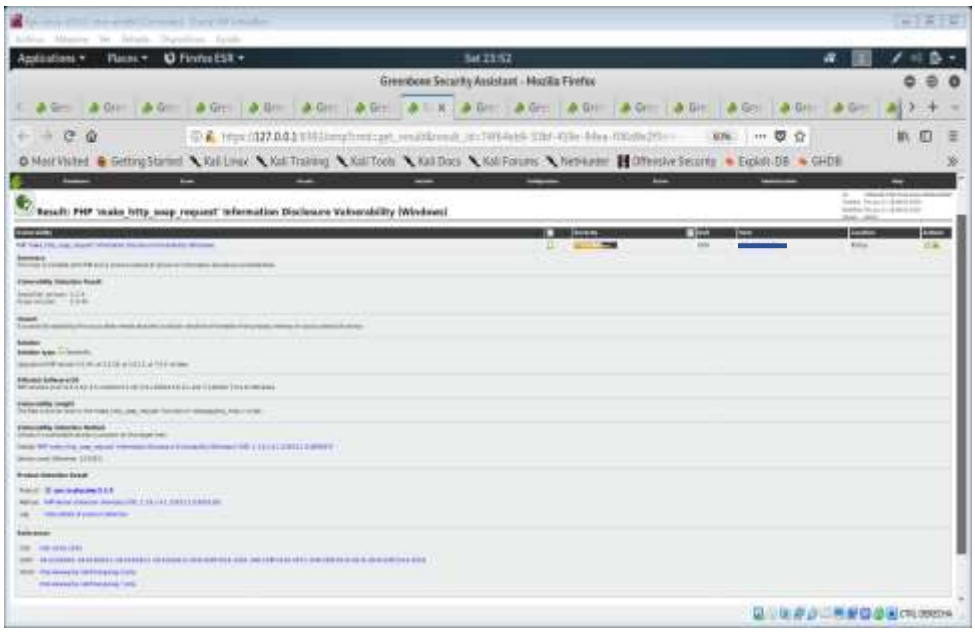



**Fig. 119.** Vulnerabilidad en divulgar información
**Fuente:** Realizado por Openvas

**Solución**:

Actualizar la versión de php según sea compatible con los servicios.

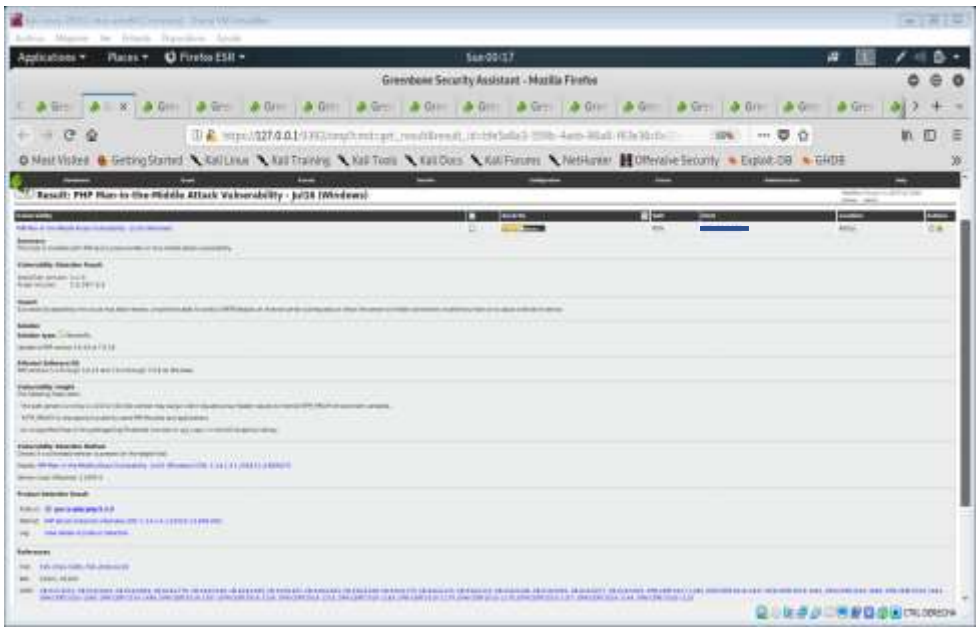



**Fig. 120.** Vulnerabilidad Ataque de hombre en medio
**Fuente:** Realizado por Openvas

**Solución**:

Siempre se debe proteger los datos con certificados SSL autorizados, realizar inicios de sesión de forma segura con autenticación en 2 pasos.

## SERVIDOR DE FACTURACION

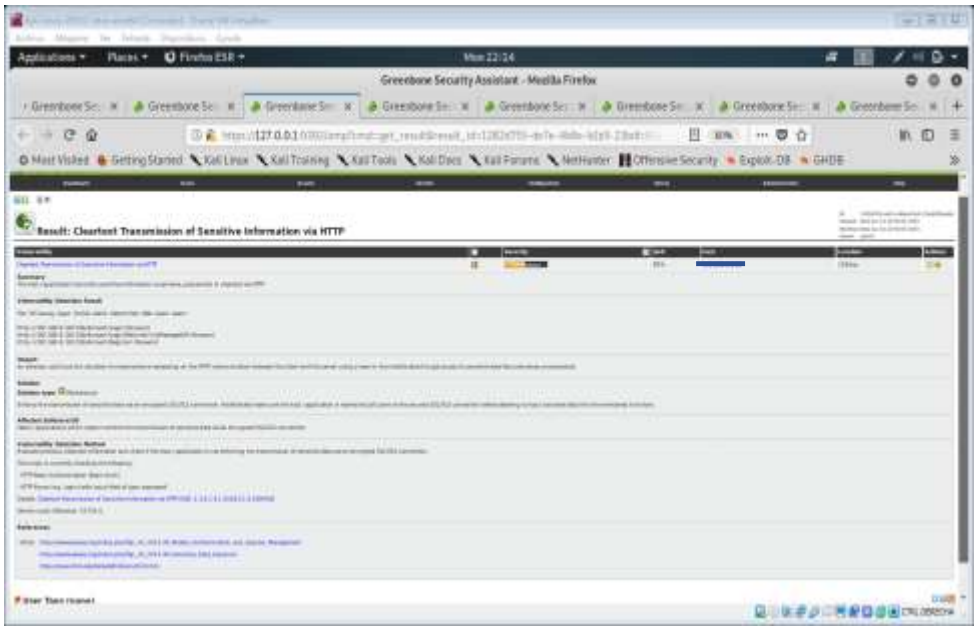



**Fig. 121.** Vulnerabilidad al borrar texto de información delicada vía PHP
**Fuente:** Realizado por Openvas

**Solución**:

Para proteger tus credencias se puede hacerlo usando Worpress o Drupal, pero lo mejor es hacerlo en el servidor web Apache y ahorrando recursos del sistema evitando ejecutar PHP lo que nos ayudara a evitar inyección sql.

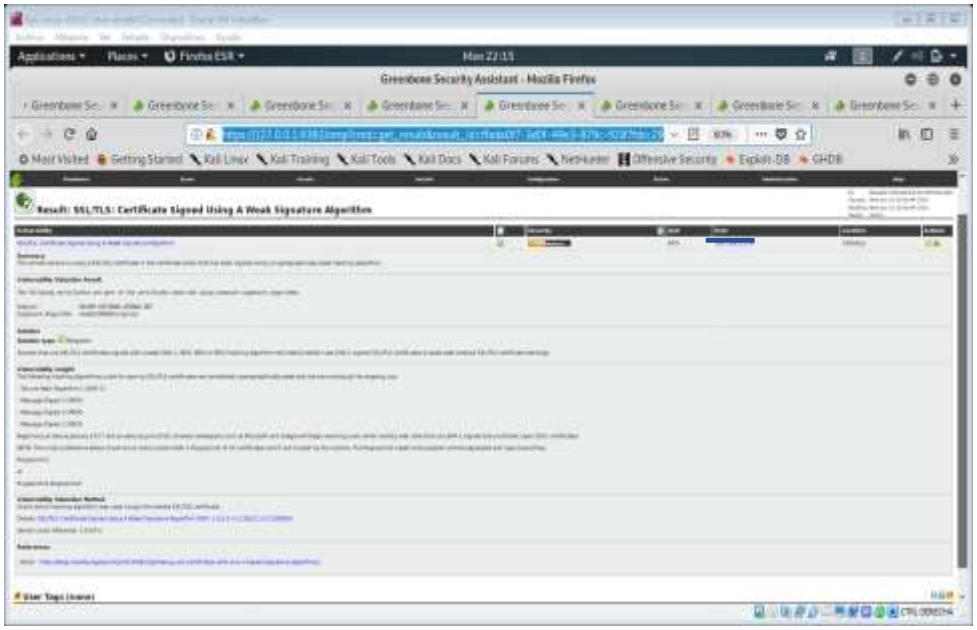



**Fig. 122.** Vulnerabilidad de firma débil con certificados SSL/TLS
**Fuente:** Realizado por Openvas

**Solución**:

Usar algoritmos de cifrado mejores se puedes usar sha-2 con certificados SSL o TLS.

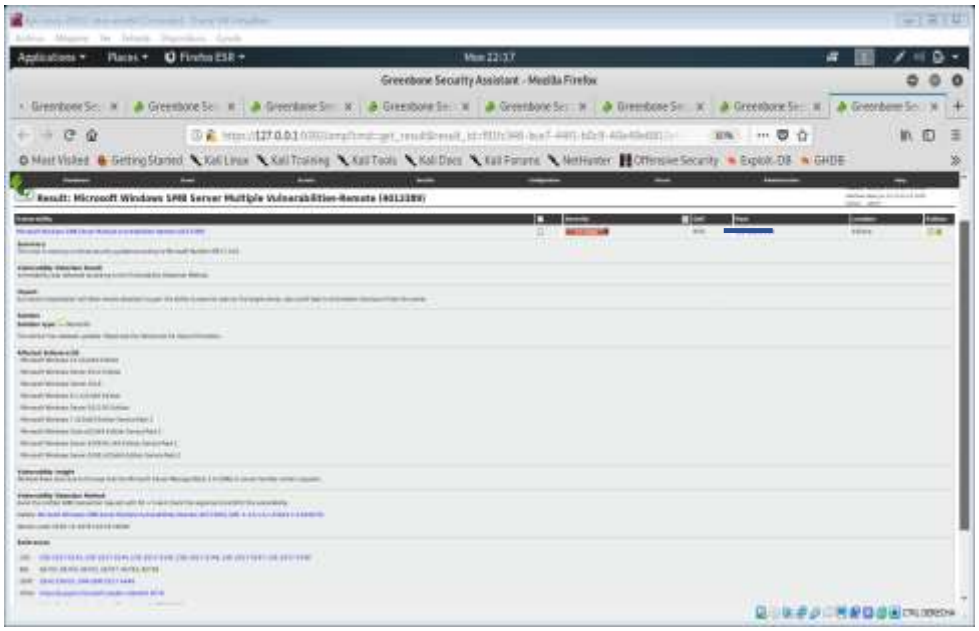



**Fig. 123.** Vulnerabilidad remota SMB
**Fuente:** Realizado por Openvas

**Solución**:

Para solucionar vulnerabilidades remotas es necesario modificar los registros haciendo un acopia previa, se debe especificar los nombres de los host para realizar la respectiva autenticación.

## SERVIDOR DE BASE DE DATOS

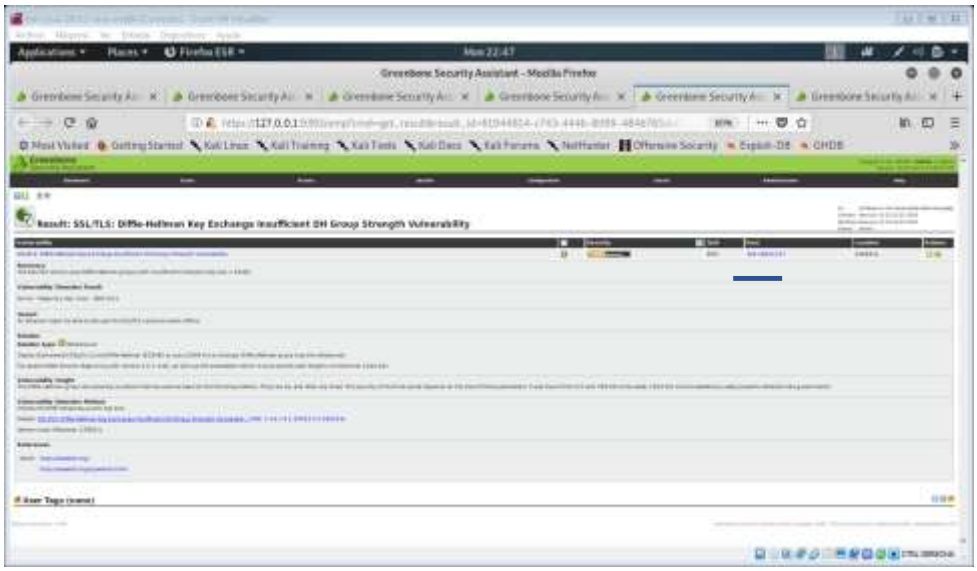


**Fig. 124.** Vulnerabilidad Diffie-Hellman
**Fuente:** Realizado por Openvas

**Solución**:

La vulnerabilidad escuchar comunicaciones cifradas esta es capaz de descifrar conexiones SSH y HTTPS, para evitar este ataque lo recomendable es desactivar la comunicación SSL o TLS.

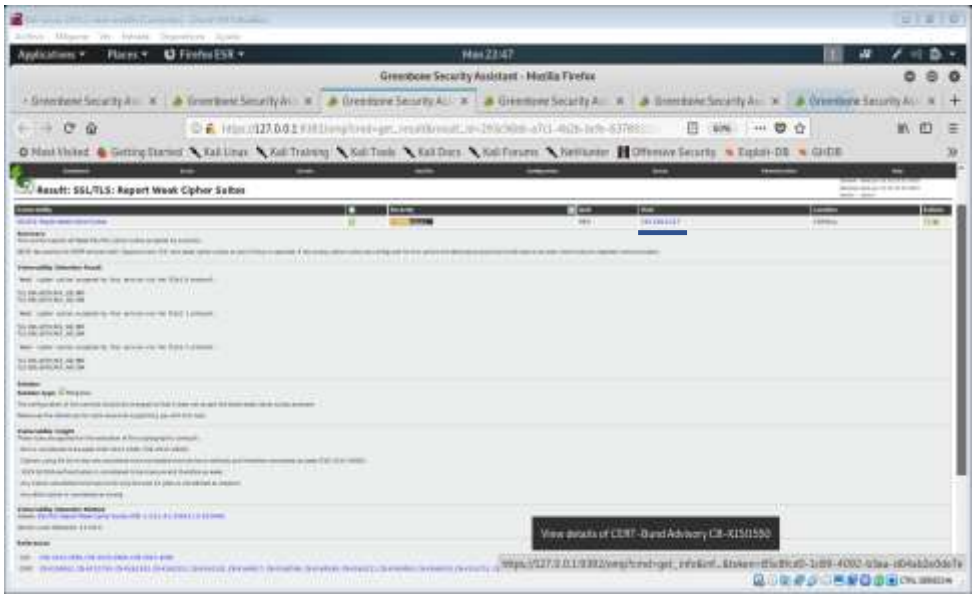


**Fig. 125.** Vulnerabilidad conjunto de cifrado débil
**Fuente:** Realizado por Openvas

**Solución**:

Determinar si el modo de cifrado CBC no está activo para dejar solo por RC4 usar la v1 de TLS o v1.2.

## SERVIDOR DE BIBLIOTECA

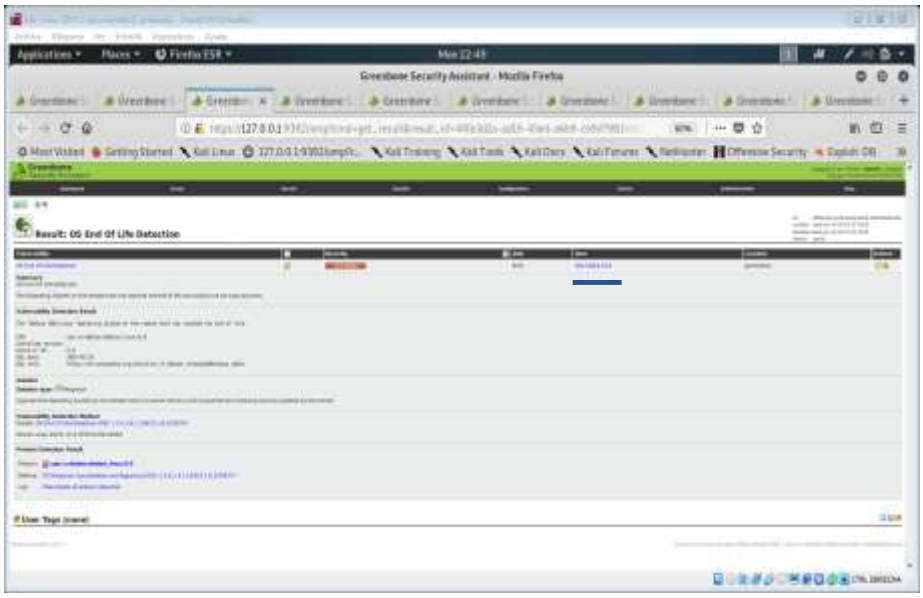



**Fig. 126.** OS detección fin de la vida
**Fuente:** Realizado por Openvas

**Solución**:

Actualizar el sistema operativo para una versión remota la cual sea compatible y soporte las actualizaciones de seguridad.

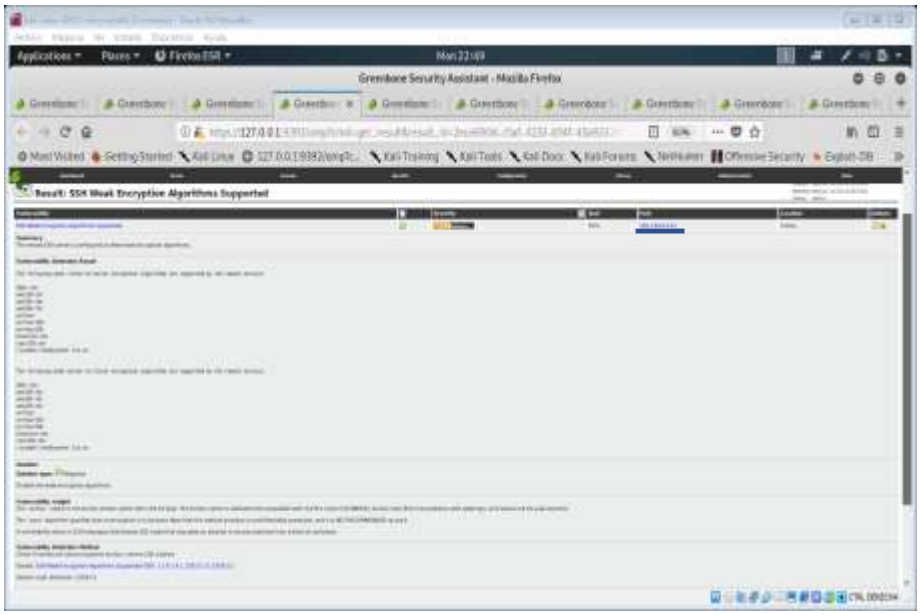



**Fig. 127.** Encriptación de algoritmo SSH débil
**Fuente:** Realizado por Openvas

**Solución**:

Un problema muy común es que el sistema remoto está configurado para usar cifrado de flujo Arcfour el cual es un algoritmo débil, se puede modificar SSH para que sea más estricto, pero se debe ver que los algoritmos ocupados sean compatibles.

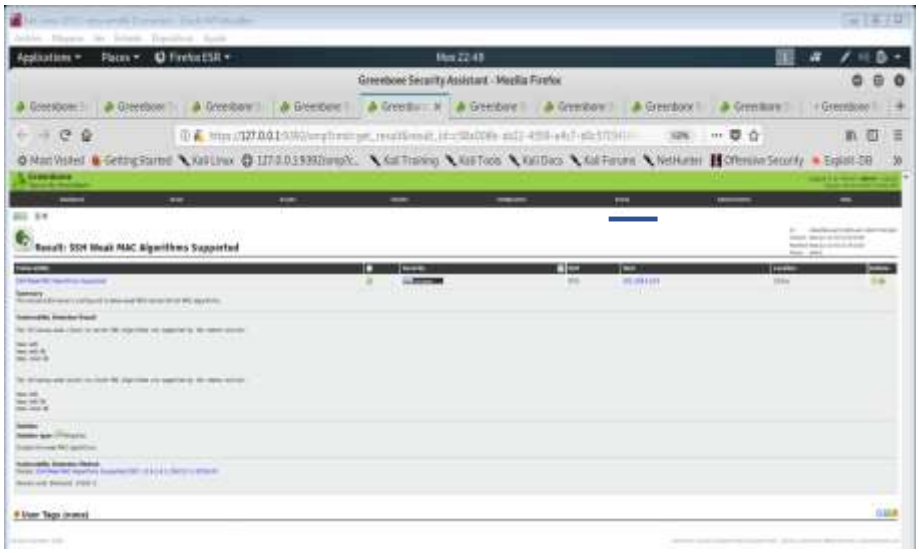


**Fig. 128.** Algoritmo en MAC SSH débil
**Fuente:** Realizado por Openvas

**Solución**:

Un problema muy grave es que por defecto vienen habilitados en la configuración algoritmos débiles SSH predeterminados, se puede habilitar el modo criptográfico heredado.

### 3.1.4.6. Testeo de aplicaciones de internet

#### 3.1.4.6.1. Autenticación


**Fig. 129.** Inicio de sesión página web Atenas
**Fuente:** Elaborado por el Investigador

La Unidad educativa Atenas cuenta con una página web informativa en la cual se realizó un ataque de fuerza bruta para poder ingresar, lo que se pudo observar fue que no permitió saltarse la autenticación ya que contaba el número de intentos fallidos y luego la página se redirigía al inicio. Lo que se noto es que no tenía control de accesos y tampoco determinaba el tiempo de uso o de una sesión activa.

#### 3.1.4.6.2. Manipulación de la Información de salida

- Recuperar información importante/comprometedora guardada en las cookies.

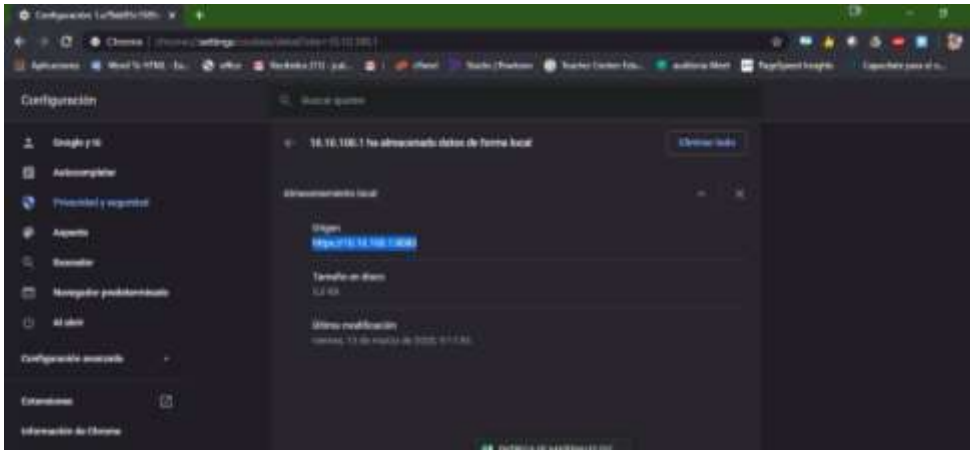



**Fig. 130.** Información en las cookies
**Fuente:** Elaborado por el Investigador

- Recuperar información importante/comprometedora en la caché de la aplicación cliente.

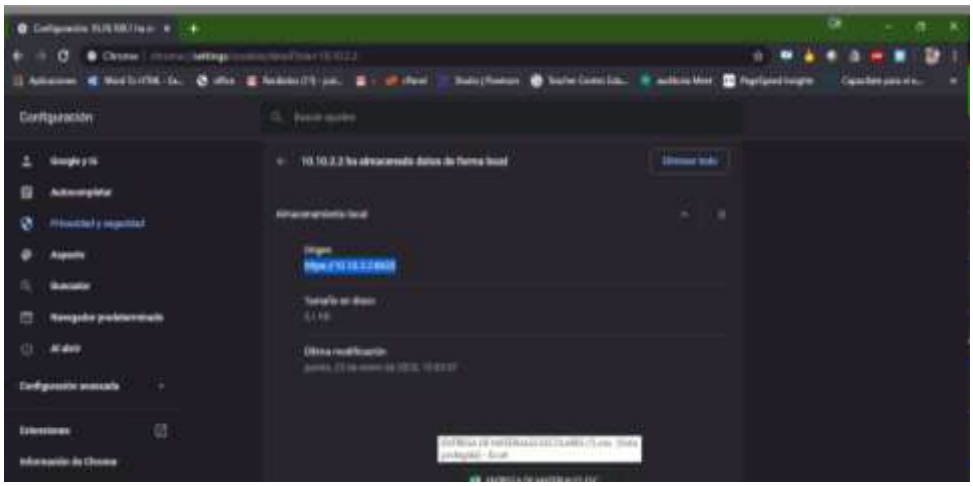



**Fig. 131.** Almacenamiento en las cookies
**Fuente:** Elaborado por el Investigador

- Recuperar información importante/comprometedora guardada en los objetos con número de serie.

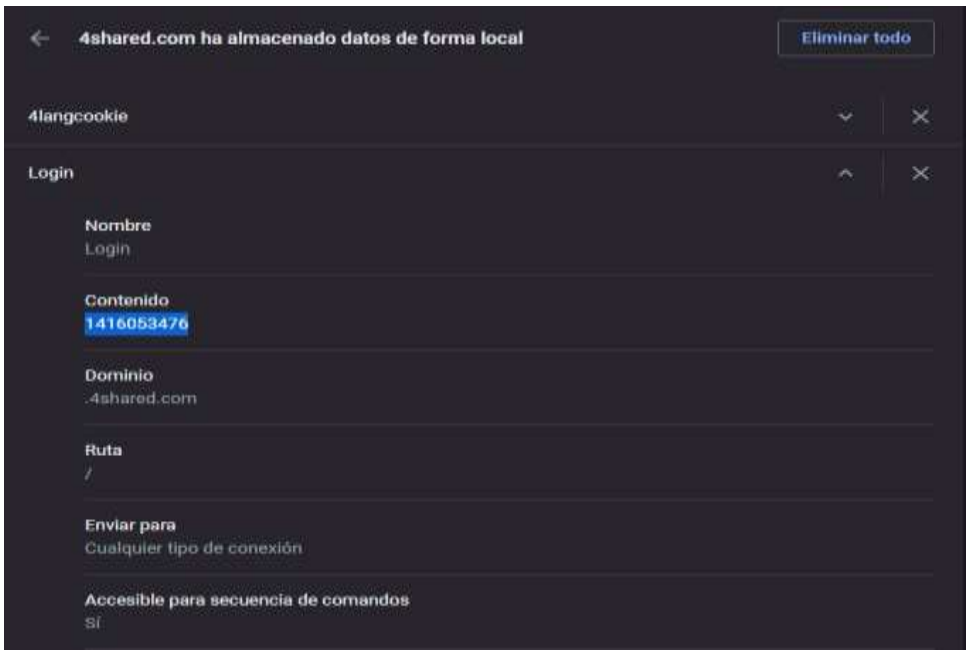



**Fig. 132.** Direcciones IP en las cookies
**Fuente:** Elaborado por el Investigador

- Recuperar información importante/comprometedora guardada en los archivos temporales y objetos.

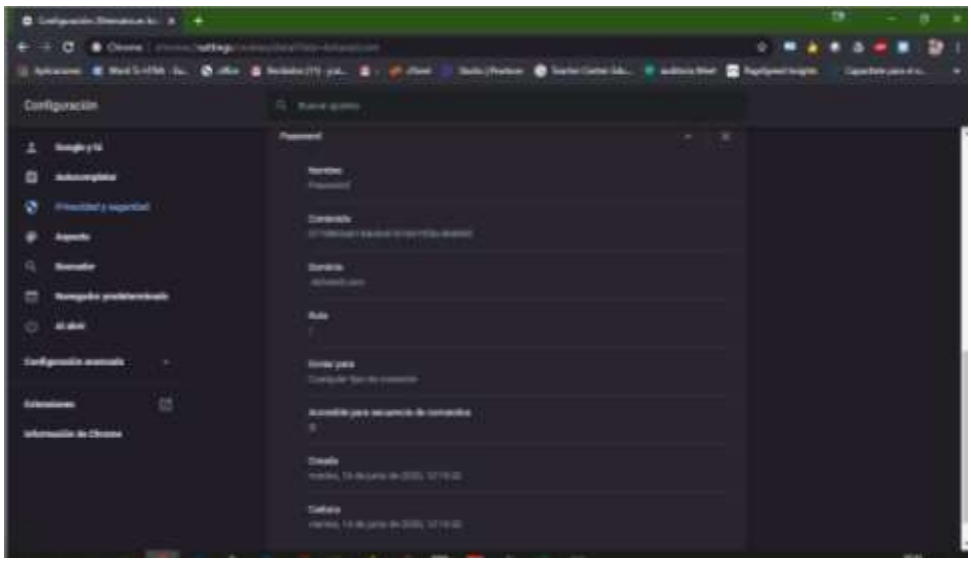



**Fig. 133.** Descripción de las cookies
**Fuente:** Elaborado por el Investigador

### 3.1.4.6.3. Filtración de información

- Al revisar la página web de la institución por medio del visor de html y buscar en las carpetas donde se guarda la información, no se encontró ninguna información comprometedora sobre la institución.

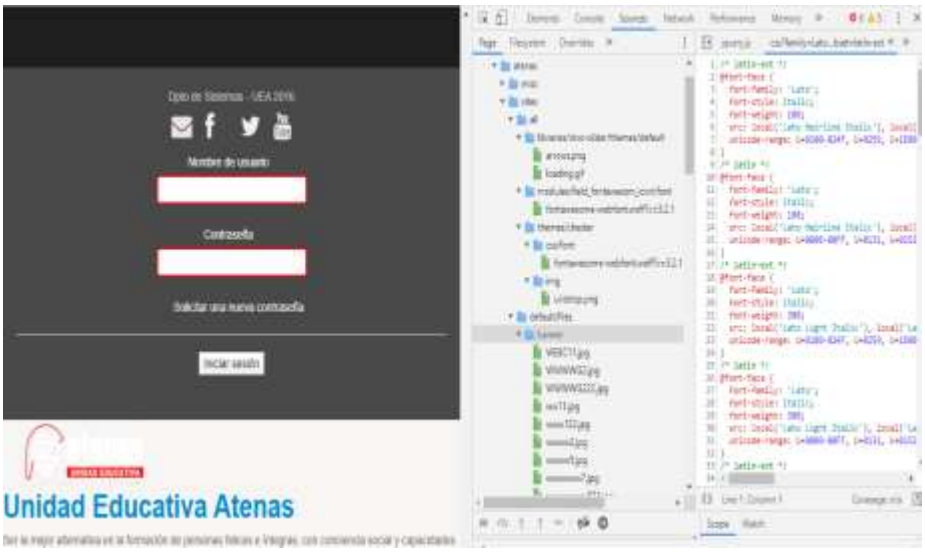



**Fig. 134.** Html página web Atenas inspección carpetas
**Fuente:** Elaborado por el Investigador

- Al examinar los banners contenidos en la página web de la institución no se encontró alguna información que sea delicada o privada. Solo se encontró imágenes y hojas de estilo CSS referenciadas a cada una de las imágenes de muestra.

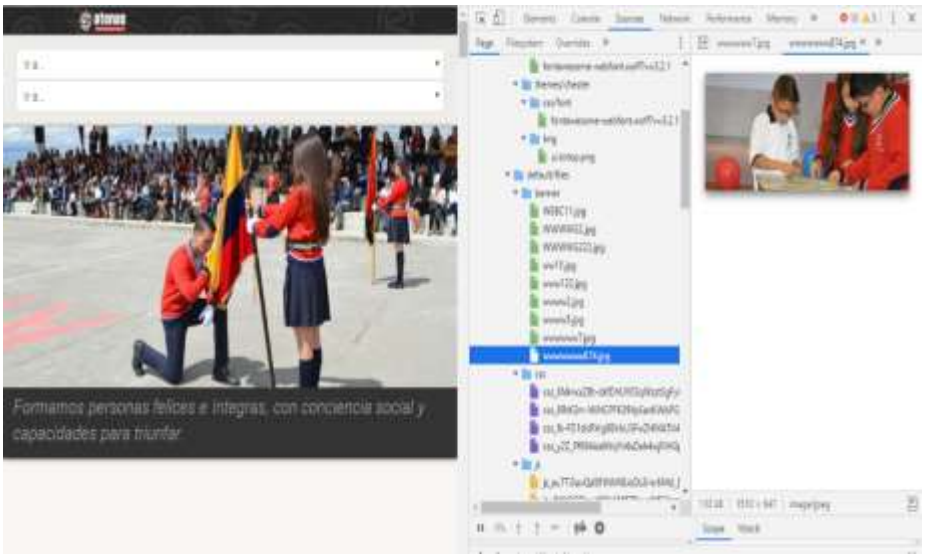



**Fig. 135.** Html página web Atenas inspección banner
**Fuente:** Elaborado por el Investigador

### 3.1.4.7. Testeo de control de acceso

#### 3.1.4.7.1. El Cortafuegos y sus características.

- Verificar el tipo de router.
  La fundación cultural y educativa Ambato (Unidad Educativa Atenas) posee router tplink, distribuidos en el colegio y en la escuela con configuraciones básicas solo para acceso por wifi tomando en cuenta la protección de WAP2.

- Verificar si el router está dando servicio de traducción de direcciones de red (NAT).

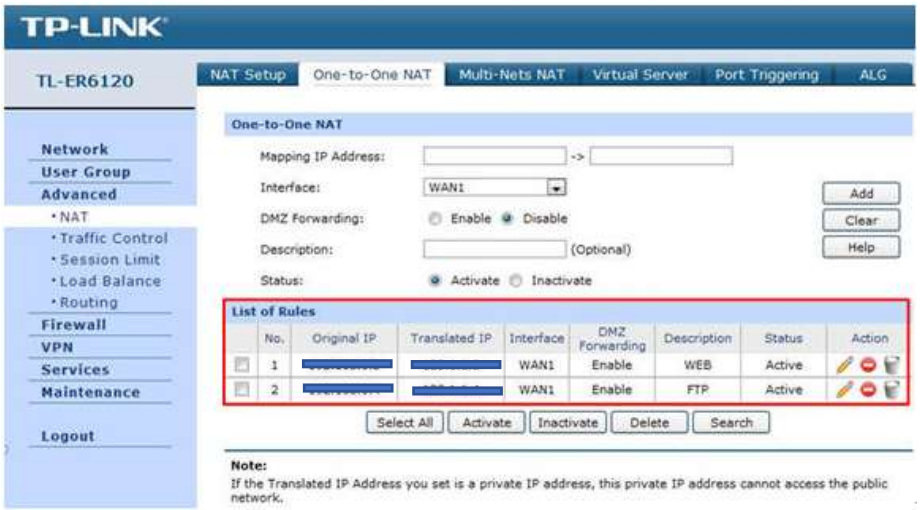



**Fig. 136.** Configuración de router Tplink
**Fuente:** Elaborado por el Investigador

- Verificar las intrusiones con opciones TTL estratégicas en los paquetes, (Firewalking) hecho en el módulo de escaneo de puertos.

  Las TTL o tiempo de vida es cuánto dura en estar almacenado un registro DNS en la memoria local antes de ser eliminado.

```
config system session-ttl
    set default [redacted]
    config port
        edit [redacted]
            set protocol [redacted]
            set timeout 10
            set start-port [redacted]
            set end-port [redacted]
        next
    end
```

**Fig. 137.** Configuración TTL
**Fuente:** Elaborado por el Investigador

Como se pudo encontrar la configuración que tenía la institución era la que bien predeterminada de esta manera los registros no quedaran por mucho tiempo en memoria.

### 3.1.4.7.2. Verificación de la configuración de las ACL

- Testear la ACL del cortafuego.

```
config firewall multicast-address
     edit "all"
          set start-ip 224.0.0.0
          set end-ip 239.255.255.255
     next
     edit "all_hosts"
          set start-ip 224.0.0.1
          set end-ip 224.0.0.1
     next
     edit "all_routers"
          set start-ip 224.0.0.2
          set end-ip 224.0.0.2
     next
     edit "Bonjour"
          set start-ip 224.0.0.251
          set end-ip 224.0.0.251
     next
     edit "EIGRP"
          set start-ip 224.0.0.10
          set end-ip 224.0.0.10
     next
     edit "OSPF"
          set start-ip 224.0.0.5
          set end-ip 224.0.0.6
     next
end
```

**Fig. 138.** Configuración ACL
**Fuente:** Elaborado por el Investigador

Se puede ver la configuración de varios protocolos que realiza el firewall

- Verificar si el cortafuego está filtrando el tráfico de la red local hacia afuera.

```
config firewall service group
    edit "Email Access"
        set member "DNS" "IMAP" "IMAPS" "POP3" "POP3S" "SMTP" "SMTPS"
    next
    edit "Web Access"
        set member "DNS" "HTTP" "HTTPS"
    next
    edit "Windows AD"
        set member "DCE-RPC" "DNS" "KERBEROS" "LDAP" "LDAP_UDP" "SAMBA" "SMB"
    next
    edit "Exchange Server"
        set member "DCE-RPC" "DNS" "HTTPS"
    next
    edit "File Acces"
        set member "AFS3" "FTP" "FTP_GET" "FTP_PUT" "NFS" "SAMBA" "SMB" "TFTP"
    next
end
```

**Fig. 139.** Configuración de filtrado del firewall
**Fuente:** Elaborado por el Investigador

- Testear las capacidades externas de los cortafuegos desde el interior determinando los métodos de identificación de cortafuegos.

```
end
config system replacemsg fortiguard-wf "http-err"
end
config system replacemsg spam "ipblocklist"
end
config system replacemsg alertmail "alertmail-virus"
end
config system replacemsg admin "pre_admin-disclaimer-text"
end
config system replacemsg auth "auth-disclaimer-page-1"
end
config system replacemsg sslvpn "sslvpn-login"
end
config system replacemsg ec "endpt-download-portal"
end
config system replacemsg device-detection-portal "device-detection-failure"
end
config system replacemsg nac-quar "nac-quar-virus"
end
config system replacemsg traffic-quota "per-ip-shaper-block"
end
config system replacemsg utm "virus-html"
end
config system replacemsg icap "icap-req-resp"
end
```

**Fig. 140.** Métodos de identificación del firewall
**Fuente:** Elaborado por el Investigador

- Verificar la habilidad de los cortafuegos que tiene para protegerse.

```
next
edit "Panda-Antivirus+Firewall-2008-AV"
     set guid "EEE2D94A-D4C1-421A-AB2C-2CE8FE51747A"
next
edit "Panda-Antivirus+Firewall-2008-FW"
     set type fw
     set guid "7B090DC0-8905-4BAF-8040-FD98A41C8FB8"
next
edit "Panda-Internet-Security-AV"
     set guid "4570FB70-5C9E-47E9-B16C-A3A6A06C4BF0"
next
edit "Panda-Internet-Security-2006~2007-FW"
     set type fw
     set guid "4570FB70-5C9E-47E9-B16C-A3A6A06C4BF0"
next
edit "Panda-Internet-Security-2008~2009-FW"
     set type fw
     set guid "7B090DC0-8905-4BAF-8040-FD98A41C8FB8"
next
edit "Sophos-Anti-Virus"
     set guid "3F13C776-3CBE-4DE9-8BF6-09E5183CA2BD"
next
edit "Sophos-Enpoint-Secuirty-and-Control-FW"
     set type fw
     set guid "0786E95E-326A-4524-9691-41EF88FB52EA"
next
edit "Sophos-Enpoint-Secuirty-and-Control-AV-Vista-Win7"
     set guid "479CCF92-4960-B3E0-7373-BF453B467D2C"
next
edit "Sophos-Enpoint-Secuirty-and-Control-FW-Vista-Win7"
     set type fw
     set guid "7FA74EB7-030F-B2B8-582C-1670C5953A57"
```

**Fig. 141.** Protección del firewall
**Fuente:** Elaborado por el Investigador

- Verificar la habilidad de los cortafuegos para protegerse de varias técnicas de ataque.

```
config firewall ssl-ssh-profile
    edit "custom-deep-inspection"
        set comment "Customizable deep inspection profile."
        config https
            set ports 443
        end
        config ftps
            set ports 990
        end
        config imaps
            set ports 993
        end
        config pop3s
            set ports 995
        end
        config smtps
            set ports 465
        end
        config ssh
            set ports 22
            set status disable
        end
        config ssl-exempt
            edit 29
                set fortiguard-category 31
            next
            edit 30
                set fortiguard-category 33
            next
        end
        set caname "Fortinet_CA_SSLProxy"
        set ssl-anomalies-log disable
```

**Fig. 142.** Habilidad del firewall en contra de un ataque
**Fuente:** Elaborado por el Investigador

### 3.1.4.7.3. Revisión de Registros del Cortafuegos

- Testear el proceso de registro de los cortafuegos y verificación deficiencias de registros de servicios.

```
end
config system replacemsg http "urlfilter-err"
end
config system replacemsg http "infcache-block"
end
config system replacemsg http "http-block"
end
config system replacemsg http "http-filesize"
end
config system replacemsg http "http-dlp-ban"
end
config system replacemsg http "http-archive-block"
end
config system replacemsg http "http-contenttypeblock"
end
config system replacemsg http "https-invalid-cert-block"
end
config system replacemsg http "http-client-block"
end
config system replacemsg http "http-client-filesize"
end
config system replacemsg http "http-client-bannedword"
end
config system replacemsg http "http-post-block"
end
config system replacemsg http "http-client-archive-block"
end
config system replacemsg http "switching-protocols-block"
```

**Fig. 143.** Procesos y verificación de registros en el firewall
**Fuente:** Elaborado por el Investigador

### 3.1.4.7.4. Testeo de denegación de servicios

- Verificar que las cuentas administrativas

```
next
edit "jcalvache"
    set accprofile "super_admin"
    set vdom "root"
    set email-to "jcalvache@atenas.edu.ec"
    set password ENC
SH2XxPeo502Lbe+DKBUTJjoVXAWB/4AGzrvOknyMA5pFSj9BkT1VTCBsMjosvA=
```

**Fig. 144.** Configuración de cuentas del firewall
**Fuente:** Elaborado por el Investigador

- Ver si los usuarios están apropiadamente creados con "Mínimo Privilegio".

```
set timezone-option default
config reserved-address
    edit 1
        set ip 192.168.2.2
        set mac f8:59:71:02:54:c2
        set description "JoseCuesta"
    next
    edit 2
        set ip 192.168.2.3
        set mac 94:e9:79:b9:cf:cb
        set description "PabloVasconez"
```

**Fig. 145.** Configuración de usuarios con privilegios en el firewall
**Fuente:** Elaborado por el Investigador

- Verificar que los puntos de referencian están establecidos a partir de una actividad normal del sistema.

```
next
edit "Patricia Aguaysa Portatil Cable"
    set uuid 38197faa-9c16-51e9-4554-eff9c1afc6dc
    set comment "Conexion por cable PC Desktop"
    set color 6
    set subnet 10.10.4.9 255.255.255.255
```

**Fig. 146.** Actividad de un usuario especifico
**Fuente:** Elaborado por el Investigador

### 3.1.5. SEGURIDAD EN LAS COMUNICACIONES

#### 3.1.5.1.Testeo del Correo de Voz

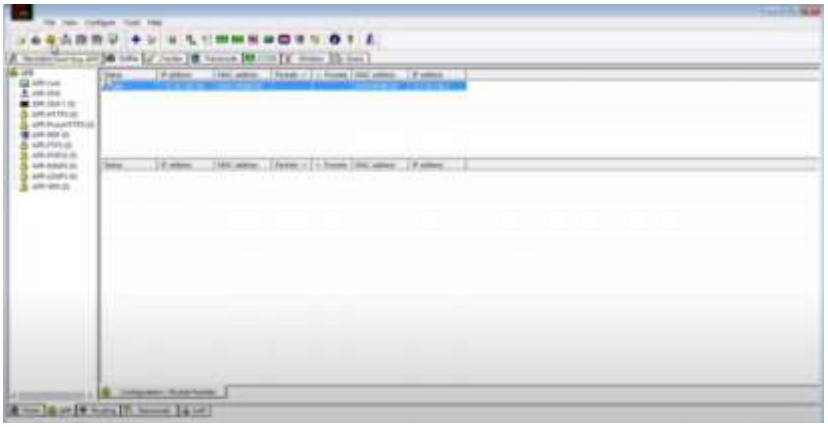


**Fig. 147.** Recepción de información Cain & Abel
**Fuente:** Elaborado por el Investigador

Se realizó una prueba de penetración para obtener información o configuración en los teléfonos IP se usó Cain & Abel el cual mediante una llamada se podía ingresar a las opciones del teléfono también se realizó de prueba de grabación de llamadas en la cual la configuración predeterminada del teléfono lo bloqueo.

#### 3.1.5.2.Testeo del Modem

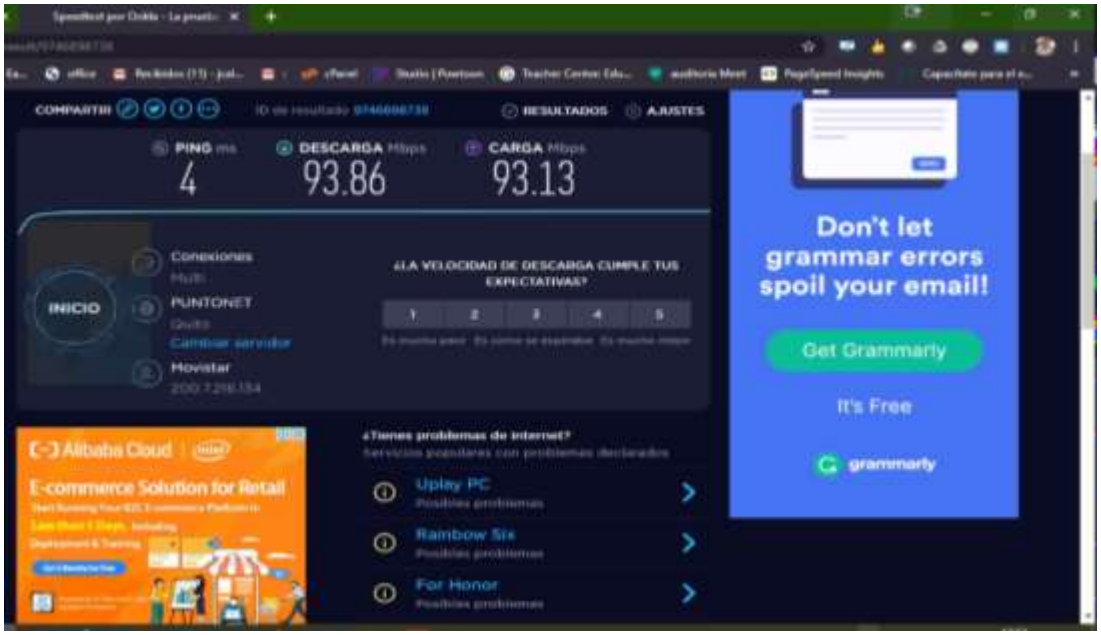



**Fig. 148.** Testeo de velocidad de internet
**Fuente:** Elaborado por el Investigador

Como se puede ver en el test de velocidad realizado por Speed Smart apreciamos que la velocidad es igual a --- de subida y --- bajada esto se debe al proveedor de internet que realizo las configuraciones previas.

### 3.1.6. SEGURIDAD INALÁMBRICA

#### 3.1.6.1.Verificación de Redes Inalámbricas [802.11]

Para la verificación de redes inalámbricas se usó el estándar IEEE 802.11 el cual propone 3 aspectos esenciales en la seguridad de las WLAN que son la Autenticación, Confidencialidad y la integridad.

#### 3.1.6.2.Verificación de Dispositivos de Vigilancia Inalámbricos sin acceso

**Fig. 149.** Cámaras de seguridad
**Fuente:** Elaborado por el Investigador

Todos los dispositivos de vigilancia están perfectamente colocados, configurados desde un VDR en el cual tienen acceso los analistas de sistemas los que monitorean las cámaras.

#### 3.1.6.3.Verificación de RFID

**Fig. 150.** Access Point Radio frecuencia
**Fuente:** Elaborado por el Investigador

Es una forma de comunicación inalámbrica en la cual participa un emisor y un receptor, la comunicación se la realiza mediante ondas de radio donde se procede a una configuración de direcciones IP tanto para el emisor como para el receptor.

### 3.1.7. SEGURIDAD FÍSICA

#### 3.1.7.1.Revisión de Perímetro

La Fundación cultural y Educativa Ambato (Unidad Educativa Atenas) tienen un cerramiento del lote de terreno que conforma la institución de igual manera el estacionamiento, todo respectivamente con forme la ley lo recomienda, siguiendo lo recomendado y las normas específicas.

#### 3.1.7.2.Revisión de monitoreo

El monitoreo es realizado por cámaras de seguridad cuidadosamente ubicadas en toda la Unidad Educativa, las cuales son verificadas por el departamento de sistemas, encargándose del funcionamiento y su mantenimiento.

El control de los servidores y la revisión con las actualizaciones son realizadas periódicamente de esta manera se puede asegurar la seguridad.

#### 3.1.7.3.Evaluación de Controles de Acceso

La Fundación cultural y Educativa Ambato (Unidad Educativa Atenas) realizan un control personalizado por el personal de recepción tomando una identificación y el motivo de la visita. Además, la unidad cuenta con servicio de vigilancia privado las 24 horas del día.

#### 3.1.7.4.Revisión de Ubicación

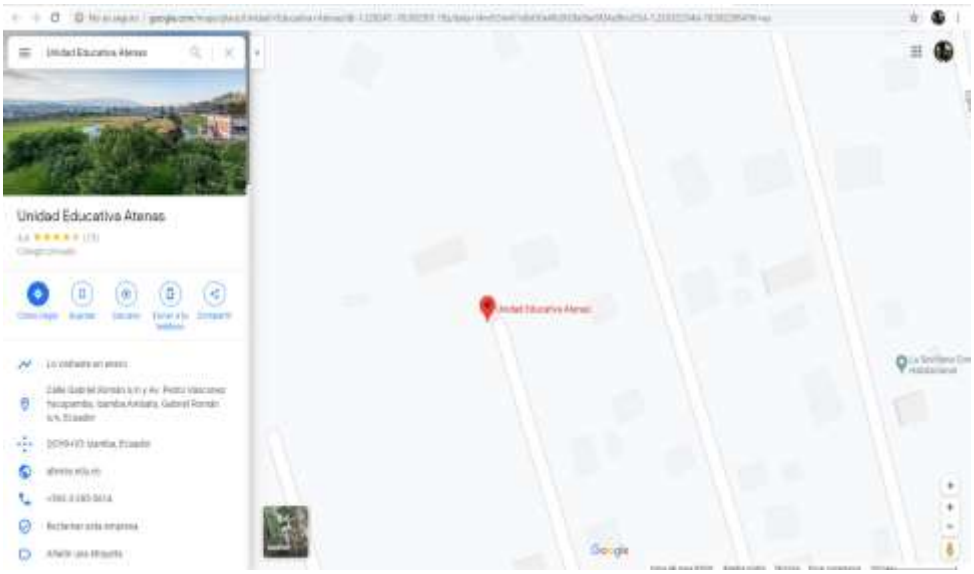



**Fig. 151.** Ubicación Fundación cultural y Educativa Ambato (Unidad Educativa Atenas)
**Fuente:** Elaborado por el Investigador

### 3.1.7.5.Revisión de Entorno

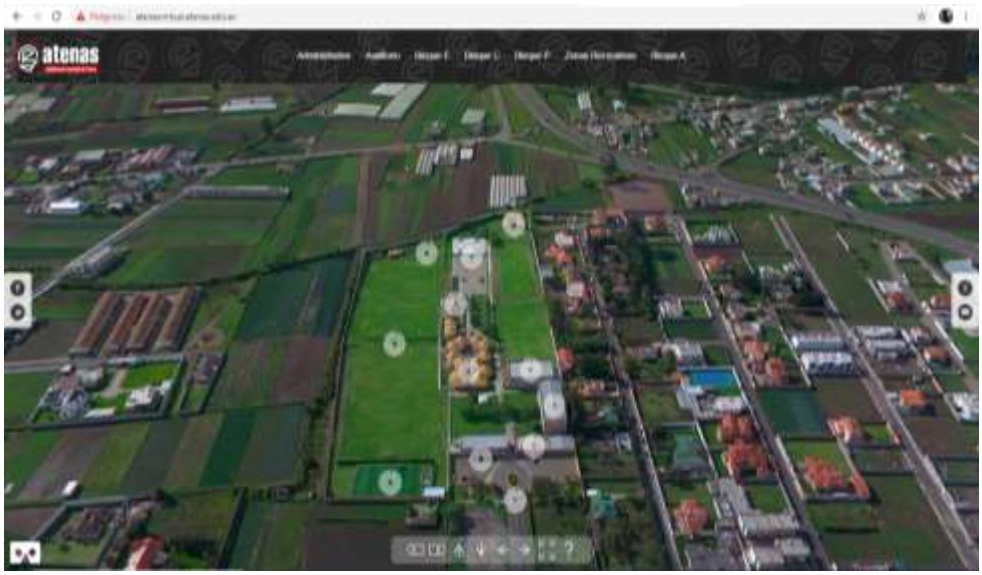



**Fig. 152.** Mapa real del Entorno de la Fundación cultural y Educativa Ambato (Unidad Educativa Atenas)
**Fuente:** Elaborado por el Investigador

# CAPITULO IV

# CONCLUSIONES Y RECOMENDACIONES

## 1.1. Conclusiones

Al culminar con el proyecto de investigación se han obtenido las siguientes conclusiones:

- OSSTMM como herramienta, nos ayudó para entender como estaba la situación actual de la Fundación Cultural y Educativa Ambato (UNIDAD EDUCATIVA ATENAS) mediante un análisis se pudo determinar los puntos donde podía ser aplicado la metodología, determinando cada uno de los riesgos a los cuales estaba expuesto.

- Aplicando la metodología OSSTMM, logramos identificar los riesgos y las vulnerabilidades a la que estaba expuesta la Fundación Cultural y Educativa Ambato (UNIDAD EDUCATIVA ATENAS) tanto en la parte física, entorno y equipos informáticos.

- Mediante el uso de herramientas para escanear vulnerabilidades y técnicas de ingeniería social se pudo identificar riesgos en partes tecnológicas y humanas referente a Seguridad Informática, mediante estos ataques se pudo analizar las debilidades a las que está expuesta la información.

- El uso de la metodología OSSTMM para el análisis e identificación de riesgos informáticos brinda de una manera muy ordenada de cómo proceder a identificar las vulnerabilidades existente mediante su distribución en fases y módulos, con los resultados obtenidos en los ataques al personal y a los equipos informáticos tanto de manera externa como interna se puede determinar el control necesario que permita mitigar los riesgos encontrados y de esta manera poder proteger la integridad y confidencialidad de la información.

### 1.2. Recomendaciones

Al culminar con el proyecto de investigación se han obtenido las siguientes recomendaciones:

- Al ocupar la metodología OSSTMM se debe realizar un análisis previo para poder determinar lo que es posible y necesario aplicar para descubrir los riesgos, y mediante el análisis previo poder seleccionar las herramientas necesarias para realizar los ataques y poder especificar las soluciones necesarias.

- La Fundación Cultural y Educativa Ambato (UNIDAD EDUCATIVA ATENAS) debe realizar una inducción en la cual se capacite al personal administrativo y a los docentes sobre la utilización correcta de la información para prevenir ataques informáticos enfocados en Ingeniería Social para conocer vulnerabilidades humanas.

- Se debe tener en claro que cada día la tecnología se actualiza y encuentran nuevas amenazas para nuestros datos, en caso de tener servidores es muy conveniente tener actualizado sus versiones ya que en el caso de Microsoft al determinar una vulnerabilidad esta lanza una actualización con parches los cuales ayudan a mitigar los riesgos de infiltración de información.

- Usar 2 herramientas para determinar análisis de vulnerabilidades para de esa manera poder evitar todos los falsos positivos que pueden encontrase cuando se realizan los ataques.

- Realizar acciones preventivas por parte del analista de sistemas antes que se produzca un ataque, organizando revisiones periódicas del funcionamiento de los servidores tomando en cuenta cada una de las soluciones a las vulnerabilidades encontradas.

- Se recomienda al analista de sistemas realizar un análisis de riesgos de la Fundación Cultural y Educativa Ambato (UNIDAD EDUCATIVA ATENAS),

detallando las vulnerabilidades encontradas en el cual se verifique el cumplimiento de las políticas y controles establecidos por la institución.

## BIBLIOGRAFÍA


[1] Acurio Del Pino, S. (2005). Delitos Informáticos. Generalidades. Crimen Organizado Transnacional: Definición, Causas Y Consecuencias, Editorial Astrea.

[2] Y. A. Zhangeriev, "What are Criterias for Substantiation of Scientific Recommendations?" Vestn. Ross. Akad. Nauk, 1996.

[3] A. Sánchez-Henarejos, J. L. Fernández-Alemán, A. Toval, I. Hernández-Hernández, A. B. Sánchez-García, and J. M. Carrillo De Gea, "Guía de buenas prácticas de seguridad informática en el tratamiento de datos de salud para el personal sanitario en atención primaria," Aten. Primaria, 2014.

[4] S. Argentina and D. R. Arias, "Los desafíos de la ciberseguridad y la ciberdefensa."

[5] D. Édison et al., "Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas Informatic organizational security: a simulation model based on systems dynamic," Sci. Tech. Año XXII, vol. 22, no. 2, 2017.

[6] INCAP. (s.f.). www.incap.int. Recuperado el julio de 2018, de http://www.incap.int/sisvan/index.php/es/acerca-de-san/conceptos/797sin-categoria/501-sistema-de-informacion.

# ANEXOS

**Anexo 1:** Encuesta para aplicación verificación de que módulos son aplicables.

**UNIVERSIDAD TÉCNICA DE AMBATO**
**FACULTAD DE TECNOLOGÍAS DE LA INFORMACIÓN, TELECOMUNICACIONES E INDUSTRIAL**
**INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS**

**Objetivo:** Analizar los módulos que son posibles aplicar en la Fundación cultural y educativa Ambato (UNIDAD EDUCATIVA ATENAS), pertenecientes a la metodología OSSTMM.

**Instructivo:** Seleccione con una X una de las opciones que usted considere conveniente en cada pregunta.

**¿Determine si es posible la aplicación de los siguientes modelos de la metodología OSSTMM, dependiendo la infraestructura en la que se desarrolle?**

- **Identificado**, pero no investigado o con resultados no concluyentes.
- **Verificado**, con un positivo absoluto o una vulnerabilidad explotada, o
- **No aplicable**, debido a que no existe porque la infraestructura o mecanismo de seguridad no se encuentra presente.

**SEGURIDAD DE LA INFORMACIÓN**

1. **Revisión de la Inteligencia Competitiva**

   Una medición de las justificaciones de negocio de la red de la organización. Tamaño y alcance de la presencia en Internet. Una medición de la política de seguridad a planes futuros de la red.

| | |
|---|---|
| Identificado | X |
| Verificable | |
| No Aplicable | |

2. **Revisión de Privacidad**

   Lista de cualquier revelación. Lista de las fallas de conformidad entre la política pública y la práctica actual. Lista de los sistemas involucrados en la recolección de datos. Lista de las técnicas de obtención de datos. Lista de los datos obtenidos

| | |
|---|---|
| Identificado | X |

Verificable ☐

No Aplicable ☐

**3. Recolección de Documentos**

Un perfil de la organización. Un perfil de los empleados. Un perfil de la red de la organización. Un perfil de las tecnologías de la organización. Un perfil de los socios, alianzas y estrategias de la organización.

Identificado ☒

Verificable ☐

No Aplicable ☐

**SEGURIDAD DE LOS PROCESOS**

**4. Testeo de Solicitud**

Lista de los métodos de código de acceso. Lista de los códigos validos Nombres de las personas de entrada. Métodos de obtención de esta información. Lista de la información obtenida.

Identificado ☐

Verificable ☒

No Aplicable ☐

**5. Testeo de Sugerencia Dirigida**

Lista de los puntos de acceso. Lista de las direcciones IP internas. Métodos de obtención de esta información. Lista de la información obtenida

Identificado ☐

Verificable ☒

No Aplicable ☐

**6. Testeo de las Personas Confiables**

Lista de las personas de confianza. Lista de las posiciones de confianza. Métodos de obtención de esta información. Lista de la información obtenida.

Identificado ☐

Verificable ☐

No Aplicable ☒

**7. Logística y Controles**

Discrepancias por el Ancho de Banda usado en el Testeo. Paquetes TCP perdidos. Paquetes UDP perdidos. Paquetes ICMP perdidos. Problemas de enrutamiento. Tráfico de Enrutamiento del ISP y Vendedores de Tráfico

| | |
|---|---|
| Identificado | ☐ |
| Verificable | ☒ |
| No Aplicable | ☐ |

**8. Sondeo de Red**

Nombres de Dominio. Nombres de Servidores. Direcciones IP. Mapa de Red. Información ISP / ASP. Propietarios del Sistema y del Servicio. Posibles limitaciones del test.

| | |
|---|---|
| Identificado | ☐ |
| Verificable | ☒ |
| No Aplicable | ☐ |

**9. Identificación de los Servicios de Sistemas**

Puertos abiertos, cerrados y filtrados. Direcciones IP de los sistemas activos. Direccionamiento de los sistemas de la red interna. Lista de los protocolos descubiertos de tunelizado y encapsulado. Lista de los protocolos descubiertos de enrutado soportados. Servicios activos Tipos de Servicios. Tipo y nivel de parcheado de las Aplicaciones de los Servicios. Tipo de Sistema Operativo. Nivel de parcheado. Tipo de Sistema. Lista de sistemas activos. Mapa de la red.

| | |
|---|---|
| Identificado | ☐ |
| Verificable | ☒ |
| No Aplicable | ☐ |

**10. Búsqueda de Información Competitiva**

Una medida de las justificaciones de negocio sobre la red de la organización. Tamaño y alcance de la presencia en Internet. Una medición de la política de seguridad a planes futuros de la red.

Identificado ☐

Verificable ☐

No Aplicable ☒

**11. Revisión de Privacidad**

Listado de cualquier revelación. Listado de las inconsistencias entre la política que se ha hecho pública y la práctica actual que se hace de ella. Listado de los sistemas involucrados en la recolección de datos. Listado de las técnicas de recolección de datos. Listado de los datos recolectados.

Identificado ☐

Verificable ☒

No Aplicable ☐

**12. Obtención de Documentos**

Un perfil de la organización. Un perfil de los empleados. Un perfil de la red de la organización. Un perfil de las tecnologías utilizadas por la organización. Un perfil de los partners, alianzas y estrategias de la organización.

Identificado ☒

Verificable ☐

No Aplicable ☒

**13. Búsqueda y Verificación de Vulnerabilidades**

Tipo de aplicación o servicio por vulnerabilidad. Niveles de parches de los sistemas y aplicaciones. Listado de posibles vulnerabilidades de denegación de servicio. Listado de áreas securizadas a través de ocultación o acceso visible. Listado de vulnerabilidades actuales eliminando falsos. Listado de sistemas internos o en la DMZ. Listado de convenciones para direcciones de e-mail, nombres de servidores, etc. Mapa de red

Identificado ☐

Verificable ☒

No Aplicable ☐

**14. Testeo de Aplicaciones de Internet**

Lista de Aplicaciones. Lista de los Componentes de las Aplicaciones. Lista de las Vulnerabilidades de las Aplicaciones. Lista de los Sistemas Confiados por las Aplicaciones.

| | |
|---|---|
| Identificado | ☐ |
| Verificable | ☒ |
| No Aplicable | ☐ |

**15. Enrutamiento**

Tipo de Router y Propiedades implementadas. Información del router como servicio y como sistema. Perfil de la política de seguridad de una red a partir de la ACL. Lista de los tipos de paquetes que deben entrar en la red. Mapa de las respuestas del router a varios tipos de tráfico. Lista de los sistemas vivos encontrados

| | |
|---|---|
| Identificado | ☐ |
| Verificable | ☐ |
| No Aplicable | ☒ |

**16. Testeo de Sistemas Confiados**

Mapa de los sistemas dependientes de otros sistemas. Mapa de las aplicaciones con dependencias a otros sistemas. Tipos de vulnerabilidades que afectan a los sistemas de confianzas y aplicaciones.

| | |
|---|---|
| Identificado | ☐ |
| Verificable | ☐ |
| No Aplicable | ☒ |

**17. Testeo de Control de Acceso**

Información en el firewall como servicio y como sistema. Información de las características implementadas en el firewall. Perfil de la política de seguridad de la red a partir de la ACL. Lista de los tipos de paquetes que deben entrar en la red. Lista de tipos de protocolos con acceso dentro de la red. Lista de los sistemas "vivos" encontrados. Lista de paquetes, por número de puerto, que entran en la red. Lista de protocolos que han entrado en la red. Lista de rutas sin monitorizar dentro de la red

Identificado ☐

Verificable ☒

No Aplicable ☐

**18. Testeo de Sistema de Detección de Intrusos**

Tipo de IDS. Nota del rendimiento de los IDS bajo una sobrecarga. Tipo de paquetes eliminados o no escaneados por el IDS. Tipo de protocolos eliminados o no escaneados por el IDS. Nota del tiempo de reacción y tipo del IDS. Nota de la susceptibilidad del IDS. Mapa de reglas del IDS. Lista de falsos positivos del IDS. Lista de alarmas perdidas del IDS. Lista de rutas no monitorizadas en la red

Identificado ☐

Verificable ☐

No Aplicable ☒

**19. Testeo de Medidas de Contingencia**

Definición de las capacidades Anti-Troyano. Definición de las capacidades Anti-Virus. Identificación de las Medidas de Contingencia de Escritorio. Identificación de las Debilidades de Contingencia de Escritorio. Lista de recursos de contingencia.

Identificado ☒

Verificable ☐

No Aplicable ☒

**20. Descifrado de Contraseña**

Ficheros de Contraseñas descifrados o no descifrados. Lista de cuentas, con usuario o contraseña de sistema. Lista de sistemas vulnerables a ataques de descifrado de contraseñas. Lista de archivos o documentos vulnerables a ataques de descifrado de contraseñas. Lista de sistemas con usuario o cuenta de sistema que usan las mismas contraseñas.

Identificado ☐

Verificable ☐

No Aplicable ☒

**21. Testeo de Denegación de Servicios**

Lista de puntos débiles en presencia de Internet incluidos los puntos individuales por averías. Establecer un punto de referencia para un uso normal. Lista de comportamientos de sistema por un uso excesivo. Lista de sistemas vulnerables a DoS.

| | |
|---|---|
| Identificado | ☐ |
| Verificable | ☐ |
| No Aplicable | ☒ |

**22. Evaluación de Políticas de Seguridad**

| | |
|---|---|
| Identificado | ☒ |
| Verificable | ☐ |
| No Aplicable | ☒ |

**SEGURIDAD EN LAS COMUNICACIONES**

**23. Testeo de PBX**

Lista de sistemas PBX que permitan ser administrados remotamente Lista de los sistemas que permitan acceso desde cualquier lugar del mundo a la terminal de mantenimiento. Lista de todos los sistemas telefónicos que estén en modo de escucha y de manera interactiva.

| | |
|---|---|
| Identificado | ☐ |
| Verificable | ☐ |
| No Aplicable | ☒ |

**24. Testeo del Correo de Voz**

Lista de las casillas de correo de voz que son accesibles desde cualquier ubicación en el mundo. Lista de los códigos de llamadas entrantes a las casillas de correo de voz y sus correspondientes Números de Identificación Personal (PINs).

| | |
|---|---|
| Identificado | ☐ |
| Verificable | ☒ |
| No Aplicable | ☐ |

**25. Revisión del FAX**

Lista de los sistemas de FAX. Lista de los tipos de sistemas de FAX y sus posibles programas operativos. Recopilación de información alojada en la memoria de los sistemas de FAX. Mapa del manejo de protocolos de FAX dentro de la organización.

| | |
|---|---|
| Identificado | ☐ |
| Verificable | ☐ |
| No Aplicable | ☒ |

**26. Testeo del Modem**

Lista de los sistemas con módems que se encuentren a la escucha. Lista de los tipos modem y sus programas operativos. Lista de los esquemas de autenticación de los módems. Lista de usuarios y contraseñas de acceso vía modem Mapa del manejo de protocolos de modem dentro de la organización.

| | |
|---|---|
| Identificado | ☐ |
| Verificable | ☒ |
| No Aplicable | ☐ |

**SEGURIDAD INALÁMBRICA**

**27. Verificación de Radiación Electromagnética (EMR)**

Evaluar las Necesidades de Negocio, Prácticas, Políticas y Ubicaciones de las Áreas Sensibles. Evaluar el Equipamiento y Ubicación. Evaluar y Verificar el Cableado y Emisiones.

| | |
|---|---|
| Identificado | ☒ |
| Verificable | ☐ |
| No Aplicable | ☒ |

**28. Verificación de Redes Inalámbricas [802.11]**

**Especificaciones 802.11:**

| | |
|---|---|
| **Capa Física** | Secuencia Directa en Espectro Ensanchado (DSSS), Saltos de Frecuencia en Espectro Ensanchado (FHSS), infrarrojos (IR) |
| **Cifrado por defecto** | Algoritmo de cifrado basado en flujo RC4 para confidencialidad, autenticación, y integridad. Gestión de Claves limitada. |
| **Rango de Operación** | Unos 150 pies en interiores y 1500 en exterior. |

Identificado [X]

Verificable [ ]

No Aplicable [ ]

**29. Verificación de Redes Bluetooth**

Verificación de redes Bluetooth de tipo ad-hoc (piconets), las cuales son populares en las redes inalámbricas de área personal (PANs) pequeñas y de poco ancho de banda.

Identificado [ ]

Verificable [ ]

No Aplicable [X]

**30. Verificación de Dispositivos de Entrada Inalámbricos**

Se trata de los dispositivos de entrada inalámbricos tales como ratones y teclados. Estos dispositivos se están popularizando aunque presentan profundas vulnerabilidades y compromisos en privacidad y seguridad.

Identificado [ ]

Verificable [ ]

No Aplicable [X]

**31. Verificación de Dispositivos de Mano Inalámbricos**

Identificado [ ]

Verificable [ ]

No Aplicable [X]

**32. Verificación de Comunicaciones sin Cable**

Verificación de dispositivos de comunicación sin cables que puedan sobrepasar los límites físicos y monitorizados de una organización. Esto incluye la verificación

de interferencia entre tipos diferentes o similares de comunicación dentro de una organización y sus organizaciones vecinas.

| | |
|---|---|
| Identificado | X |
| Verificable | |
| No Aplicable | x |

**33. Verificación de Dispositivos de Vigilancia Inalámbricos**

Dispositivos de vigilancia inalámbricos que han empezado recientemente a reemplazar los alámbricos – tales como cámaras, micrófonos, etc.

| | |
|---|---|
| Identificado | |
| Verificable | x |
| No Aplicable | |

**34. Verificación de Dispositivos de Transacción Inalámbricos**

Dispositivos de transacción inalámbricos instalados en numerosas tiendas. Este equipamiento se está utilizando para proporcionar conexión con cajas registradoras y otros dispositivos de punto de venta a lo largo de los comercios.

| | |
|---|---|
| Identificado | |
| Verificable | |
| No Aplicable | X |

**35. Verificación de RFID**

Las etiquetas de RFID (Radio Frequency Identifier) se componen de un circuito integrado (IC), a menudo del tamaño de medio grano de arena, y una antena – habitualmente una espiral de cables. La información está almacenada en el IC y se transmite mediante la antena.

| | |
|---|---|
| Identificado | |
| Verificable | X |
| No Aplicable | |

**36. Verificación de Sistemas Infrarrojos**

Este es el método de verificación de dispositivos de comunicaciones infrarrojas que pudieran sobrepasar los límites físicos y monitorizados de la organización.

Identificado ☐

Verificable ☐

No Aplicable ☒

**37. Revisión de Privacidad**

Enumerar cualquier revelación. Enumerar las anomalías en el cumplimiento entre la política pública y la práctica actual. Enumerar las comunicaciones inalámbricas involucradas en la obtención de datos. Enumerar las técnicas de obtención de datos. Enumerar los datos obtenidos.

Identificado ☒

Verificable ☐

No Aplicable ☒

**SEGURIDAD FÍSICA**

**38. Revisión de Perímetro**

Mapa del perímetro físico. Tipos de medidas de protección física. Lista de áreas desprotegidas o insuficientemente protegidas.

Identificado ☒

Verificable ☐

No Aplicable ☐

**39. Revisión de monitoreo**

Lista de puntos de acceso monitoreados. Tipos de monitoreo. Lista de puntos de acceso estándar y privilegiados, no monitoreados. Lista de disparadores de alarmas.

Identificado ☐

Verificable ☒

No Aplicable ☐

**40. Evaluación de Controles de Acceso**

Lista de puntos de acceso físicos. Tipos de autenticación. Tipos de sistemas de alarmas. Lista de disparadores de alarmas.

Identificado ☐

Verificable [X]

No Aplicable [ ]

**41. Revisión de Respuesta de Alarmas**

Lista de tipos de alarmas. Lista de disparadores de alarmas. Mapa de procedimiento en caso de alarma. Lista de personas involucradas en el procedimiento en caso de alarma. Lista de medidas de contención y precauciones de seguridad activadas por alarmas.

Identificado [ ]

Verificable [ ]

No Aplicable [X]

**42. Revisión de Ubicación**

Mapa de ubicación física de los bienes. Lista de ubicación física de los puntos de acceso. Lista de puntos de acceso vulnerables en la ubicación. Lista de la ubicación de los accesos de terceras partes.

Identificado [X]

Verificable [ ]

No Aplicable [ ]

**43. Revisión de Entorno**

Mapa físico de bienes en cada ubicación. Lista de ubicaciones vulnerables. Lista de leyes, costumbres, y ética locales. Lista de leyes, costumbres, y ética operativas.

Identificado [ ]

Verificable [X]

No Aplicable [ ]

**Anexo 2:** Encuesta para verificar el cumplimiento de las políticas internas.

**UNIVERSIDAD TÉCNICA DE AMBATO**
**FACULTAD DE TECNOLOGÍAS DE LA INFORMACIÓN, TELECOMUNICACIONES E INDUSTRIAL**
**INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS**

**Objetivo:** Analizar el cumplimiento de las políticas internas de seguridad de la Fundación cultural y educativa Ambato (UNIDAD EDUCATIVA ATENAS).

**Instructivo:** Seleccione con una X una de las opciones que usted considere conveniente en cada pregunta.

**Políticas de seguridad en correo electrónico**

**44. ¿El personal de la institución ha intentado atentar a la integridad de la misma por medio del uso indebido del correo electrónico?**

SI [X]
NO [ ]

**45. ¿El personal divulga información que incite a la discriminación o a la violencia?**

SI [X]
NO [ ]

**46. ¿Se ha enviado contenido con fines publicitarios y comerciales de bienes y servicios en beneficio propio, sin la autorización pertinente?**

SI [ ]
NO [X]

**47. ¿Se ha usado el correo institucional para él envió de SPAM, por parte del personal?**

SI [X]
NO [ ]

**48. ¿Se ha enviado correos masivos de cuentas personales, sin autorización del rectorado?**

SI [X]

NO [ ]

**49. ¿Se ha registrado casos donde el personal ha utilizado la cuenta de otro usuario o ha facilitado sus contraseñas propias a terceros?**

SI [X]

NO [ ]

**50. ¿El personal de la institución ha falsificado mensajes de correo electrónico?**

SI [ ]

NO [X]

**51. ¿Se ha dado casos donde el personal de la institución lee, copia, borra o modifica mensajes de correo electrónico de otras personas, sin autorización previa?**

SI [ ]

NO [X]

**52. ¿Ha comprobado que el personal inicia o continua con cadenas de mensajes los cuales congestionan innecesariamente la red?**

SI [X]

NO [ ]

**53. ¿Los recursos de computación son usados exclusivamente con propósitos educativos?**

SI [ ]

NO [X]

**54. ¿La unidad educativa entrega un equipo de cómputo en perfecto funcionamiento con lo necesario para la actividad del usuario?**

SI [X]

NO [ ]

**55. ¿Se reporta a Sistemas por medio correo electrónico cualquier tipo de daño en los equipos?**

SI [X]

NO [ ]

**56. ¿El departamento de sistemas realiza revisiones sin previo aviso del usuario: el tráfico de internet, software instalado, y la información almacenada en cada una de ellos, verificando el cumplimiento de las políticas de seguridad y aplicando las consecuencias que corresponda?**

SI [X]

NO [ ]

**57. ¿El personal de la institución cumple con las normas internas establecidas para el correcto uso de las computadoras?**

SI [X]

NO [ ]

**58. ¿El departamento de sistemas lleva un control de todo el software que están instalado en las computadoras?**

SI [X]

NO [ ]

**59. ¿Se ha producido alguna intervención en las redes de cableado por parte del personal de la institución?**

SI [ ]

NO [X]

**60. ¿Existe el previo registro de las direcciones Mac para el uso del internet en pc personales y celulares?**

SI [X]

NO [ ]

**61. ¿Considera usted que cada usuario es responsable del buen uso de su computador institucional, personal o celular?**

SI [X]

NO [ ]

**62. ¿Existe el bloque respectivo de páginas con contenido para adultos?**

SI [X]

NO [ ]

**63. ¿El departamento de sistemas realiza el bloqueo respectivo de las redes sociales para evitar el uso del chat?**

SI [X]

NO [ ]

**64. ¿El personal de la institución realiza la petición para descargar música?**

SI [X]

NO [ ]

**65. ¿Sistemas lleva un control para evitar que los usuarios no descarguen aplicaciones que permitan escuchar radio o ver televisión por internet, así como también realizar llamadas nacionales, locales o internacionales por medio del internet?**

SI [X]

NO [ ]

**66. ¿Sistemas realiza la suspensión de internet de un equipo donde se detecte un mal uso del internet?**

SI [X]

NO [ ]

**Anexo 3:** Aprobación para escaneo a los servidores de la institución.

Ambato, 12 de Septiembre del 2019

Señor
Marcelo Velasco
**EGRESADO UNIVERSIDAD TÉCNICA DE AMBATO**
Ciudad

De mi consideración:

Yo, **Manuel Fierro** en calidad de Rector de la **UNIDAD EDUCATIVA ATENAS - FUNDACIÓN CULTURAL Y EDUCATIVA AMBATO** le autorizo a realizar el escaneo y ataque de los servidores de la UNIDAD EDUCATIVA ATENAS, supervisado por el Analista de Sistemas 1 - Juan Carlos Calvache Paredes, durante los días 13 al 27 de septiembre de 2019, a partir de las 14h00.

Es importante mencionar **UNIDAD EDUCATIVA ATENAS - FUNDACIÓN CULTURAL Y EDUCATIVA AMBATO** solicita que la todos los datos obtenidos en este proyecto de titulación se manejen con confidencialidad.

Saludos cordiales,

Manuel Fierro
**RECTOR**

C.I.: 1802274892
mfierro@atenas.edu.ec

Juan Calvache
**ANALISTA DE SISTEMAS 1**

C.I.:1804339008
jcalvache@atenas.edu.ec

**Anexo 4:** Solicitud para escaneo a los servidores de la institución.

Ambato, 13 de Septiembre del 2019

Sr. Dr.

Manuel Fierro
RECTOR UNIDAD EDUCATIVA ATENAS

Presente

De mi consideración:

Yo, Marcelo David Velasco Trujillo, con cedula de ciudadanía Nº 1804874079, egresado de la Carrera de Ingeniería en Sistemas Computacionales e Informática de la Facultad de Ingeniería en Sistemas Computacionales Electrónica e Industrial, solicito se me autorice con fecha y hora para realizar el escaneo y ataque de los servidores de la Fundación Cultural y Educativa Ambato(UNIDAD EDUCATIVA ATENAS), como parte de mi trabajo de titulación "Análisis de riesgos informáticos aplicando la metodología OSSTMM para la Fundación Cultural y Educativa Ambato (Unidad Educativa Atenas)" ,es necesario el escaneo para verificar vulnerabilidades en los mismo. Además se procederá a realizar un ataque de ingeniería social el cual se coordinará con el departamento de sistemas.

El escaneo de los servidores será supervisado por el Analista de Sistemas 1, Juan Carlos Calvache Paredes.

Por la favorable que se le dé al presente, agradezco y suscribo.

Atentamente.

Marcelo Velasco

1804874079

0963033420-0990018283

david1mtv@gmail.com

## GLOSARIO Y ACRÓNIMOS

**OSSTMM:** Metodología Abierta de Comprobación de la seguridad (Open Source Security Testing Methodology) un estándar usado para la Auditoria de Seguridad por ser una metodología completa, usada en su mayoría para el testeo

**EIGRP: (**Enhanced Interior Gateway Routing Protocol) Protocolo de encaminamiento de vector distancia.

**OSPF:** Open Shortest Path First, Abrir el camino más corto primero es un protolo de encamiento el cual usa el algoritmo de Dijkstra, el cual selecciona el major camino.

**NMAP:** Es un programa de código abierto el cual orincipalmente ayuda a la detección de puertos abiertos y detectar vulnerabilidades, originario de Gordon Lyon (más conocido por su alias Fyodor Vaskovich y cuyo desarrollo se encuentra hoy a cargo de una comunidad), desarrollada para Linux pero en la actualidad existe versiones multiplataforma.

**NESSUS:** Es un programa el cual nos ayuda a la detección de vulnerabilidades multiplataforma en el cual se puede especificar el tipo de ataque y nos brinda el estado del escáner.

**BONJOUR:** Software de Apple que usa paquetes DNS sobre IP.

**PTES:** The Penetration Testing Execution Standard

**OWASP:** The Open Web Application Security Project

**SIEM:** Security information and event management

**PHISHING:** Termino informático usado para identificar un intento de suplantación de información para obtener información de forma fraudulenta.