UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ
EXTENSIÓN EN EL CARMEN
CARRERA DE INGENIERÍA EN SISTEMAS
Creada Ley No. 10 – Registro Oficial 313 de Noviembre 13 de 1985

TRABAJO DE INVESTIGACIÓN

PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS

ANÁLISIS DE SEGURIDAD MEDIANTE METODOLOGÍA OWASP A REDES INALÁMBRICAS EN "UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ EXTENSIÓN EN EL CARMEN"

JONATHAN MOISÉS DELGADO BASURTO
AUTOR

RENELMO WLADIMIR MINAYA MACÍAS Mg. Sc.
TUTOR

EL CARMEN, ENERO DE 2020

DECLARACIÓN DE AUTORÍA

Quien suscribe **JONATHAN MOISÉS DELGADO BASURTO** C.I. N° **131366349-2,** hace constar que es el autor de la Tesis Titulada: **Análisis de seguridad mediante metodología OWASP a redes inalámbricas en "Universidad Laica Eloy Alfaro de Manabí Extensión en El Carmen",** el cual constituye una elaboración personal realizada únicamente con la dirección del asesor de dicho trabajo, A.S. Renelmo Wladimir Minaya Macías, Mg.

En tal sentido, manifiesto la originalidad de la Conceptualización del trabajo, interpretación de datos y la elaboración de las conclusiones, dejando establecido que aquellos aportes intelectuales de otros autores se han referenciado debidamente en el texto de dicho trabajo.

_____

Jonathan Delgado Basurto
C.I. 131366349-2

CERTIFICACIÓN

En calidad de docente tutor de la Facultad de la Carrera de Ingeniería en Sistemas de la Universidad Laica "Eloy Alfaro" de Manabí, certifico:

Haber dirigido y revisado el trabajo de titulación, cumpliendo el total de 400 horas, bajo la modalidad de proyecto de investigación, cuyo tema del proyecto es "**ANÁLISIS DE SEGURIDAD MEDIANTE METODOOGÍA OWASP A REDES INALÁMBRICAS "EN UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ EXTENSIÓN EN EL CARMEN**", el mismo que ha sido desarrollado de acuerdo a los lineamientos internos de la modalidad en mención y en apego al cumplimiento de los requisitos exigidos por el Reglamento de Régimen Académico, por tal motivo CERTIFICO, que el mencionado proyecto reúne los méritos académicos, científicos y formales, suficientes para ser sometido a la evaluación del tribunal de titulación que designe la autoridad competente.

La autoría del tema desarrollado, corresponde al señor **DELGADO BASURTO JONATHAN MOISÉS,** estudiante de la carrera de Ingeniería en Sistemas, período académico 2019-2, quien se encuentra apto para la sustentación de su trabajo de titulación.

Particular que certifico para los fines consiguientes, salvo disposición de Ley en contrario.

El Carmen, 16 de enero de 2020.

Lo certifico,

A.S. Wladimir Minaya Macías, Mg. SC
Docente Tutor
Área: Tecnología de la información

DEDICATORIA

Este trabajo se lo dedico a todas aquellas personas que fueron mi inspiración y de alguna forma u otra aportaron ese granito de arena para que esto funcionara. A esos angelitos que Dios pone en mi camino y fueron fuente de inspiración para seguir creciendo como profesional, familia, enamorada, amigos, entre otros.

Este trabajo investigativo además de todas las personas que he mencionado, se lo dedico a Dios.

Gracias por estar siempre junto a mí.

Jonathan Moisés.

AGRADECIMIENTO

A Dios. Por la vida, la sabiduría, la inteligencia y las ganas de seguir adelante cada día cumpliendo sueños.

A mis Padres. Miguel y Carmen por el apoyo incondicional en este arduo camino de preparación, por el ejemplo de trabajo y honradez.

A mi tutor. AS. Wladimir Minaya infinitas gracias por guiarme en este proceso de titulación, sus conocimientos y enseñanzas fueron parte fundamental para lograr este objetivo.

A mis docentes. Mis más sinceros agradecimientos a cada uno de ustedes ya que forman parte de mi vida profesional compartiéndome sus conocimientos e instruyéndome cada vez que lo necesitaba, Ing. Andrea, AS. Soraida, Ing. Clarita, AS. Wladimir, Ing. Danilo, Ing. Sergio.

A toda mi familia. Por estar siempre presentes con sus buenos deseos y consejos que sirvieron de mucho.

Al amor de mi vida.

A mis amigos. Porque formamos un grupo de trabajo muy unido que perduró hasta el final Jéssica, Liliana, Ovidio y Yo.

Jonathan Moisés.

ÍNDICE GENERAL

ÍNDICE DE CUADROS

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE ANEXOS

RESUMEN

En este apartado se da a conocer el trabajo de titulación que tuvo como base realizar un Análisis de seguridad mediante metodología OWASP a redes inalámbricas en “Universidad Laica Eloy Alfaro de Manabí Extensión en El Carmen”.

Para cumplir con el objetivo establecido en el análisis de seguridad se ha determinado tareas científicas que permitieron cumplir con el proceso de evaluación a las aplicaciones web y las redes inalámbricas de uso frecuente en la universidad, con la finalidad de escanear posibles vulnerabilidades que puedan existir en cada una de ellas, para ello se empleará el uso de la metodología OWASP que permite identificar riesgos a los que se encuentran expuestos en la web además de herramientas como Nessus que examinan las redes Wifi y los puertos de conexión a internet.

Para llevar a cabo cada una de estas acciones y verificar su cumplimiento se aplicaron los métodos deductivos e inductivo; la metodología OWASP es la encargada de analizar las posibles vulnerabilidades que se puedan encontrar, ya que está enfocada en verificar la seguridad de las aplicaciones web en tiempo real y los riesgos a las que se exponen los sitios de internet además es un método formal para identificar la inseguridad a los que se exponen, la herramienta Nessus se implementa para verificar las seguridades de las redes inalámbricas y sus puertos de internet, además de encontrar las vulnerabilidades recomienda las posibles soluciones y las medidas apropiadas a los problemas encontrados.

Los resultados de relevancia que se presentaron en esta investigación fueron los análisis de seguridad en contraseñas que arrojaron en sus informes algunos inconvenientes, el más común de todas contraseñas débiles que los usuarios utilizan en sus sitios web. En los ataques llevados a cabo fueron bloqueados satisfactoriamente por los protocolos de seguridad que rigen en la universidad.

SUMMARY

In this section, the titling work that was based on conducting a security analysis through OWASP methodology to wireless networks in “Lay University Eloy Alfaro de Manabí Extension in El Carmen” is disclosed.

In order to fulfill the objective established in the security analysis, scientific tasks have been determined that allowed us to comply with the evaluation process for web applications and wireless networks frequently used in the university, in order to scan possible vulnerabilities that may exist in each of them, for this purpose the use of the OWASP methodology will be used, which allows identifying risks to which they are exposed on the web, as well as tools such as Nessus that examine Wi-Fi networks and internet connection ports.

To carry out each of these actions and verify compliance, deductive and inductive methods were applied; The OWASP methodology is in charge of analyzing the possible vulnerabilities that can be found, since it is focused on verifying the security of web applications in real time and the risks to which the Internet sites are exposed. It is also a formal method to identify The insecurity to which they are exposed, the Nessus tool is implemented to verify the security of wireless networks and their internet ports, in addition to finding vulnerabilities, it recommends possible solutions and appropriate measures to the problems encountered.

The results of relevance that were presented in this investigation were the security analyzes in passwords that threw in their reports some inconveniences, the most common of all weak passwords that users use in their websites. In the attacks carried out they were successfully blocked by the security protocols that govern the university.

INTRODUCCIÓN

En su gran mayoría las actividades realizadas en la vida diaria de los países en desarrollo como también los desarrollados tienden a depender de sistemas y redes informáticas debido al crecimiento del internet y las herramientas que ofrece para facilitar el trabajo dentro de las organizaciones y la estructuración sistemática de sus operaciones. (Gómez Vieites, 2011)

De ahí nace la importancia de contar con medidas de seguridad para proteger el sistema del cual depende la organización, teniendo en cuenta que se debe tener presente impedir la ejecución de operaciones no hayan sido autorizadas y que puedan causar efectos en la integridad de la información que se almacene en sus servidores.

La seguridad informática ha sido un dolor de cabeza a lo largo de los años en todo el mundo, es por eso que en los diferentes lugares del planeta se implementan medidas de seguridad para salvaguardar la información dentro de las organizaciones e impedir que los determinados hackers materialicen ataques con fines maliciosos. Existen métodos de seguridad informática que le permiten a las empresas contar con herramientas para controlar acceso no autorizado a su sistema de información, identificando los puntos de acceso vulnerables donde podrían correr peligro en caso de infringir las normas que protegen a mencionado sistema.

Es el caso de la metodología OWASP cuyo objetivo es brindar seguridad en el acceso a páginas web mediante el uso de una red inalámbrica, es aquella que centra sus funciones en realizar auditorías webs con la finalidad de analizar y evaluar los riesgos ocasionados por personas malintencionadas, el propósito de esta metodología es revisar la plataforma a la cual se vaya a ingresar verificando la autenticidad, vectores de ataques, los fallos de seguridad y que al momento de escribir contraseñas y usuarios estos no sean capturados y redirigidos a sitios emergentes de similares características que la original.

Para este problema se ha planteado el objetivo de analizar la seguridad de las redes inalámbricas existentes en la Universidad Laica Eloy Alfaro de Manabí Extensión en El Carmen mediante la metodología OWASP, para cumplir este

propósito se han propuesto un conjunto de tareas científicas que permitieron conocer el resultado del análisis.

- Fundamentar teóricamente la metodología OWASP y las redes inalámbricas mediante bibliografía actualizada.
- Recopilar información acerca de las vulnerabilidades a las que se exponen las redes inalámbricas.
- Aplicar la metodología OWASP para el estudio de la seguridad en las redes inalámbricas.
- Realizar presentación de resultados con los casos encontrados dentro del estudio realizado.

Cada una de las acciones antes mencionadas se han podido realizar mediante métodos y técnicas de investigación como la de campo, la encuesta y la observación, las cuales permitieron obtener información directamente facilitada por los estudiantes de la universidad acerca de la seguridad en las redes inalámbricas. La población que se ha estimado como base para la presente investigación se ha considerado al conjunto de estudiantes de la planta central de la universidad (978 estudiantes) excluyendo a la carrera de Ingeniería Agropecuaria los cuales usan las redes inalámbricas objeto de este trabajo investigativo. La muestra a quien se aplicará el estudio se ha considerado a la totalidad de docentes al ser una cantidad pequeña, y el caso de los estudiantes mediante la fórmula muestral donde se obtuvo un total de 76 estudiantes como muestra, mismos que serán objeto del presente estudio. Cada uno de los resultados obtenidos mediante los diferentes métodos investigativos fueron analizados posteriormente.

Esta investigación se la detalla de la siguiente manera.

El capítulo uno está compuesto por todo el soporte teórico de la variable independiente y la variable dependiente la cual permite conocer la metodología seleccionada, la forma de como implementarla y los beneficios que provee en cuanto a seguridad en el acceso a los sitios web. El capítulo dos está constituido por información que se ha recolectado en el campo de estudio, obteniendo resultados en diagnósticos, entrevistas y observaciones como también de la

técnica de la observación. Mientras que en el capítulo tres lo componen la parte fundamental de la auditoria informática, ya que es aquí donde se aplicaron los instrumentos de seguridad basados en la metodología OWASP, también se puede citar en este apartado a la herramienta Nessus con la cual realizó análisis a las redes inalámbricas

Con el estudio de la metodología OWASP se pretendió verificar que las redes inalámbricas existentes en ULEAM Extensión en El Carmen cumplan con los protocolos de seguridad adecuada para el proceso de traslado de información y que no representen riesgos para las personas que las utilizan sean estos docentes, estudiantes y directivos.

CAPITULO I

1 MARCO TEÓRICO

1.1 Metodología OWASP

La metodología OWASP (Open Web Application Security Project) es aquella que centra sus funciones en las aplicaciones web y las seguridades que estas presentan para resguardar su integridad, la misión planteada por esta metodología de análisis es la de asistir a organizaciones en la toma de decisiones evidenciando las vulnerabilidades y riesgos que puedan existir. (Benchimol, 2012)

Metodología OWASP es una herramienta de reporte que se utiliza en las organizaciones para informar sobre las amenazas y posibles riesgos que tienden a presentarse en páginas web de mayor concurrencia en la empresa, la cual detecta incidentes ajenos al uso habitual e informa sobre lo acontecido. (Rault, y otros, 2015)

La metodología OWASP presenta un plan de ejecución ordenado que recorre las distintas áreas vulnerables de forma sistemática de una aplicación web, analizando las posibilidades que tiene una organización de ser victimada cibernéticamente, lo cual manifiesta una guía que el especialista en informática puede utilizar al momento de auditar los vectores de ataques y los fallos de seguridad.

Los autores antes mencionados hacen referencias similares a la definición y utilidad acerca de la metodología OWAP y su función dentro de una organización, cabe recalcar que es una herramienta de análisis de uso gratuito que se centra en mejorar la seguridad de las aplicaciones web debido a que los ciberataques utilizan diferentes rutas en los que se pueden materializar y causar pérdidas cuantiosas a las organizaciones.

1.1.1 Top 10 vulnerabilidades más comunes.

La funcionalidad de OWASP permite recolectar información y realizar un informe sobre un conjunto de vulnerabilidades presentes en las aplicaciones web, el cual podemos emplearlo al momento de analizar la seguridad web en la organización. Adicional provee una gama de herramientas de detección y consejos sobre las

soluciones que se pueden ejecutar para resolver las inseguridades encontradas, entre las más comunes se presentan a continuación: (OWASP, 2013)

A. **Inyección.**

   Este tipo de amenaza es producida por un atacante externo que envía datos de forma anónima y poco confiable adjuntos a una petición o comando a ejecutar en bases de datos o en el mismo sistema operativo con la finalidad de apoderarse de información. Un claro ejemplo de este ataque es SQL Injection. (OWASP, 2013)

B. **Ruptura de la atenuación y gestión de sesiones.**

   Son ataques relacionados con el control de acceso o inicio de sesión que tienden a dejar vulnerables sitios de privacidad al momento de realizar una tarea o petición a un intérprete, obteniendo credenciales de usuario y permisos que el mismo puede poseer. (OWASP, 2013)

C. **Secuencia de comandos en sitios cruzados (XSS).**

   La forma de materializar este tipo de ataque se relaciona directamente con el navegador web predeterminado adjuntos en páginas emergentes que descargan datos pocos confiables y permitiendo la instalación de programas maliciosos. (OWASP, 2013)

D. **Referencia directa insegura a objetos.**

   Este tipo de ataques tienen su origen en la inadecuada administración de seguridad llevada a cabo por un usuario realizando tareas o peticiones sobre las cuales no bebería tener acceso ni recursos dentro de un sistema de información. (OWASP, 2013)

E. **Configuración de seguridad incorrecta.**

   Las configuraciones inadecuadas o incorrectas son el principal inconveniente que enfrentan las aplicaciones web en cuanto a seguridad se refiere. Debe existir una amplia gama de filtros que complementen y resguarden los servidores donde se aloja la información de las aplicaciones, en las bases de datos y en el mismo sistema operativo. (OWASP, 2013)

F. **Exposición de datos sensibles.**

   Los datos son la parte de mayor importancia dentro de una organización y si no se toman las medidas de control adecuadas se correrán grandes

riesgos de perder de información. Este tipo de ataques tienden a llevarse a cabo cuando se accede fácilmente a la información almacenada de las aplicaciones web, es decir alojamiento de contraseñas en la red sin medidas de cifrado alguna y establecer contacto con el servidor de forma insegura. (OWASP, 2013)

G. Ausencia de control de acceso a funciones.

Al momento de realizar tareas en el servidor a un usuario se le otorgan permisos de funcionamiento sobre las cuales realizar su función, estos ataques llevados a cabo por personal malicioso suelen ser identificados por tratar de acceder o tomar atribuciones en el servidor a las cuales no debería tener acceso y realizar cambios en la información como también apoderarse de ella. (OWASP, 2013)

H. Falsificación de peticiones en sitios cruzados.

Son acciones realizadas dentro de un ordenador que ejecutan acciones HTTP falsificadas o clonadas por un atacante aplicado a una página web con vulnerabilidades significativas. (OWASP, 2013)

I. Utilización de componentes con vulnerabilidades conocidas.

Los ataques que ocurren en esta sección son debido a la utilidad de aplicaciones que contienen vulnerabilidades como antivirus, framewokrs entre otras, que se utilizan para la seguridad, es importante indagar en las actualizaciones disponibles ya que la implementación de estas medidas dependerá de las mejoras implementadas en su historial de seguridad. (OWASP, 2013)

J. Redirecciones y reenvíos validados.

Los ataques que se materializan en este apartado tienen su fundamento en las páginas web frecuentadas con mayor regularidad, al momento de establecer contacto con otras aplicaciones no se tiene la certeza de la veracidad del sitio de destino. La principal vulnerabilidad de la misma son ventanas emergentes estéticamente idénticas a la original cuya función es capturar credenciales de usuarios para cometer delitos informáticos. (OWASP, 2013)

1.1.2 Seguridad.

Según Aguilera López (2010), explica que la seguridad de los sistemas informáticos es una disciplina compuesta por normas de protección, métodos y técnicas orientados a salvaguardar la integridad de los sistemas de información existentes en una organización.

Un sistema de información al mantenerse conectado a la red tiende a exponerse en riesgo por los múltiples ataques que realizan los hackers, no obstante, se debe conocer qué medidas de seguridad se podría implementar para proteger un sistema y para ello se debe tener conocimiento sobre lo siguiente:

- Cuantos y cuáles son los elementos que conforman el sistema, información que se puede obtener con el administrador o responsable del mismo.
- A que peligros se expone o están afectando al sistema ya sean estos provocados o accidentalmente alojados dentro del sistema de información, acción que se puede realizar con pruebas directas en busca de fallos.
- Qué tipo de medidas de seguridad estaría dispuesto a implementar para reducir riesgos al máximo posible dentro del sistema de información.

Una vez establecidas las medidas de seguridad a implementar se debe realizar un seguimiento periódico con el fin de monitorear el cumplimiento de las medidas adoptadas. A continuación, se mencionan los tipos de seguridad de mayor recurrencia

1.1.2.1 Tipos de seguridad.

1.1.2.1.1 Activa.

La seguridad activa es aquella que está compuesta por un conjunto de normas o medidas de defensa que tienen como objetivo primordial la reducción de los constantes riesgos que afectan a un sistema de información. Con la implementación de esta medida se pretende impedir el acceso a información confidencial a usuarios no autorizados. (Aguilera López , 2010)

1.1.2.1.2 Pasiva.

Es aquella que tiene la finalidad de facilitar la recuperación del sistema después de estar expuesto a ataques y presentar perdidas de información, además de minimizar el riesgo acontecido en el sistema. (Aguilera López , 2010)

1.1.3 Análisis de riesgos

El autor Baca Urbina (2016), describe que el análisis de riesgos es una de las pautas con mayor importancia dentro de un sistema de información ya que da la posibilidad del estudio de vulnerabilidades o puntos débiles dentro de los componentes del sistema. El estudio de vulnerabilidades se lo realiza con la finalidad de no permitir el acceso a información importante de una organización.

En el texto de Aguilera López (2010), explica que el análisis de riesgo conlleva al estudio de las vulnerabilidades que tiene un sistema de información teniendo en cuenta cada elemento que lo conforma y ante algunas determinadas amenazas estimar el nivel de pérdidas que dejaría un ataque sorpresa sobre todo el sistema. Acto siguiente se mencionan algunos elementos de estudio considerados en esta investigación.

1.1.3.1 Elementos de estudio.

Cuando se aplica un análisis de riesgos dentro de un sistema de información hay que tener en cuenta varios puntos de acceso débiles a los cuales se pretende otorgar con medidas de protección, tales como:

1.1.3.2 Activos.

Los activos son aquellos que permiten o hacen posible el funcionamiento de un sistema de información dentro de una empresa como son: los datos, software, hardware, las redes, instalaciones y personal. (Aguilera López , 2010)

1.1.3.3 Amenazas.

Aguilera López (2010) menciona que, Las amenazas presentes en un sistema de información son aquellas alojadas en el propio sistema esperando el momento adecuado para cometer un ataque a la información almacenada y perteneciente a una organización. Dichas amenazas pueden ser de índole accidental o intencionada.

1.1.3.4 Riesgos.

El riesgo se considera como una posibilidad que las amenazas presentes en un sistema se materialicen o no mediante la apertura de una vulnerabilidad ya que se emplean de estas para producir un ataque. (Aguilera López , 2010)

1.1.3.5 Vulnerabilidades.

Según Aguilera López (2010), Una vulnerabilidad es la puerta de acceso que tienen los hackers para materializar un ataque dentro de los activos de un sistema de información. Cabe recalcar que los activos no son vulnerables a la misma amenaza.

1.1.4 Análisis interior.

Romero Castro & Figueroa Morán (2018) indican que, El análisis interior es aquel que demuestra que acciones se pueden realizar con los privilegios que un usuario posee dentro de la organización, para poder sobrellevar este tipo de análisis en una empresa, esta debe proveer a sus empleados con una computadora con acceso al sistema de información como también de un usuario y contraseña de acceso con la finalidad de llevar a cabo una observación y control sobre las actividades que este usuario realice en la integridad de la información almacenada. El análisis interior es un tipo de test que realiza un conjunto de pruebas las cuales se describen a continuación:

1.1.4.1 La revisión de la privacidad.

Trata de verificar cual es el manejo que un usuario de la organización realiza con la información almacenada desde el punto de vista legal y ético en su día a día. (Romero Castro & Figueroa Morán, 2018)

1.1.4.2 Testeo de aplicaciones de internet.

Tiene como tarea encontrar fallas en las aplicaciones web que utiliza el sistema de información y la empresa, específicamente fallas de seguridad ya que al estar conectados en red tienden estar expuestos a ataques. (Romero Castro & Figueroa Morán, 2018)

1.1.4.3 Testeo de sistema de detección de intrusos.

Tiene la función de escanear la presencia de intrusos en los sistemas de información, normalmente se enfoca en el estudio del rendimiento de la red que mantiene en comunicación a los usuarios con el sistema. (Romero Castro & Figueroa Morán, 2018)

1.1.4.4 Testeo de medidas de contingencia.

Este análisis se lo realiza con la finalidad de comprobar el funcionamiento y cumplimiento de los estándares de seguridad seleccionados, como también monitorea los intentos de acceder a los recursos protegidos de una organización. (Romero Castro & Figueroa Morán, 2018)

1.1.4.5 Descifrado de contraseña.

Tiene la función de probar la seguridad de las contraseñas empleadas en el sistema de información además de validar los sistemas de recuperación de manera automática mediante criptografías. (Romero Castro & Figueroa Morán, 2018)

1.1.4.6 Testeo de denegación de servicios.

Es aquel que se encarga de la suspensión de acceso temporal o definitivo a usuarios reales o ficticios ya sea en circunstancias accidentales o de manera intencional que se presenten como amenaza al sistema de información.

1.1.5 Análisis exterior.

Romero Castro & Figueroa Morán (2018), Este tipo de análisis basa su funcionamiento en la manera de acceder remotamente a los servidores de una organización con el objetivo de bloquear o eliminar aquellos usuarios ilegales que tengan asignados privilegios o permisos que no deberían existir o estar en funcionamiento dentro de la empresa. La aplicación del test de análisis exterior se lo puede realizar con la implementación de técnicas para la recolección de información con la ingeniería social y después utilizar dichos datos en posibles intentos de ataques o accesos no registrados a los servidores. El análisis exterior tiene como base los siguientes puntos:

1.1.5.1 Revisión de la inteligencia competitiva.

Hace referencia a la participación activa de una organización en el internet a través del cual se puede recolectar información necesaria y alojarla en sus servidores.

1.1.5.2 Revisión de la privacidad.

Tiene como objetivo brindar apoyo en el almacenamiento de información personal de un cliente basado en el punto de vista ético y legal que asegura la

integridad de los datos almacenados sin el riesgo de ser publicadas por terceras personas. Es decir, una empresa controla que la información almacenada y que circula por toda la red no sea utilizada por personas ajenas a la organización e incluso que un colaborador de la misma pueda sacar información y llevársela a casa.

1.1.5.3 Análisis de sugerencia dirigida.

Este análisis intenta descubrir aquellos atacantes que cuentan con ayuda directa de algún colaborador de la empresa como también se dirige al bloqueo de aplicaciones emergentes que deseen aplicar cambios en la integridad de la información a través de virus, es decir, que se instalen herramientas por parte de algún cómplice o mediante descarga que les facilite a los atacantes tener el acceso a los servidores donde se aloja la información. Este método de ataque se lo puede realizar de la manera antes mencionada como también se lo puede realizar con el envío de correos electrónicos falsos que infesten de virus maliciosos a la red de comunicación. (Romero Castro & Figueroa Morán, 2018)

1.1.6 Control de riesgos.

Aguilera López (2010), menciona que el control de riesgos tiene como propósito el estudio del cumplimiento de las medidas de seguridad empleadas en la protección de un sistema de información además de medir la efectividad que proveen los mecanismos de seguridad correspondientes a cada activo. Los servicios de seguridad de mayor utilidad se mencionan a continuación.

1.1.6.1 Servicios de seguridad.

1.1.6.1.1 Integridad.

Aguilera López (2010) explica que la integridad, Es aquel que tiene la función de asegurar que la información existente en una organización no presente modificaciones en su estructura realizada por personas ajenas o no autorizadas en la empresa.

1.1.6.1.2 Confidencialidad.

Es un servicio que se ofrece a las organizaciones en el control de riesgos ya que proporciona seguridad en contra de la revelación intencionada o de manera accidental de información personal. (Aguilera López , 2010)

1.1.6.1.3 Disponibilidad.

Permite la utilidad de la información desde cualquier lugar donde se encuentre o sea requerida con la previa autorización de las entidades encargadas u organizaciones a la que pertenezcan los datos. (Aguilera López , 2010)

1.1.6.1.4 Mecanismos de seguridad.

Son aquellos que se aplican en el control de riesgos para proteger la integridad de la información los cuales pueden clasificarse de la siguiente manera:

1.1.6.1.5 Preventivos.

Aguilera López (2010), Es aquel que se mantiene latente dentro de un sistema de información escaneando posibles ataques con la finalidad de evitarlo es decir actúan antes que se produzca el ataque.

1.1.6.1.6 Detectores.

Es aquel que emplea su funcionamiento después que un ataque se lleve a cabo dentro del sistema con el objetivo de prevenir daños severos en la funcionalidad del sistema. (Aguilera López , 2010)

1.1.6.1.7 Correctores.

Como indica Aguilera López (2010), son aquellos que se emplean para corregir los daños causados por ataques en el sistema de información es decir actúa después que un ataque se materialice y encuentre daños significantes en el sistema.

1.1.7 Definición y tipos de seguridad.

La seguridad en informática es una disciplina que toma como base las políticas de una empresa a través de las normas externas e internas, su función principal es la de precautelar la seguridad, privacidad e integridad de información relevante que se almacena en un sistema de información contra las constantes amenazas a las que se expone al mantenerse conectada a internet, tratando de minimizar riesgos físicos y lógicos. (Baca Urbina, 2016)

Los mecanismos de seguridad que se van a implementar para proteger un sistema de información tienden a depender de las características del mismo, de

su función y lo principal al riesgo que se expone de manera directa. También tiene la potestad de recuperar información robada o dañada mediante un ataque.

1.1.7.1 La atenuación.

Tiene su aplicación en el control de acceso verificando la autenticidad e identidad de los usuarios que acceden a la información por medio de la red. Esta acción se la realiza con la finalidad de que las transacciones realizadas contengan datos reales y que no traten de suplantar usuarios verdaderos. (Aguilera López , 2010)

1.1.7.2 No repudio.

Es la acción que le permite a los sistemas tener la capacidad de prevención ante la negación de un usuario sobre las operaciones realizadas con los datos dentro de una organización. Gracias al avance tecnológico la seguridad informática adjunta pruebas irrefutables que demuestran las acciones realizadas por un usuario con los datos, tales como el envío y recepción, la modificación y eliminación. (Aguilera López , 2010)

1.1.7.3 Características que debe poseer la información protegida.

1.1.7.3.1 Efectividad.

Es aquella que demuestra la importancia de la información para una organización al momento de llevar a cabo una tarea además de mantener fácil acceso, veracidad en su estructura, consistente y accesible. (Baca Urbina, 2016)

1.1.7.3.2 Confidencialidad.

Protección de accesos no autorizados al sistema de información que puedan generar perdidas, alteración y robos datos. (Baca Urbina, 2016)

1.1.7.3.3 Integridad.

Asegura que la información enviada por la red llegue a su destino completa y sin alteraciones en su contenido. (Baca Urbina, 2016)

1.1.8 Seguridad lógica.

Aguilera López (2010), mencionó que la seguridad lógica es aquella que mediante el empleo de software tiene la ardua tarea de proteger la información de manera digital directamente por medio del empleo de herramientas o mecanismos de seguridad.

Entre las herramientas con mayor utilidad para realizar dichas acciones son las siguientes:

1.1.8.1 Control de acceso.

Es aquel que por medio de usuarios y contraseñas se restringe el acceso a la información por parte de personal no autorizado dentro de la organización.

1.1.8.2 Cifrado de datos.

El cifrado de datos no es más que la encriptación de la información que circula por la red entre un emisor y un receptor, para realizar esta acción se enmascaran los datos a circular con claves especiales implementadas por sistemas de encriptación donde solo los integrantes del envío tienen conocimiento de dichas claves. Esta medida de seguridad se lo realiza con el fin de proteger la confidencialidad e integridad de la información enviada. (Aguilera López , 2010)

1.1.8.3 Antivirus.

Son muy comunes en sistemas de información ya que se mantienen latentes impidiendo el ingreso y propagación de virus o software malicioso. Por otra parte, ofrece la opción de eliminarlos y corregir los daños causados por la infección de los mismos. (Marroquín, 2010)

1.1.8.4 Cortafuegos.

Los cortafuegos son sistemas de seguridad de hardware y software que tienden a evitar el acceso no autorizado a un sistema de información con la finalidad de precautelar la información almacenada, es necesario mencionar que un cortafuego no elimina los virus de un ordenador, solo sirve como escudo para que no acceda a los dotas almacenados. (Cabello García, 2014)

1.1.8.5 Certificados digitales.

Son un tipo de documentos que se aplican en la verificación de accesos a los sistemas de información mediante el usuario y contraseña, garantiza que dicho intento de acceso sea efectuado por el usuario correcto y autorizado por la organización. (Aguilera López , 2010)

1.1.9 Seguridad física.

La seguridad física es aquella que tiende a la aplicación de barreas y procedimientos de control cuyo objetivo es la protección a los peligros físicos que se exponen los componentes de un sistema de información. (Costas Santos, 2011)

La seguridad informática tiene como prioridad brindar protección a cada uno de los mecanismos informáticos que componen un sistema de información, aplicando medidas de control como barreras físicas para reducir amenazas que pueden ser provocadas por el hombre, accidental o voluntaria. (Alegre Ramos, García , & Hurtado, 2011)

Como lo mencionan los autores anteriormente citados la seguridad física tiende a activar un plan de contingencia ante problemas físicos como: las inundaciones que se presentan en épocas de lluvia, también tienen participación los incendios que se pueden generar por desperfectos de la energía eléctrica, se incluyen en estos factores también los terremotos ya que a causas de colisión de las instalaciones físicas y por último la consecuencia más suscitada es el robo de equipos computacionales y dispositivos de almacenamiento. A continuación, se presentan técnicas de seguridad que se deben tener en cuenta:

1.1.9.1 Respaldo de datos.

Es la acción de realizar copias de seguridad de la información que existente en una organización y mantenerla segura y disponible ante cualquier eventualidad de riesgo que se pueda presentar con el sistema de información. (Zabía de la Mata & Agúndez Lería, 2008)

1.1.9.2 Importancia de los respaldos de datos.

La realización de una copia de seguridad tiene altos niveles de importancia debido a que los dispositivos tecnológicos tienden a fallar en cualquier momento inesperado ya que la probabilidad que fallen dos equipos de manera simultánea es poco sustentable. (Aguilera López , 2010)

1.1.9.3 Dispositivos físicos.

Para proteger la integridad de las instalaciones físicas de un sistema de información se deben aplicar tecnologías de aviso que pueden llegar a ser de

mucha utilidad en situaciones de riesgo. Tal es el caso de la implementación de dispositivos de prevención como son detectores de humo, extintores, cortafuegos para hardware, sensores de movilidad, sistema de alarmas y entre otras medidas de seguridad. En cuanto al personal que labora en la organización acceso restringido de forma directa a las instalaciones donde se encuentren los servidores. (Moreno Pérez, 2014)

1.1.10 Vulnerabilidades y amenazas.

Como lo expresa Baca Urbina (2016), amenazas es el término utilizado para referirnos a los peligros que se exponen los sistemas de información como una condición de entornos, áreas o dispositivos que almacenen información de suma importancia. Es la causa principal por la cual se materializa una violación de seguridad la misma que afecta integridad y confidencialidad de la organización.

1.1.10.1 Vulnerabilidad.

Es el punto de acceso por el cual una amenaza tiene la libertad y el espacio libre de realizar un ataque a la información que se almacena en la organización, se aprovecha la poca protección que presentan algunos activos que componen el sistema de información. Existen dos tipos de ataques intencionados y no intencionados. Cuando existe vulnerabilidades en el sistema de información estos se suelen considerar como un defecto de diseño. (Marco Galindo & Marco Simó, 2010)

1.1.10.2 Ataques no intencionados.

Son aquellos que se producen por el descuido de algún empleado de la organización ya que es un hecho que perjudica directamente a la información, tales como: la eliminación, modificación e ingreso en la estructura. Además, se consideran otros factores como un incendio generado por accidente, una inundación por causas del cambio climático, corto circuito debido a la caída de tormenta eléctrica, caída de satélites de comunicación entre otros. (Baca Urbina, 2016)

1.1.10.3 Ataques intencionados.

Como menciona José Luis Raya (2014), Los ataques intencionados son aquellos que se llevan a cabo mediante los accesos no autorizados de usuarios a la

información de una organización, donde el atacante consigue ingresar al sistema y apoderarse de los privilegios de recursos para lograr su cometido. La principal acción que conlleva a estos ataques es robar información o alterarla a su conveniencia con fines inapropiados.

Todos los ataques que se materialicen en un sistema de información suelen provenir del exterior por personas ajenas a la organización que buscan beneficio propio. Aunque también los pueden cometer personas que laboran en la organización al estar en desacuerdo con sus actividades.

1.1.11 Métodos de escaneo de vulnerabilidades.

En el texto de Romero Castro (2018), describe que las vulnerabilidades suelen ser detectadas a través de herramientas de control que realizan un escaneo de los diferentes puertos de accesibilidad con el fin de determinar cuales permanecen abiertos con mayor regularidad y tartar de implementar medidas de seguridad que respalden su protección.

1.1.11.1 Métodos de escaneo.

Existen varios métodos que se pueden utilizar para realizar un escaneo de vulnerabilidades:

1.1.11.2 Caja blanca.

El método de caja blanca es un escaneo que maneja una visión global de la red que pretende analizar, como también tiene el acceso todos los equipos de un modo especifico de super usuario con todos los permisos de usuario adjuntados. Su funcionamiento se basa en la utilidad de usuarios dentro de una red, dentro del software con el propósito de auditar su funcionamiento y seguridad. Además, este método ofrece la posibilidad de realizar acciones adicionales con los privilegios asignados a otros usuarios. (Romero Castro & Figueroa Morán, 2018).

1.1.11.3 Caja negra.

Tiene como función proporcionar información acerca de los accesos a la red o al sistema de información en el que se haya implementado, esta acción se la realiza para controlar el acceso de usuarios no autorizados a la información disponible en la red de comunicación de una organización. Su funcionalidad radica en el análisis de las direcciones IP de los dispositivos conectados a la red recolectando

la mayor cantidad de información acerca de su procedimiento y las acciones realizadas al momento de estar en conexión. Cabe mencionar que solo se aplica este método para documentación de la posible vulnerabilidad que presenten las direcciones IP. (Del Peso Navarro, 2003)

1.2 Redes inalámbricas.

1.2.1 Redes inalámbricas.

En el texto de Joaquín Andreu Gómez (2011) menciona que las redes inalámbricas son aquellas que funcionan sin la necesidad de un cable comunicándose a través de medios no guiados es decir con ondas electromagnéticas que se expanden con el aire.

Las señales que viajan por los medios no guiados son receptadas y emitidas por antenas que cumplen la función de intermediarias o repetidoras con el fin de impulsar las señales con mayor potencia por la red hasta alcanzar su objetivo final el cual puede estar ubicado a varios kilómetros de distancia. Cabe recalcar que dichas antenas pueden ser empleadas en ambos sentidos tanto para emitir como para receptar.

El uso que se le dan a las redes inalámbricas siempre varía con frecuencia, muchas empresas las utilizan para ofrecer servicios de telefonía, otras las emplean en las señales de televisión, incluso para dar seguridad a través de webcam. De esta manera podemos observar que no solo se las emplean en la conexión de datos a través de internet.

1.2.1.1 Características de las redes inalámbricas.

Este medio de conexión nos ofrece muchas ventajas las cuales se describen a continuación:

- Rapidez en la instalación de este tipo de red ya que no necesita de cableado ni autorización para construcciones de obras.
- Facilita la movilidad en la recepción y envío de información ya que no se encuentra atada a cables de red.
- Reducción en los costos por mantenimiento al no existir una red física o cableada que cause desperfectos materiales.

- Fácil acceso a dispositivos móviles y portátiles debido a la utilidad del internet.
- Se presenta como una solución óptica para aquellas zonas a las que es dificultoso acceder con una red cableada como las rurales.

1.2.1.2 Desventajas de las redes inalámbricas.

- Suelen afectarle los cambios atmosféricos como las lluvias, tornados, etc.
- Pueden ser perjudicadas por las interferencias (montañas, velocidad).

1.2.2 Red inalámbrica de área metropolitana.

Como explica José Dordoigne (2015), la red metropolitana (MAN) es aquella que permite alcanzar grandes distancias en la comunicación gracias a la interconexión de múltiples redes de área local. Este tipo de redes prestan sus servicios al interconectar a varios kilómetros de distancia comunidades, ciudades incluso países mediante enlaces públicos o privados.

Las redes de área metropolitana utilizan altos niveles de ancho de banda para dar cobertura a varios kilómetros de distancia facilitando la transmisión en el envío y recepción de datos.

1.2.2.1 IEEE 802.16

El IEEE 802.16 se trata de una norma de especificación que utilizan las redes de área metropolitana inalámbricas la misma que cumple una función de interoperabilidad que permitiendo el acceso o la comunicación a través de microondas.

El objetivo que persigue esta norma es la de potenciar la compatibilidad de conexiones entre los distintos dispositivos que se acojan o estén besados a dicha medida de interoperabilidad tanto para fijos y móviles.

Una de las observaciones más comunes de esta norma es que utiliza una conexión de banda ancha mediante el empleo de arquitecturas en especial la de Punto a Multipunto. En sus inicios las primeras versiones fueron empleadas para la regulación de requisitos necesarios en los sistemas BWA (sistemas de ancho de banda) que tuvieran un rango de operación entre 10 a 66 GHz. (Corral González, 2016)

1.2.2.2 ETSI HiperMan.

El Instituto Europeo de Normas de Telecomunicaciones (ETSI), desarrollo un estándar al cual dio por nombre HiperMan el cual se dedica a proveer DSL (línea de abonado digital) para el acceso a radio de ancho de banda con el objetivo de expandirse en áreas geográficamente grandes. (Corral González, 2016)

1.2.2.3 TTA WiBro.

Desarrollado en Corea de Sur por la Asociación de Tecnología de las Telecomunicaciones (TTA), el WiBro trata de un servicio portátil de internet el cual cumple la función de compatibilidad para la norma IEEE 802.16 presentando en conjunto el sistema WirelessMAN Advanced cuya finalidad es mejorar la señal en un radio geográfico determinado. (Corral González, 2016)

1.2.3 Red inalámbrica de área local.

Local Área Network (LAN) como menciona José Dordoigne (2015), es una red de magnitudes pequeñas que abarcan varios metros de distancia en sus conexiones de red. La red de área local permite la interconexión y comunicación entre si a ordenadores y servidores con la finalidad de compartir recursos similares entre los participantes ya sean estos periféricos, datos o aplicaciones.

La finalidad de una red LAN es la de interconectar un conjunto de ordenadores de un mismo edifico para que compartan información entre sí, es decir, conectados en red a través de señales inalámbricas o cableadas. El uso más adecuado que se le da a las redes LAN es de compartir recursos en conjunto con sus integrantes tales como bases de datos, chat, correos electrónicos. Cabe recalcar que la inversión en la utilidad de esta red conlleva al ahorro tanto de dinero como de tiempo.

1.2.3.1 IEEE 802.11

Como explica Pablo Corral Gonzales (2016), el IEEE 802.11 es un estándar de especificaciones que se utilizan en las redes de áreas locales inalámbricas, el cual regula a los niveles más bajos del modelo OSI como son la capa física y de enlace de datos. En si la función que cumple esta norma es la sustitución de la

capa física y la MAC del conocido Ethernet haciéndola compatible con las redes de áreas locales cableadas.

La compatibilidad que representa la norma especificada tiende a compartirse y tener aceptación en varias topologías, una de ellas la de punto a multipunto, punto a punto siempre y cuando estas se manejen a distancias adecuadas dentro del rango en el que trabajan las redes LAN.

1.2.3.2 ETSI HIPERLAN/2

La red radio de área local de alto rendimiento (HIPERLAN/2) es un estándar que se encarga de la división de frecuencia en anchos de banda de 5 GHz para la cual utiliza la multiplexación de alta velocidad (54 Mbps), además ofrece ahorros de energía, movilidad y una extensión en cobertura de hasta 50 metros de distancia.

Dentro de la capa física HIPERLAN/2 actúa en diferentes modos de trabajo permitiendo que se puedan interconectar con varios tipos de tecnologías sean estas fijas o inalámbricas siendo compatible con cualquier tipo de información. (Corral González, 2016).

1.2.4 Red inalámbrica de área personal.

José Dordoigne (2015), describe que las redes de área personal (PAN) tienen adjudicados alcances restringidos en su arquitectura de red. Este tipo de red es utilizada comúnmente en los hogares ya que se consideran redes individuales o domésticas que permiten la conexión de dispositivos informáticos en espacios cerrados o determinados por distancia (30 metros del usuario). La característica principal que ofrece este servicio es la comunicación de los usuarios participantes desde dispositivos móviles o portátiles de una forma sencilla, práctica y veloz.

1.2.4.1 Tecnologías de la red PAN.

1.2.4.1.1 Infrarrojo.

Es un tipo de tecnología que se basa en la radiación para la transmisión de datos generando bajos niveles en el consumo de energía como también representando bajos costos. La utilidad del infrarrojo atrae consecuencias como la distancia

debido a su corto alcance, además para compartir información entre dispositivos estos deben situarse en línea directa o recta para que sea exitosa la transferencia. (Andreu Gómez, 2011)

1.2.4.1.2 Bluetooth.

Trata de una tecnología que sustituye al infrarrojo en dispositivos móviles y portátiles para la comunicación en áreas de corto alcance mediante la utilización de ondas de radio. A diferencia de la anterior el Bluetooth no es necesario que los dispositivos se encuentren en línea directa para realizar un intercambio de información. (Rodríguez Ávila, 2007)

1.2.4.1.3 Wi-Fi.

Se considera la tecnología más utilizada en la red PAN, es aquella que permite disfrutar de un ancho de banda de mayor densidad en conjunto con un mayor alcance a diferencias de las anteriores. Para poder disfrutar de esta tecnología los dispositivos deben regirse a los estándares IEEE 802.11a y 802.11b. (Marroquín, 2010)

1.2.4.1.4 IEEE 802.15

Pablo Corral Gonzales (2016), menciona que este estándar actúa en los niveles más bajos del modelo OSI como son la capa física y la capa de enlace de datos similar al 802.11. Tiene como base de desarrollo la tecnología Bluetooth para cumplir su trabajo en un ancho de banda de 2.4 GHz cuyo objetivo radica en aumentar la velocidad de interconexión de dispositivos.

1.2.5 Virtualización.

De acuerdo con Miguel Darío González Río (2016), la virtualización corresponde a una tecnología prácticamente de software el cual da la facilidad de ejecución de máquinas virtuales alojadas o pertenecientes a una misma máquina física compartiendo entre si las mismas características de dicho ordenador. A partir de la implementación de esta tecnología los sistemas operativos de servidores fueron los primeros en experimentar la virtualización obteniendo soluciones prácticas a los puestos de trabajo VDI (infraestructura virtual de escritorio) como también representan soluciones basadas en las aplicaciones virtualizadas.

1.2.5.1 Soluciones de virtualización típicas.

A continuación, se describen algunos escenarios de utilización de la virtualización. (Dordoigne, 2015)

1.2.5.1.1 Los equipos clientes están disponibles bajo demanda a través de la red.

Para realizar esta acción es necesario la utilización de terminales ligeros con el fin de conectarse a un sistema operativo cliente ejecutándose o alojado en un ordenador físico. (Dordoigne, 2015)

1.2.5.1.2 Las aplicaciones están disponibles bajo demanda y se publican automáticamente en los puestos de trabajo.

Se basan en la utilización de tecnologías combinadas con Citrix (corporación multinacional que suministra tecnología), las cuales ofrecen un modo de funcionamiento multiusuario a aquellas aplicaciones que se ejecuten dentro de un sistema operativo alojado. Además, permite la ejecución de un perfil de usuario perteneciente a un servidor que aparecerá de manera adjunta en el escritorio del sistema alojado. (Dordoigne, 2015)

1.2.5.1.3 Virtualización de aplicaciones.

Es uno de los objetivos que tienen más expectativa dentro de la virtualización con el fin de la reducción de costos en el mantenimiento y administración de las aplicaciones. Cada aplicación se ejecuta dentro de burbujas donde no representen ningún riesgo a la ejecución de otras aplicaciones en segundo plano. (Dordoigne, 2015)

1.2.5.1.4 Virtualización de puestos de trabajo.

Tiene planteado como objetivo la reducción de costes en cuanto al número de puestos de trabajo existentes dentro del sistema virtualizado aplicando arquitecturas dinámicas y evolutivas. (González Río, 2016)

1.2.6 Redes informáticas actuales.

Según José Dordoigne (2015), en la actualidad las redes se constituyen a través de ordenadores y sistemas operativos que en la mayoría de ocasiones permanecen conectados a internet. Para su respectivo funcionamiento cada red

necesita de recursos y cuya distribución se la realiza por medio de su arquitectura y sus diferentes capas que la constituyen. Los recursos que dispone el usuario en su red los utilizan para la organización de la información recibida de las aplicaciones administradas por las capas que conforman la red especificada.

1.2.6.1 Principales elementos de una red.

José Carlos Gallego (2015) menciona que el sistema operativo de una red es aquel que está constituido por determinadas capas lógicas entre las más comunes los protocolos de comunicación y la capa de aplicación, cuya función es la de mantener conectadas a varias personas físicamente trabajando con los mismos recursos existentes en la red.

La función principal es la de proveer un control en el acceso a la red permitiendo un coordinado sistema de seguridad en accesos simultáneos como por ejemplo la cola de espera.

1.2.6.2 Seguridad a niveles de recursos.

La seguridad de los sistemas operativos basados en red trata de aquellos que tienen la función de pedir u ofrecer servicios más eficientes, con la característica de soportar hardware con niveles avanzados en memorias y espacios de discos.

Al momento de referir sobre la seguridad en los recursos, es específicamente allí donde se debe centrar la seguridad con la aplicación de usuarios y contraseñas para precautelar la integridad de la información que estos puedan contener, la acción para impedir que otros usuarios accedan a los recursos sencillamente es cambiar la contraseña e informar de lo acontecido a los usuarios a quienes conceda el permiso de acceso. (Dordoigne, 2015)

1.2.6.3 Seguridad a nivel de usuario.

La seguridad en niveles de usuarios según José Dordoigne (2015), tienen la función de conceder permisos de manera específica a cada usuario según la acción que vayan a realizar en un recurso determinado, es necesario que cada uno de estos usuarios se encuentren regulados y se identifiquen ante una entidad reguladora de referencia.

1.2.7 Estructura de una red inalámbrica.

1.2.7.1 Necesidad de una red inalámbrica.

La gran necesidad de las redes inalámbricas radica en que la mayoría de las personas esperan conectarse a internet en cualquier parte a cada instante desde los hogares, en el trabajo, en los parques incluido en los viajes. Hace algunos años en el pasado las personas solían estar restringidos con el uso del internet debido a la falta de conocimiento o a la falta de recursos para poder disfrutarlos. En la actualidad en base al avance tecnológico cada persona se mantiene comunicada mediante las redes inalámbricas existentes facilitando la revisión de correos personales a cada momento, comunicarse a través del internet con otros lugares del mundo, facilitar la expansión de información almacenada en la web por medio de dispositivos móviles. (Romero & Barbancho Consejero , 2010).

Un cliente puede acceder a una LAN inalámbrica a través de adaptadores que cumplen la función de captar las ondas electromagnéticas que viajan con el aire y así poder disfrutar del internet por medio de routers inalámbricos o puntos de acceso configurados adecuadamente para la emisión de señales WIFI.

1.2.7.2 Configuración de una red inalámbrica.

Los WAP o punto de acceso inalámbrico es aquel que permite la conexión de diferentes dispositivos a las señales inalámbricas las mismas que conforman una red denominada infraestructura, aunque dichos puntos de acceso pueden permitir que los dispositivos tengan acceso a una red cableada. Cabe recalcar que un punto de acceso es parecido a lo que se conoce como Hub en una red por cable, además da la facilidad de conexión entre otros puntos con el fin formar una red de mayor densidad. (Romero & Barbancho Consejero , 2010)

1.2.7.3 La itinerancia.

Es un término que se lo emplea para referirnos a la capacidad que un dispositivo inalámbrico tiene para desplazarse en varias zonas de coberturas en la cual cada zona está protegida o regulada por un punto diferente. La itinerancia es un proceso que cumple un dispositivo cliente al viajar por toda la red sin perder acceso a la misma. Para que el proceso antes mencionado se cumpla dentro de los puntos de acceso deben existir superposiciones de coberturas de tal manera

que en cada desplazamiento de un cliente no pierda la conexión, el cumplimiento de este proceso se debe a un algoritmo de decisión que deduce en qué momento desconectarse de un punto de acceso y conectarse al siguiente más cercano. (Domínguez, 2014)

1.2.8 Dispositivos inalámbricos.

Como menciona María del Carmen Romero (2010), se pueden dividir los dispositivos que permiten el funcionamiento de una red inalámbrica en aquellos que cumplen la función de generar señales y los que son dedicados a la recepción de ondas o señales que le dan vida a la red WIFI. En la primera clasificación está conformada por los puntos de acceso y los routers que son los encargados de expandir señales para el funcionamiento del internet, por otra parte, citamos a las tarjetas adaptadoras de red que dan paso a la conexión de ordenadores personales pueden ser de tipos internas conectadas mediante los slots, como también externas a través de conectores USB. A continuación, se describe detalladamente la función que cumple cada uno de los dispositivos mencionados.

1.2.8.1 Los puntos de acceso.

Su funcionalidad se representa por un intercambiador de acceso remoto permitiendo a la red inalámbrica tener conexión o acceso a una red alámbrica que reciba las señales por medio de cableado. Entre las funciones que realizan los puntos de acceso se encuentra la captura de señales débiles para impulsarla con mayor potencia.

1.2.8.2 Los routers.

Son aquellos que se encargan de la recepción de señales brindadas por su operador de servicios de telecomunicaciones. Su funcionamiento es simple, repartir señales a los elementos que están conectados a la red y los que forman parte de la red inalámbrica. Cumplen con la corrección de errores al momento de receptar señales.

1.2.8.3 Tarjetas PCI.

Son diseñadas para la tecnología WIFI vienen incorporadas en las portátiles como también en ordenadores de escritorio.

1.2.8.4 Tarjetas USB.

Es un tipo de tarjeta cuyo funcionamiento es el más sencillo de realizar ya que solo se debe conectar a un computador ya sean estos portátiles o de escritorio.

1.2.8.5 Tarjetas PCMCIA.

Son antiguas en la actualidad ya que fueron las primeras tarjetas de red que se incorporaron a las portátiles para su posible conexión a las redes inalámbricas

1.2.9 Seguridad de las redes inalámbricas.

Una vez identificados cuales son los tipos de patrones que un atacante puede utilizar con el fin de obtener información a través de las redes inalámbricas para beneficio propio, existen medidas como el uso de criptografía que al aplicarlas daría una mejor solución en cuanto a seguridad. (Díaz Uretra & Alonso Castro, 2014)

1.2.9.1 Principios de diseño seguro para redes inalámbricas.

1.2.9.1.1 Defensa en profundidad.

La principal idea que aborda a esta medida es la de usar diferentes medios para darle seguridad a la red. En muy común ver que los administradores utilicen medios de defensa como el WEP o WPA como un solo método de prevención ya que trabajan con técnicas de autenticación y cifrado para proteger a la red. Un atacante puede vulnerar este tipo de seguridad ya que puede conocer las claves de acceso mediante aplicaciones que dejan al descubierto a las redes inalámbricas (Díaz Uretra & Alonso Castro, 2014)

1.2.9.1.2 Privilegios mínimos.

La finalidad de esta medida de seguridad es la de conceder permisos solo a los recursos que sean necesario o que se soliciten para emplear en un lugar de trabajo, un usuario normal no debe tener privilegio a todos los recursos de la red ya que representaría un riesgo a la información almacenada. Los permisos o privilegios en su totalidad solo el administrador puede tener control sobre ellos.

1.2.9.1.3 Cajas Faraday.

Este método de seguridad tiene la finalidad de bloquear las señales inalámbricas ubicadas en una empresa determinada, es decir, limitar el perímetro de

funcionalidad dejando libre acceso a las señales que provienen del exterior y a su vez impidiendo que las señales provenientes del interior no puedan salir del rango delimitado. Las cajas de Faraday en el ámbito de la seguridad pueden representar una costosa inversión de dinero debido a los equipos que necesitan para implementarla. (Díaz Uretra & Alonso Castro, 2014)

1.2.9.1.4 Filtro de direcciones MAC.

Los filtros de direcciones MAC es una lista que brinda la capacidad de controlar a los clientes cuyo permiso de acceso a la red es concedido, su funcionamiento radica en proteger a la red de intrusos que deseen ingresar y alojarse en los recursos de la red inalámbrica negándoles la conectividad si su dirección MAC no consta ingresada en la lista de permisos activos. (Navarro Lacoba, 2014)

1.2.10 La red extendida.

Como describe en su texto José Dordoigne (2015), una red extendida es aquella que tienen alcances a mayores densidades de áreas geográficas. Las redes WAN son aquellas conformadas por redes de tipo LAN e incluso MAN, las capacidades que alcanzan este tipo de redes son increíblemente grandes que llegan a cubrir miles de kilómetros alrededor del mundo. La red que más fama mundial tiene es el conocido internet que mantiene comunicado al mundo a través de múltiples servicios que ofrece

Este tipo de redes como lo menciona Pedro Mora Pérez (2017), pueden ser desarrolladas y a la vez utilizadas por organizaciones como las proveedoras de servicios como las telecomunicaciones. La funcionalidad que maneja este tipo de red es de punto a punto cuyos beneficios pueden utilizarse en grandes radios geográficos incluso satelitales.

1.2.10.1 Ventajas de las redes WAN.

- No cuenta con limitaciones en lugares o espacios para la instalación de sus equipos.
- Dentro de sus mayores beneficios esta red ofrece un conjunto de medios que se pueden emplear en transmisión de datos: fibra óptica, cableado de cobre, satelitales, radio enlaces, etc.

- Los dispositivos utilizados por esta red tienen incorporado un software especial que ayuda en la conexión de grandes computadoras y dispositivos móviles a equipo de recepción pequeños.

1.2.10.2 Desventajas de las redes WAN.

- Para el correcto funcionamiento de este tipo de red es necesario contar con equipos de altos niveles de memoria y procesamiento, de aquello dependerá la velocidad con la que trabaje la red.
- La desventaja más significativa que esta red representa es el software malicioso al que es vulnerable ya que es infectada por piratas informáticos para apoderarse de la información que circula por la red.

1.2.11 Herramientas de testeo de seguridad

1.2.11.1 Hombre en el Medio (Man in the Middle)

Un ataque Hombre en el Medio (Man in the Middle), es aquel que se materializa mediante un intermediario donde tiene la facilidad de acceder a las comunicaciones que se establecen en una red ya sea inalámbrica o cableada. Este tipo de ataque funciona mediante el desvío de información a una dirección alterna que le permite al atacante tener acceso a ella y modificarla antes de llegar a su destinatario correcto. (Broy de la Cruz, 2013)

Para protegerse de un ataque de MITM (hombre en el medio) se utiliza un tipo de cifrado o autenticación SSL de extremo a extremo que protege la información que circula por la red cuando esté en conexión, también se debe tener en cuenta las siguientes medidas:

- Usar HTTPS
- Activar la verificación de dos pasos
- Usar una red VPN

1.2.11.2 La herramienta NESSUS.

Castro Gil, Díaz Orueta, Alzórriz Armendáriz & Sancristóbal Ruíz (2014), Es una herramienta empleada para el análisis de vulnerabilidades cuyo objetivo es detectar puertos abiertos por donde se puede llevar a cabo un ataque por parte de los hackers. Este tipo de herramientas para el análisis de vulnerabilidades utilizan un sistema conocido como Nessus Profesional-Feed el cual se dedica a

buscar puertos con vulnerabilidades en la red y generar un informe con los resultados reflejados en el testeo. Las características más comunes de la herramienta Nessus son:

1.2.11.2.1 Análisis en profundidad

La herramienta Nessus realiza este tipo de análisis con rapidez a aquellos programas pertenecientes a la organización escaneando los diferentes puertos de acceso a internet existentes en la red de una organización utilizando direcciones IP dinámicas, direcciones MAC o DNS, cuya finalidad es dar a conocer el nivel de vulnerabilidad que posee cada puerto.

1.2.11.2.2 Auditoria Antivirus, de botnets y procesos maliciosos.

Este proceso realiza un análisis para detectar procesos maliciosos en las computadoras que utilicen el sistema operativo Windows, mejorando la función del antivirus para su correcta ejecución, también lleva a cabo un eficiente escaneo para detectar infecciones en los ordenadores ya sean por parte de botnets (infecciones con software malicioso) o servidores web, brinda control sobre la búsqueda de vulnerabilidades y configuraciones erróneas.

1.2.11.3 La herramienta Wireshark

Es una herramienta que analiza el tráfico que circula por la red de una organización, con la implementación de sus módulos permite el acceso a los paquetes capturados dejando a la vista de los clientes los protocolos que lo integran sean estos de tipo HTTP, TCP. Con la implementación de Wireshark el cliente tendrá la posibilidad de visualizar la disección de los paquetes que viajan por la red. (Hertzog & Mas, 2016)

CAPITULO II

2 DIAGNOSTICO O ESTUDIO DE CAMPO

2.1 Tipos de investigación

2.1.1 Estudio de campo

La principal función de este tipo de investigación es recolectar información a través de testificaciones que tienen su fundamento en la realidad, dependiendo de interpretaciones subjetivas como documentos o evaluaciones que comprueben la veracidad del tema que se está planteando a tratar. (Landean, 2007)

Con la implementación de este tipo de investigación se facilitó la interpretación de resultados obtenidos en los diferentes medios de recolección de datos.

2.1.2 Investigación descriptiva

La investigación descriptiva basa sus funciones en describir, analizar e interpretar de realidades, detalles y comportamiento de los fenómenos como también su composición. Con la finalidad de presentar interpretaciones correctas, hace referencias en las características fundamentales del objeto de estudio. (Rodríguez Moguel E. , 2005)

Este procedimiento fue aplicado en esta investigación, con la finalidad de entender y realizar las fichas de observación donde se organizó la información obtenida en los análisis de seguridad y sus hallazgos aplicados con la herramienta Nessus.

2.1.3 Investigación explicativa.

Como explica Emilio Latorre Estrada (1996), la investigación explicativa es aquella que busca establecer una serie de proposiciones coherentes sobre un objeto de estudio, mediante las cuales se conoce la realidad. Buscan explicar las causas que originaron la situación que se está analizando.

Mediante este tipo de investigación se generaron las conclusiones del estudio realizado en la cual se explicó los acontecimientos encontrados mencionando las causas que los pudieron generar.

2.1.4 Investigación cuantitativa.

La investigación cuantitativa se basa en el estudio y análisis de la realidad a través de diferentes procedimientos basados en la medición, además permite

obtener un mayor nivel de control e inferencia, siendo posible realizar experimentos y obtener explicaciones a partir de la hipótesis. Los resultados de esta investigación se basan en la estadística. (Latorre Estrada, 1996)

2.2 Métodos de la investigación

2.2.1 Método inductivo.

"El método inductivo el cual es un proceso en el que, a partir de un estudio de casos particulares se obtienen conclusiones o leyes universales que explican o relacionan los fenómenos estudiados". (Rodríguez Moguel E. , 2005, pág. 29)

Este tipo de método ayudó en la obtención de conclusiones acerca de los resultados obtenidos de la metodología aplicada en el análisis que se llevó a cabo dentro de la investigación

2.2.2 Método deductivo.

En el año (2012) José Cegarra Sánchez mencionó que el método deductivo se lo emplea para buscar solución a los problemas que nos planteamos. Consiste en emitir hipótesis acerca de las posibles soluciones al problema encontrado y además comprobar con los datos disponibles si estos están de acuerdo con aquellas.

Este método se lo empleó en la ayuda con las posibles soluciones que se emplearon a las vulnerabilidades que se encontraron en el análisis ejecutado dentro de la investigación.

2.3 Población y Muestra

2.3.1 Población

La población que se ha estimado como base para la presente investigación se ha considerado al conjunto de estudiantes de las diferentes carreras que residen en la planta central de la Universidad Laica Eloy Alfaro de Manabí Extensión en El Carmen, sin incluir a los estudiantes de la carrera de Ingeniería Agropecuaria (978 estudiantes) los cuales usan las redes inalámbricas objeto de este trabajo investigativo.

2.3.2 Muestra

La muestra a quien se aplicó el estudio se ha considerado una cantidad estudiantes obtenida mediante la fórmula muestral donde se obtuvo un total de 74 estudiantes como muestra, mismos que fueron objeto del presente estudio.

Para establecer el resultado de la muestra se estableció mediante los siguientes datos:

- Población (N) 978
- Número 5 coeficiente de confiabilidad para el 95%
- p y q probabilidad de éxito y fracaso (40)
- E margen de error seleccionado (10)g

Fórmula.

$$n = \frac{5Np.q}{E^2\ (N-1) + 5p.q}$$

$$n = \frac{5(978)(40)(40)}{10^2\ (978-1) + 5(40)(40)}$$

$n = 74$ (valor redondeado)

2.4 Técnicas de investigación

2.4.1 La encuesta.

Esta técnica se aplicó a los estudiantes de la carrera de sistemas para obtener información o el punto de vista de aquellos que utilizan aplicaciones web mediante las redes inalámbricas de la ULEAM El Carmen. (Huaman Valencia , 2005)

2.4.2 La entrevista.

Como menciona Acevedo Ibáñez y López Martín (2004), la entrevista es un medio por el cual dos personas (entrevistado y entrevistador) establecen una conversación con la finalidad de obtener datos sobre un tema de interés para el entrevistador, donde el entrevistado da respuestas a interrogantes relacionadas a un objeto de estudio o problema específico. Esta técnica se le aplicó al administrador del área de informática de la ULEAM El Carmen con la finalidad de obtener información relevante para esta investigación.

La observación.

Esta técnica de investigación se la aplicó con el fin de observar el comportamiento de las redes inalámbricas y sus vulnerabilidades para obtener información acerca de ellos. (Huaman Valencia , 2005)

2.5 Resultados de Diagnósticos

2.5.1 Entrevista

Realizar entrevista sobre la seguridad en redes inalámbricas al administrador del área informática de la ULEAM El Carmen

1. **¿Quién es el proveedor que presta servicios de internet a la universidad?**

   El proveedor de internet que da este servicio a la universidad es la compañía CNT mediante un túnel de datos, es decir no ofrece salida a internet directamente sino un servicio de datos, con un ancho de banda de 90 megabyte.
2. **¿Por qué medio llega el internet a la universidad?**

   El encargado del área de sistemas mencionó a esta interrogante que el medio por el cual llega el internet hasta la universidad es la fibra óptica hasta el servidor principal.
3. **¿Existen tipos de redes WIFI, y cuales se implementan en las redes de la universidad?**

   Menciona el administrador de sistemas que existen configuraciones a redes WIFI de la universidad de 2.4 GHz y 5 GHz para la conectividad de los dispositivos a internet.
4. **¿Qué tipo de seguridad se implementan en las redes inalámbricas de la universidad?**

   Como respuesta a esta pregunta el encargado de sistemas mencionó que en la actualidad no configura personalmente ningún tipo de seguridad en las redes inalámbricas de la universidad, pero que hace unos años atrás se utilizaba el medio de seguridad portal cautivo.
5. **¿Existe algún control en la navegación de internet en la universidad?**

   Hace referencia el encargado de sistemas que en los predios de la ULEAM Extensión en El Carmen no se lleva un control en la navegación por el motivo que no tiene acceso a los equipos y sus configuraciones.
6. **¿Los estudiantes tienen libre acceso a todo tipo de sitios web cuando utiliza las redes inalámbricas de la universidad?**

En este apartado el encargado del área de informática asegura que los estudiantes no tienen libre acceso a los sitios web mientras utilizan el internet de la universidad, ya que existen páginas bloqueadas por categorías entre ellas vinculadas con la violencia, sitios pornográficos, entre otros.

7. **¿Los sitios web de la universidad se encuentran protegidos, de qué manera?**

   Según el encargado del área de informática de la universidad los sitios web pertenecientes a la misma tienen una protección en cuanto a protocolos de seguimientos de acceso y contraseñas dificultosas.

8. **¿Cómo gestiona el proveedor los riesgos de seguridad de la información?**

   Las acciones que toma el encargado del área de informática de la universidad según menciona ante esta interrogante es la de contactar a los encargados en la matriz en Manta para dar soluciones a los inconvenientes en cuestiones de instalaciones físicas de internet, en cuanto al servicio de datos los encargados de Manta levantan un contacto con el proveedor para verificar el acontecimiento.

9. **¿Qué tipo de incidentes de seguridad son mitigados por usted?**

   Según el encargado del área de informática menciona que en la actualidad su función es la de actuar como un intermediario o soporte de redes de los encargados en la matriz en Manta y no realiza ningún tipo de acción hacia los incidentes de seguridad. Lo que el realiza es acciones de seguridad en conexiones físicas como por ejemplo el cable de red que conecta a una computadora con el puerto de internet.

10. **¿Utiliza un Firewall para que la organización pueda identificar las susceptibilidades del sistema y también prevenir una invasión de hackers?**

    Como menciona el encargado del área de informática, hace un tiempo atrás él tenía a su cargo la administración y configuración de seguridad y utilizaba en los servidores un Firewall de Linux llamado IPtables. En la actualidad no tiene acceso a ningún tipo de configuración y administración lógica en las redes de la universidad.

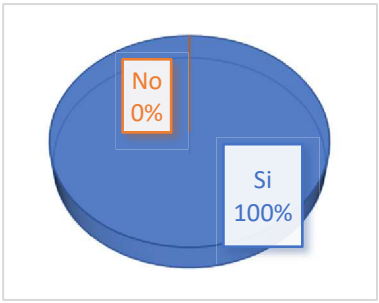
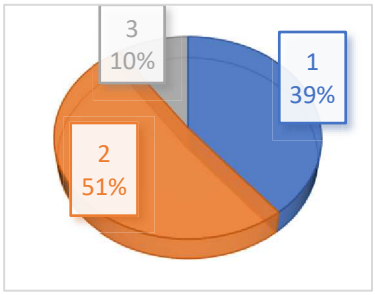
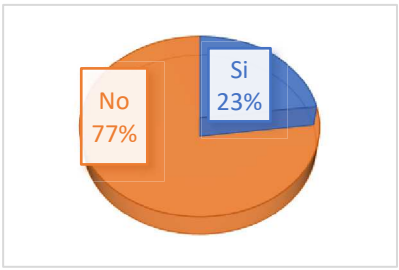
11. **¿Ante un ataque informático llevado a cabo por hackers cuales son las primeras acciones que se toman?**

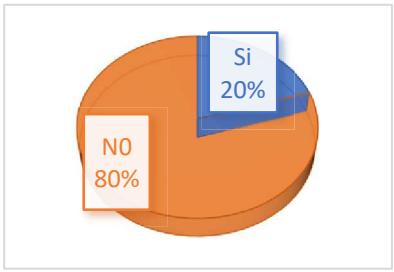
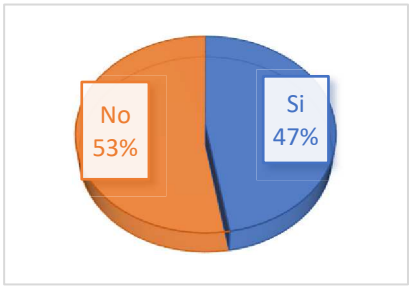
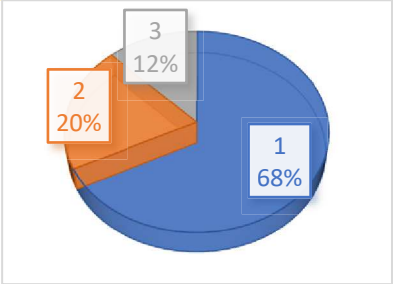
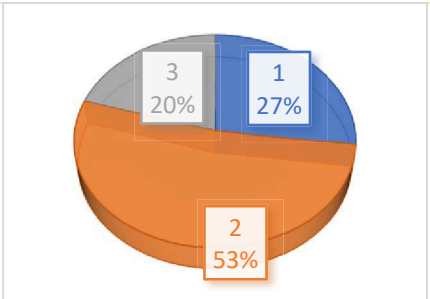
    El encargado del área de informática de la universidad, menciona que en lo personal recomienda el cambio de contraseñas y capacita a los afectados que no realicen acciones en coreos electrónicos enviados desde fuentes peligrosas cuyo fin es hackear cuentas y hurtar información, además de la suspensión temporal del sitio que haya sido victimado.

12. **¿Cuenta con las soluciones de seguridad adecuadas?**

    Menciona el encargado del área de informática que en cuestiones de soluciones adecuadas a los inconvenientes de seguridad están limitados por falta de recursos en los dispositivos para la instalación de los antivirus oficiales como Kaspersky que necesita grandes espacios de almacenamiento. Además, hace referencia que falta capacitación para los estudiantes y docentes quienes son los principales facilitadores de información dentro del uso de internet en la universidad.

2.5.2 Encuesta

Pregunta	Gráficos	Descripción
1. ¿Utiliza usted las redes inalámbricas de la universidad?	 Si: 74 No: 0	En base a los datos obtenidos en la encuesta, el 100% de la población tomada en cuenta para este trabajo ha mencionado que utilizan las redes inalámbricas de la universidad para desarrollar diversas actividades mientras se encuentran en ella.
2. ¿Con qué frecuencia utiliza las redes inalámbricas de la universidad?	 De 1 a 2 horas: 29 De 2 a 3 horas: 38 Más de 5 horas: 7	Como reflejan los datos obtenidos en la encuesta los estudiantes mientras están en la universidad utilizan las redes inalámbricas un periodo de tiempo que se estima entre 3 a 4 horas con un total de 52%, el 40% de la población estudiantil permanecen en conexión de 1 a 2 horas, mientras que un 8% las utilizan por más de 5 horas.
3. ¿Usted cree que las redes inalámbricas de la universidad son seguras?	 Si: 17 No: 57	Con el total de la población encuestada los datos obtenidos en este apartado reflejan que un 80% de los estudiantes piensan que las redes inalámbricas de la universidad no están adecuadamente protegidas, mientras que el 20% piensa que los protocolos de seguridad funcionan adecuadamente

4. ¿Ha ingresado a la banca móvil utilizando la red de la universidad?	 Si: 15 No: 59	De los estudiantes encuestados el 85% mencionaron que no han ingresado a una banca móvil desde la conexión de las redes de la universidad ya que consideran que no son correctamente seguras para realizar este tipo de transacciones, tan solo el 15% de ellos han realizado ingresos a esta plataforma bancaria.
5. ¿Ingresa contraseñas importantes utilizando la red de la universidad?	 Si: 35 No: 39	Con la encuesta finalizada los datos obtenidos demostraron que el 52% de los estudiantes de la universidad no acostumbran a ingresar contraseñas de sus cuentas personales al estar en conexión de las redes inalámbricas por temor a ser hackeados en cualquier momento ya que las consideran inseguras
6. ¿Con qué fin utiliza las redes inalámbricas de la universidad?	 Estudios: 50 Entretenimiento: 15 Redes sociales: 9	En su gran mayoría los estudiantes de la universidad utilizan las redes inalámbricas con fines educativos representando un 66% del total de encuestados, un 19% de ellos las utilizan en redes sociales y el 15% mantienen otro tipo de actividades de entretenimiento.
7. ¿Qué tipo de aplicaciones utiliza cuando está en la universidad?	 Correo: 20 Aula virtual: 39 Webs informativas: 15	Un total de 59% de la población sometida a la encuesta afirmaron que la aplicación más utilizada mientras se encuentra en la universidad es el aula virtual, un 21% de ellos mencionaron al correo electrónico como favorito y el 20% restante invierten su tiempo en páginas webs informativas.

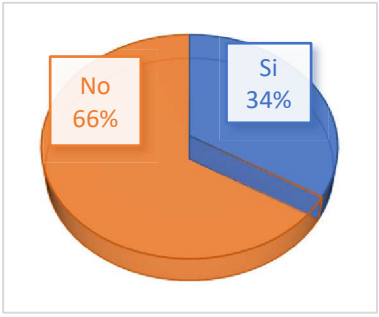
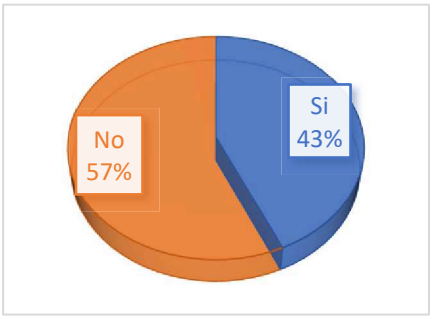
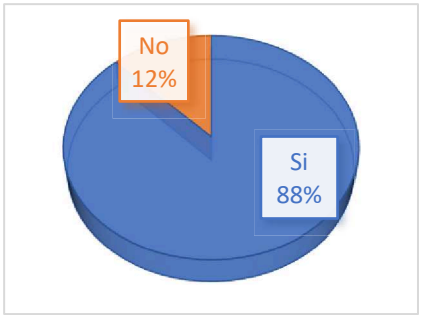
8. ¿Tiene libre acceso a todo tipo de páginas webs cuando utiliza las redes inalámbricas de la universidad?	 Si: 25 No: 49	Los datos que se obtuvieron al realizar esta encuesta mencionan que los estudiantes no tienen libre acceso a cualquier página alojada en la web, la respuesta negativa del 66% de los estudiantes encuestados mientras que el 34% restantes dijeron sí.
9. ¿Existe algún control en la navegación en la universidad?	 Si: 32 No: 42	El resultado reflejado por esta pregunta de la encuesta menciona que un total del 57% de la población piensa que no existe un control en la navegación con el internet de la universidad, es decir que se puede acceder a cualquier contenido alojado en la web desde los dispositivos móviles o computadoras, mientras que el 43% piensa que si existe un control que limita la navegación.
10. ¿Le gustaría contar con sistemas que protejan la información que usted envía mientras utiliza las redes de la universidad?	 Si: 65 No: 9	Un 95% de los encuestados mencionaron que es factible implementar sistemas o protocolos que protejan la información que circula por las redes de la universidad, y que se realicen acciones de test para verificar la fuente y originalidad de las páginas Web a la que se tenga acceso, e impida el hurto informático, un 3% menciona que no es factible dicha acción ya que consideran que están en óptimas condiciones las redes de la universidad.

Ilustración 1: *R*esultados de encuesta.

Fuente: Estudiantes de la Universidad Laica Eloy Alfaro de Manabí Extensión en El Carmen
Autor: *Jonathan Delgado Basurto (2019)*

2.6 Análisis de Resultados o Triangulación

Con los datos obtenidos de los instrumentos utilizados para la recolección de información dentro de la Universidad Laica Eloy Alfaro de Manabí Extensión en El Carmen (planta central) sin incluir a los estudiantes de la carrera de Ingeniería Agropecuaria, se puede deducir que en su gran mayoría los estudiantes consideran que las redes inalámbricas no brindan una seguridad adecuada al momento realizar sus funciones y en ciertas ocasiones es preferible utilizar plan de datos para mantener segura la integridad de su información en sus dispositivos móviles. Esta consecuencia tiene su origen al no tener conocimientos si existen medidas de seguridad que se implementen para controlar y limitar la navegación y el acceso a páginas webs, así como también compartir archivos de dudosa procedencia.

Se cuestionó tanto a estudiantes (pregunta número 9 de la encuesta) como al encargado del área de informática de la universidad (pregunta número 5 de la entrevista) si existe control en la navegación de internet cuando se encuentran en uso de las redes inalámbricas a la cual el estudiantado respondió en su mayoría que no están al tanto si existen denegación de usabilidad, mientras que el personal administrador de sistemas hace referencia en que no cuenta con la autorización de realizar configuraciones a sistemas de ninguna índole en la ULEAM Extensión El Carmen, pero que en la Matriz de la universidad radicada en la ciudad de Manta si llevan registros de navegación. Se ha evidenciado que no existe una socialización por parte del personal encargado hacia los estudiantes acerca de las seguridades que se ejecutan dentro de la Universidad y que restringen el acceso a diversas fuentes de la web.

Por otra parte, el personal encargado de los sistemas informáticos de la universidad hace referencia en que, sí se implementan técnicas de seguridad (pregunta número 6 de la entrevista) para que el estudiantado tenga total privacidad al conectarse en las redes inalámbricas de internet, con ciertas limitaciones, bloqueando el acceso a páginas que contengan virus informático, relacionados con violencia o que puedan descargar automáticamente archivos de procedencia indebida, mientas que los estudiantes (pregunta número 8 de la encuesta) acertaron que si existe control en la navegación al no poder ingresar a cualquier contenido en la web.

CAPITULO III

3 PROPUESTA

3.1 Antecedentes

El 10 de junio de 1986, el Comité de Gestión para la creación de esta Unidad Académica, el cual estuvo conformado por el Sr. Gilberto Farfán Espinoza, Dr. Jorge Garzón Delgado, Sr. Ever Barberán Vera, Prof. Ariolfo Cuadros, Sr. Benigno Andrade Falcones, Sr. Ernesto García Espinoza y Sr. Walter López Candela, viajó a la ciudad de Manta para sostener un diálogo con el Señor Dr. Medardo Mora Solórzano, Rector de la Universidad Laica “Eloy Alfaro” de Manabí, a fin de solicitarle la creación de un centro de estudios superiores en El Carmen. El Dr. Mora manifestó que realizaría un estudio de la Ley de Universidades y en base a aquello determinaría la posibilidad de atender el pedido.

En marzo de 1987, el Sr. Rector acompañado entre otras personas por el Ing. José Emilio Muñoz Galarraga, director del Departamento de Planeamiento de la Universidad, visitó este cantón. Sostuvo una reunión con las fuerzas vivas de El Carmen. El Dr. Mora se comprometió realizar el mejor de los esfuerzos para darle a este cantón un Centro Universitario; así, le encargó en ese mismo momento al Director de Planeamiento que iniciara el estudio necesario para el efecto.

El 12 de marzo de 1988, el Ing. José Emilio Muñoz Galarraga, comunicó al Comité de Gestión que la creación del Centro Universitario de Estudios a Distancia de El Carmen es un hecho, y que se abrirá con tres carreras: Tecnología Agropecuaria, Tecnología en Administración Rural y Licenciatura en Educación Primaria.

En ese mismo mes y año, el Señor Rector invitó al Comité para dar lectura al Proyecto de Creación del Centro de Estudios a Distancia de El Carmen. Posteriormente, se lo puso a consideración del Honorable Consejo Universitario; este organismo resolvió su aprobación. El Ing. Emilio Muñoz Galarraga fue designado como director, el Sr. Klever Soledispa Tóala, Coordinador en Manta y el Lic. Guido Vásconez González, Coordinador en El Carmen.

El 4 de julio del 1988 el Sr. Rector inauguró oficialmente el Centro Universitario de Estudios a Distancia. El 9 de julio del mismo año iniciaron formalmente las actividades académicas.

El personal docente estuvo integrado por: Ing. José Robles García, Ing. Víctor Román Posligua, Dr. Auter Cuenca Ramón, Dr. Miguel Santana Chávez, Dr. Oliver Vera Paz, Lic. Iván Medranda Saltos, Lic. Milton Utreras y el Lic. Stalin Morejón. Fue designada como secretaria- Tesorera la Lic. Patricia Salvatierra y, posteriormente, el Sr. Nery Ramón Figueroa, como Auxiliar de servicios. El lugar donde se laboró inicialmente fue en el Colegio Nacional Mixto El Carmen. EL 13 enero 1994, por gestión del Dr. Medardo Mora Solórzano, Rector, el CONESUP entregó a esta Institución de Estudios Superiores de El Carmen, la calidad de Extensión Universitaria, facultando expresamente la modalidad presencial. (ULEAM, 2019)

3.2 Misión Universidad Laica Eloy Alfaro de Manabí Extensión en El Carmen

La Universidad Laica “Eloy Alfaro” de Manabí Extensión en El Carmen es una institución de Educación Superior cuyo compromiso es formar ciudadanos y ciudadanas profesionales responsables, éticos y solidarios con la sociedad; capaces de generar y aplicar sus conocimientos y estrategias que contribuyan al desarrollo sustentable y al mejoramiento de las condiciones de vida de los y las habitantes de El Carmen y Manabí. (ULEAM, 2019)

3.3 Visión Universidad Laica Eloy Alfaro de Manabí Extensión en El Carmen

La Universidad Laica Eloy Alfaro de Manabí Extensión El Carmen es una institución de Educación Superior moderna y líder en el ámbito de su actividad académica-científica y formativa de ciudadanos profesionales, quienes participan, colaboran, promueven y se comprometen con el desarrollo sustentable y el mejoramiento de las condiciones de vida de los y las habitantes de El Carmen y Manabí. (ULEAM, 2019)

3.4 Organigrama

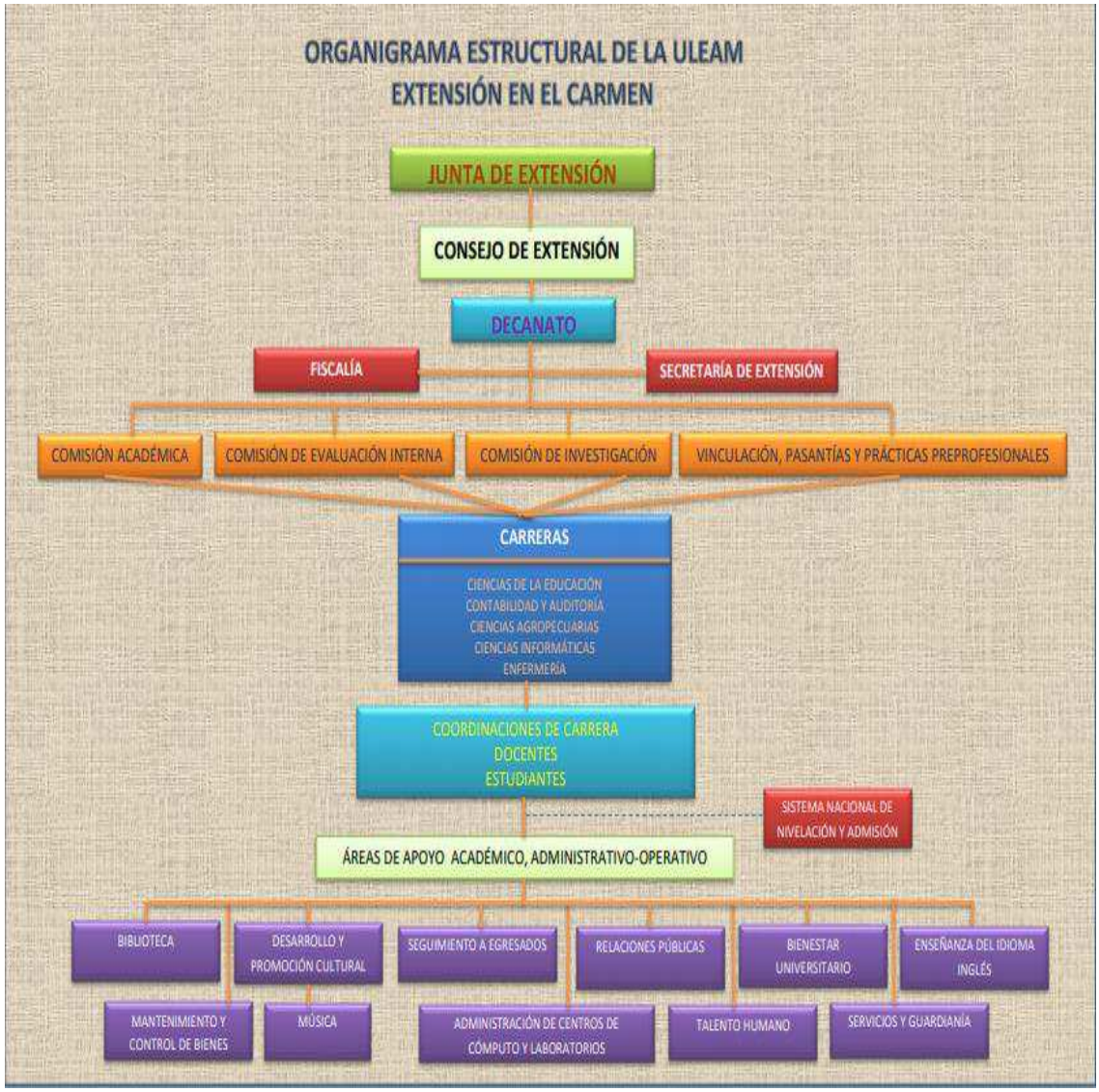


Ilustración 2: *Estructura Orgánica de la Universidad Laica Eloy Alfaro de Manabí Extensión en El Carmen*
Fuente: *(ULEAM, 2019)*

3.5 Programa de auditoría

PROGRAMA DE AUDITORÍA DE ANÁLISIS DE SEGURIDAD MEDIANTE METODOLOGÍA OWASP A REDES INALÁMBRICAS EN "UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ EXTENSIÓN EN EL CARMEN"

Objetivos:

- *Analizar la seguridad en las aplicaciones web que utilizan las redes inalámbricas en la ULEAM Extensión El Carmen con la finalidad de verificar el cumplimiento de los estándares.*
- *Comprobar el nivel de seguridad en las redes inalámbricas de la Extensión universitaria.*

Técnicas y procedimientos	Papel de trabajo	Fecha
Revisar la metodología OWASP.	C	26-04-2019
Elaborar cuestionarios según la OWASP sección seguridad web.	C	28-04-2019
Entrevista a los estudiantes de la universidad para identificar vulnerabilidades	C	06-05-2019
Realizar observaciones mediante herramientas seleccionadas	C	16-05-2019
Identificación de amenazas	PT	24-05-2019
Análisis de instrumentos e identificación de vulnerabilidades	PT	10-06-2019
Clasificar los riesgos encontrados	PT	20-06-2019
Elaborar informe	PT	01-07-2019

Realizado por: Delgado Basurto Jonathan
Fecha: 22-04-2019

3.6 Oficio de presentación

OFICIO DE PRESENTACIÓN

El Carmen, 11 de septiembre del 2019

Dr. Temístocles Bravo T., Mg.

Decano de la Universidad Laica Eloy Alfaro de Manabí Extensión en El Carmen

De mi consideración. –

El presente tiene como finalidad dar a conocer el informe de auditoría informática realizada en la Universidad Laica Eloy Alfaro de Manabí Extensión en El Carmen durante el período comprendido entre 2018 – 2019 con la finalidad de evaluar la seguridad de las redes inalámbricas de la institución y el aula virtual en función de la Metodología OWASP, verificando que se cumplan los procedimientos que garanticen la integridad, disponibilidad y confidencialidad de la información; basado en la evidencia que se obtuvo durante el tiempo de evaluación me permito emitir un informe sobre el nivel de seguridad encontrado así como también proponer medidas que podrían prevenir riesgos detectados.

Adjunto informe.

_____
Jonathan Delgado Basurto
C.I. 1313663492

INFORME DE AUDITORÍA DE ANÁLISIS DE SEGURIDAD MEDIANTE METODOLOGÍA OWASP A REDES INALÁMBRICAS EN “UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ EXTENSIÓN EN EL CARMEN”

Realizado por: DELGADO BASURTO JONATHAN MOISÉS

El Carmen, enero 2020

Lugar: **ULEAM El Carmen**

Provincia: **Manabí**

Número de Instituciones evaluadas: 1

3.7 Informe de auditoría

En este informe se presentan los resultados acerca del análisis de seguridad aplicado a las redes inalámbricas de la Universidad; en el mismo se detallan los riesgos que tiene relación con las vulnerabilidades en cuanto a conexión inalámbrica de los dispositivos móviles y la navegación en la aplicaciones web de mayor utilidad por los estudiantes mientras se encuentran en uso del internet de las instalaciones en toda la universidad, también se detalla las acciones que se debe considerar para la solución de los acontecimientos encontrados durante el análisis y reducir en gran parte el posible impacto que podría ocasionar un riesgo.

3.7.1 Dirigido a:

Este análisis de seguridad a redes inalámbricas va dirigido a la Universidad Laica Eloy Alfaro de Manabí Extensión en El Carmen.

3.7.2 Objetivos:

Para llevar a cabo el desarrollo de análisis de seguridad se plantearon objetivos los cuales influyeron en las apreciaciones acerca de los aspectos a estudiar en las redes inalámbricas de la Universidad los mismos que fueron:

- *Analizar la seguridad en las aplicaciones web que utilizan las redes inalámbricas en la ULEAM Extensión El Carmen con la finalidad de verificar el cumplimiento de los estándares.*
- *Comprobar el nivel de seguridad en las redes inalámbricas de la universidad.*

3.7.3 Personal relacionado

En el estudio de este análisis de seguridad se encuentran involucrados todos aquellos que utilizan las redes inalámbricas en la ULEAM El Carmen para tener acceso a las diferentes aplicaciones web y plataformas relacionadas al estudio y entretenimiento, sean estos: estudiantes, docentes y administrativos, los cuales brindaron información relevante acerca del uso que le dan al objeto de estudio.

3.7.4 Alcance

Como parte fundamental de esta auditoria informática se utilizó la metodología de análisis web OWASP cuya función radica en la protección de sitios web ya sean estos de uso académico, empresarial y personal además de informar sobre la existencia de vulnerabilidades en configuraciones o en la utilidad de los mismos fomentando la necesidad de gestionarlos, brindando planes para mantener bajo control los riesgos y las vulnerabilidades a los que se encuentran expuestos, esta metodología cuenta con un top diez en vulnerabilidades que se utilizaron en el proceso de evaluación, en el cual se inició con la elaboración de cuestionarios con la finalidad de evaluar la seguridad que los usuarios de los sitios web implementan al utilizar las redes inalámbricas de la universidad, dicho instrumento de evaluación está compuesto por 69 preguntas basados en los controles establecidos por la metodología OWASP.

Una vez que la información necesaria se recolectó dentro de la universidad (planta central), se procedió a la tabulación en una matriz de Excel el instrumento utilizado en base a porcentajes.

NRO.	PREGUNTA	Si	No	% Si	% No
	Seguridad web				
1	¿Se conecta de forma fácil al Wifi de la universidad?			92%	8%
2	¿Ha suministrado datos correctos en aplicaciones web, y al momento de cargar regresan al mismo lugar de ingreso de datos?			30%	70%
3	¿Dentro de los parámetros de búsqueda ha experimentado pérdida de información?			60%	40%
4	¿Divisa publicidad indebida al intentar acceder a una aplicación web?			18%	82%
5	¿Ha experimentado algún tipo de filtración en sus sitios web privados?			17%	83%
6	¿Tiene registradas automáticamente las contraseñas de sus sitios webs?			23%	77%
7	¿Usa contraseñas fuertes en sus sitios webs?			77%	23%
8	¿Sus contraseñas están cifradas al momento de ser ingresadas?			85%	15%
9	¿Ha perdido acceso a sus sitios webs después de ser víctima de hackers?			61%	39%
10	¿Almacena información sensible como datos personales en la web?			34%	66%
11	¿Utiliza datos de tarjetas de crédito en sitios webs?			60%	40%
12	¿Realiza compras en línea por medio de portales webs?			57%	43%
13	¿Ha Experimentado descargas de documentos no confiables en sitios webs?			12%	87%
14	¿Tiene servicio en la nube?			99%	1%
15	¿Realiza configuraciones adecuadas en los servicios que le ofrece la nube?			7%	93%
16	¿Experimenta fallos en inicio de sesión a sus sitios webs?			12%	88%
17	¿Su correo electrónico le informa sobre un intento de vulnerabilidad?			69%	31%
18	¿Utiliza métodos de seguridad que le permita identificar actividades sospechosas?			60%	40%
19	¿Los sitios webs que utiliza le informa en tiempo real sobre un ataque realizado?			54%	46%
20	¿Los sitios webs que utiliza detectan cuentas sospechosas?			76%	24%
21	¿Las aplicaciones que utiliza se bloquean momentáneamente si intentan acceder de manera inadecuada?			60%	40%
22	¿Han eliminado o modificado información importante compartida en sus sitios webs?			68%	32%
23	¿Los sitios webs que utiliza son seguros?			74%	26%
24	¿Sus sitios webs utilizan estándares de verificación de seguridad?			64%	36%
25	¿Ha recibido información dañina por medio de sus sitios webs?			12%	88%
26	¿Ha descargado documentos de sospechosa procedencia de sitios webs?			28%	72%
27	¿Utiliza rotación de contraseñas en sus sitios webs?			89%	11%
28	¿Los sitios webs que utiliza le informa si su contraseña es fuerte o débil?			99%	1%
29	¿Los sitios webs que utiliza, gestiona protección de seguridad automática?			36%	64%
30	¿Mantiene sesión iniciada de sus sitios web en computadores personales?			13%	87%
31	¿Sus equipos informáticos están en constante uso?			18%	82%
32	¿Sus equipos informáticos tienen usuario y contraseña de inicio de sesión?			89%	11%
33	¿Sus equipos cuentan con antivirus instalados?			89%	11%
34	¿Tiene contraseñas grabadas en sus computadores en documentos de texto?			22%	78%
35	¿Las sesiones en su navegador tienen tiempo de caducidad?			66%	34%
36	¿Ha cambiado, o deshabilitado, las contraseñas de sus cuentas predeterminadas?			31%	69%
37	¿Permiten que personas particulares utilicen sus equipos informáticos?			65%	35%
38	¿Verifica la identidad digital del remitente de una comunicación?			61%	39%
39	¿Verifica que las sesiones se invalidan cuando cierra la sesión?			82%	18%
40	¿Posee cuentas en sitios webs que ya no utilice?			34%	66%
41	¿Ha sido víctima de robo de cuentas en redes sociales?			70%	30%
42	¿Comparte claves de sitios webs con otras personas?			66%	34%
43	¿Ha cambiado su contraseña en los sitios webs que utiliza?			80%	20%
44	¿Con que frecuencia cambia sus contraseñas?			84%	16%
45	¿Su contraseña tiene 8 caracteres o más?			80%	20%
46	¿Combina letras, números y caracteres en sus contraseñas?			82%	18%
47	¿Ha perdido la contraseña de acceso a sus sitios webs?			90%	10%
48	¿Recuperó con facilidad la contraseña de acceso a sus sitios webs?			47%	53%

Ilustración 3: Tabulación de cuestionario - Seguridad Web

NRO.	PREGUNTA	Si	No
	Administrador del sistema informático		
1	¿Recupera usted contraseñas de acceso a sitios webs?	1	0
2	¿Indica a los estudiantes como recuperar sus contraseñas?	1	0
3	¿Monitorea inicios de sesión inadecuados?	0	1
4	¿Almacena sus contraseñas de administrador en su pc personal?	1	0
5	¿Almacena sus contraseñas de administrador en agendas?	1	0
6	¿Actualiza constantemente sus contraseñas?	1	0
7	¿Sus contraseñas tienen 8 caracteres o más?	1	0
8	¿Combina letras, números y caracteres en sus contraseñas?	1	0
9	¿Personas particulares tienen acceso a su pc personal?	0	1
10	¿Su pc personal tiene usuarios de invitado para personas particulares?	0	1
11	¿Su pc personal cuenta con usuario y contraseña para inicio de sesión?	1	0
12	¿Administra servidores de la universidad?	0	1
13	¿Escanea puertos de acceso a internet?	0	1
14	¿Minimiza vulnerabilidades en los puertos de internet?	1	0
15	¿Configura bloqueos de acceso a puertos de internet?	0	1
16	¿Monitorea uso indebido de navegación en internet?	0	1
17	¿Capacita a estudiantes para que no sean víctimas de ataques informáticos?	1	0
18	¿Tiene medidas de seguridad que protegen la información de los servidores?	0	1
19	¿Cuenta con antivirus para los servidores?	1	0
20	¿Cuenta con informe en tiempo real si está siendo víctima de un ataque informático?	0	1
21	¿Bloquea cuentas sospechosas?	0	1

Ilustración 4: Tabulación de cuestionario - administrador del sistema informático

Con la tabulación de los instrumentos aplicados a la comunidad estudiantil de la planta central de la ULEAM El Carmen y al administrador del sistema informático de la misma, se ha llegado a la determinación que en su mayoría los usuarios de sitios y aplicaciones web guardan por defecto sus contraseñas en dispositivos informáticos personales, los cuales son manipulados por ellos o por familiares dejando en claro que personas particulares no tienen autorización de utilizarlos.

Las contraseñas guardadas automáticamente en dispositivos personales dificultan el acceso desde otro lugar a los sitios webs (computadores de la universidad, por ejemplo) ya que al no recordar su contraseña y al no mantener una actualización periódica de la misma conlleva la dificultad de tener a la mano siempre su computadora personal o sus dispositivos móviles.

Muchos de las personas a quien se les aplicó el instrumento de seguridad en sitios webs hicieron referencias que una de las desventajas de utilizar las redes inalámbricas de la universidad es la velocidad de navegación debido que al momento de ingresar a sus plataformas digitales tienden a demorar en el tiempo de respuesta, también mencionaron que el uso que ciertos estudiantes le dan a las redes inalámbricas es el inadecuado ya que tienden a utilizar el internet para actividades de entretenimiento (juegos en línea).

Por otra parte, el administrador del sistema informático mencionó que hace unos años podía realizar algunas configuraciones en cuanto a seguridad en la navegación se refiere, pero que en la actualidad presta sus servicios como un asistente ya que todo el sistema es manejado por los directivos de la universidad directamente desde la matriz radicada en la ciudad de Manta.

En cuanto a la solicitud de recuperación de contraseñas de sitios web, el administrador del sistema informático utiliza sus conocimientos para solventar la necesidad de estudiantes, maestros y personal administrativos al momento que lo requieran, además asesora a cada uno de ellos en la parte técnica para que realicen configuraciones en sus portales digitales y no sean víctimas de delitos informáticos. Cabe recalcar que también les explica que no deben manipular documentos, enlaces, publicidad, y descargas de archivos de sitios sospechosos.

Por último, el administrador del sistema informático mencionó que sus funciones radican en mantener funcionando las redes e instalaciones físicas que se encuentran dentro de las instalaciones de la universidad, siendo estos laboratorios de cómputo, conectores a punto de internet en cada aula, computadores de biblioteca y demás instalaciones físicas que requieran de su atención, mientras que la parte lógica es monitoreada, manipulada y administrada por el departamento informático de la matriz.

3.7.5 Hallazgos

En la auditoria informática realizada en la ULEAM Extensión El Carmen (planta central) específicamente a las redes inalámbricas y los sitios web que utilizan los estudiantes, personal docente y administrativo, se le adjunto el análisis de una herramienta cuya funcionalidad radica en escanear puertos de internet y encontrar vulnerabilidades que pueden ser utilizados por terceros para materializar ataques y delitos informáticos que perjudiquen la veracidad y la integridad de la información que se almacena en la universidad. En la siguiente ficha de observación podemos encontrar las principales causas y vulnerabilidades encontradas por la herramienta Nessus.

3.7.6 Fichas de observación

Nombre de la institución: ULEAM Extensión El Carmen	
Nro. De observación: 1	**Periodo sujeto a revisión:** 1er día
Nombre del informe de auditoría: Escaneo de red básico	
Calificación de la observación **Alta (x)** **Media ( )** **Baja ( )**	
Descripción de la observación: Escaneo básico de redes inalámbricas y puertos de conexión a internet mediante herramienta Nessus.	
Fundamento específico legal y/o técnico: Escáner local • Puerto 1111 • Puerto 9876	
Causas: • Puertos de internet medio abiertos • Servicios rotos	
Efectos: • Causa problemas en el Firewall • Conexiones no cerradas de destino remoto	
Recomendaciones **Correctivas:** • Proteger objetivo con filtro IP • Consolidar las direcciones MAC en una lista única. **Preventivas:** • Cada dirección MAC debe comenzar con un identificador organizacional único (OUI) • Calcular el tiempo de actividad del host remoto	

Tabla1: Nessus - Prueba de escaneo básico (red Estudiantes)
Elaborado por: Jonathan Delgado Basurto
Anexo: 1

Nombre de la institución: ULEAM Extensión El Carmen	
Nro. De observación: 2	**Periodo sujeto a revisión:** 2do día
Nombre del informe de auditoría: Escaneo avanzado	
Calificación de la observación **Alta (x)** **Media ( )** **Baja ( )**	
Descripción de la observación: Escaneo avanzado de redes inalámbricas y puertos de conexión a internet mediante herramienta Nessus.	
Fundamento específico legal y/o técnico: Escáner local	
Causas:	
Efectos:	
Recomendaciones **Correctivas:** **Preventivas:** No se encontró ningún tipo de vulnerabilidad en el análisis avanzado.	

Tabla 2: Nessus - Prueba de escaneo avanzado (red Estudiantes)
Elaborado por: Jonathan Delgado Basurto
Anexo: 2

Nombre de la institución: ULEAM Extensión El Carmen	
Nro. De observación: 3	**Periodo sujeto a revisión:** 3er día
Nombre del informe de auditoría: Detección de Badlock	
Calificación de la observación **Alta (** x **)** **Media ( )** **Baja ( )**	
Descripción de la observación: Detección de Badlock, es un error de seguridad que afecta a protocolos remotos.	
Fundamento específico legal y/o técnico: Escáner local	
Causas:	
Efectos:	
Recomendaciones **Correctivas:** **Preventivas:** No se encontró ningún tipo de vulnerabilidad en la detección de Badlock.	

Tabla 3: Nessus - Detección de Badlock (red Estudiantes)
Elaborado por: Jonathan Delgado Basurto
Anexo: 3

Nombre de la institución: ULEAM Extensión El Carmen	
Nro. De observación: 4	**Periodo sujeto a revisión:** 4to día
Nombre del informe de auditoría: Choque de Detección Shellshock	
Calificación de la observación **Alta (** x **)** **Media ( )** **Baja ( )**	
Descripción de la observación: El cheque de detección Shellshock es un intérprete de comandos del sistema	
Fundamento específico legal y/o técnico: Escáner local	
Causas:	
Efectos:	
Recomendaciones **Correctivas:** **Preventivas:** No se encontró ningún tipo de vulnerabilidad en la detección de Shellshock	

Tabla 4: Nessus - Detección Shellshock (red Estudiantes)
Elaborado por: Jonathan Delgado Basurto
Anexo: 4

Nombre de la institución: ULEAM Extensión El Carmen	
Nro. De observación: 5	**Periodo sujeto a revisión:** 5to día
Nombre del informe de auditoría: Detección de DROWN	
Calificación de la observación **Alta (x)** **Media ( )** **Baja ( )**	
Descripción de la observación: El análisis de detección DROWN es una vulnerabilidad en protocolos cruzados que tiende afectar los servidores	
Fundamento específico legal y/o técnico: Escáner local	
Causas:	
Efectos:	
Recomendaciones **Correctivas:** **Preventivas:** No se encontró ningún tipo de vulnerabilidad en la detección DROWN	

Tabla 5: Nessus - Detección de DROWN (red Estudiantes)
Elaborado por: Jonathan Delgado Basurto
Anexo: 5

Nombre de la institución: ULEAM Extensión El Carmen	
Nro. De observación: 6	**Periodo sujeto a revisión:** 6to día
Nombre del informe de auditoría: Descubrimiento de Host	
Calificación de la observación **Alta (x)** **Media ( )** **Baja ( )**	
Descripción de la observación: El descubrimiento de host es una vulnerabilidad que se la realiza a través del sondeo de ping y solicitudes realizados a los servidores.	
Fundamento específico legal y/o técnico: Escáner local	
Causas:	
Efectos:	
Recomendaciones **Correctivas:** **Preventivas:** No se encontró ningún tipo de vulnerabilidad en Descubrimiento de Host	

Tabla 6: Nessus - Descubrimiento de Host (red Estudiantes)
Elaborado por: Jonathan Delgado Basurto
Anexo: 6

Nombre de la institución: ULEAM Extensión El Carmen	
Nro. De observación: 7	**Periodo sujeto a revisión:** 7mo día
Nombre del informe de auditoría: Derivación de seguridad Intel AMT	
Calificación de la observación **Alta (** x **)** **Media ( )** **Baja ( )**	
Descripción de la observación: La vulnerabilidad Intel AMT es aquella que se materializa para apoderarse de la administración remota de los servidores incluido el sistema operativo	
Fundamento específico legal y/o técnico: Escáner local	
Causas:	
Efectos:	
Recomendaciones **Correctivas:** **Preventivas:** No se encontró ningún tipo de vulnerabilidad en Derivación de seguridad Intel AMT	

Tabla 7: Nessus - Derivación de seguridad Intel AMT (red Estudiantes)
Elaborado por: Jonathan Delgado Basurto
Anexo: 7

Nombre de la institución: ULEAM Extensión El Carmen	
Nro. De observación: 8	**Periodo sujeto a revisión:** 8vo día
Nombre del informe de auditoría: Escaneo de red básico	
Calificación de la observación **Alta (** x **)** **Media ( )** **Baja ( )**	
Descripción de la observación: Escaneo básico de redes inalámbricas y puertos de conexión a internet mediante herramienta Nessus.	
Fundamento específico legal y/o técnico: Escáner local • Puerto 445 • Puerto 49664 • Puerto 135 • Puerto 49665 • Puerto 49666 • Puerto 49667 • Puerto 49668 • Puerto 49670	
Causas: • Ataques “Man in the Middle” • Acceso compartido a archivos y dispositivos	
Efectos: • Solicitudes RPC a puertos vulnerables • Obtención del nombre y versión del sistema operativo remoto	
Recomendaciones **Correctivas:** • Firmas de mensajes en la configuración de Host • Configurar con clave pública el host remoto • Bloqueo de vulnerabilidades SMB. • Registre errores de control de acceso. **Preventivas:** • Firmar digitalmente las configuraciones del host • Firmar el servidor • Limitar tasa de acceso a los servidores	

Tabla 8: Nessus - Escaneo básico de red (red Estudiantes)
Elaborado por: Jonathan Delgado Basurto
Anexo: 8

Nombre de la institución: ULEAM Extensión El Carmen	
Nro. De observación: 9	**Periodo sujeto a revisión:** 7mo día
Nombre del informe de auditoría: Escaneo de red básico	
Calificación de la observación **Alta (x)** **Media ( )** **Baja ( )**	
Descripción de la observación: Escaneo básico de redes inalámbricas y puertos de conexión a internet mediante herramienta Nessus.	
Fundamento específico legal y/o técnico: Escáner local	
Causas:	
Efectos:	
Recomendaciones **Correctivas:** **Preventivas:** No se encontró ningún tipo de vulnerabilidad en Derivación de seguridad Intel AMT	

Tabla 9: Nessus - Escaneo básico de red (red Uleam.Funcionarios)
Elaborado por: Jonathan Delgado Basurto
Anexo: 9

Nombre de la institución: ULEAM Extensión El Carmen	
Nro. De observación: 10	**Periodo sujeto a revisión:** 7mo día
Nombre del informe de auditoría: Escaneo avanzado	
Calificación de la observación **Alta (x)** **Media ( )** **Baja ( )**	
Descripción de la observación: Escaneo avanzado de redes inalámbricas y puertos de conexión a internet mediante herramienta Nessus.	
Fundamento específico legal y/o técnico: Escáner local	
Causas:	
Efectos:	
Recomendaciones **Correctivas:** **Preventivas:** No se encontró ningún tipo de vulnerabilidad en Derivación de seguridad Intel AMT	

Tabla 10: Nessus - Escaneo avanzado (red Uleam.Funcionarios)
Elaborado por: Jonathan Delgado Basurto
Anexo: 10

Ilustración 5: Análisis de seguridad en contraseñas

Elaborado por: Jonathan Delgado Basurto

Interpretación. El análisis de seguridad a las aplicaciones web mediante la metodología OWASP se llevó a cabo ejecutando la herramienta WebGoat perteneciente a la misma metodología, con la cual se analizó la seguridad de las contraseñas en sitios web. Como se muestra en la ilustración la clave de acceso a un correo electrónico (a9z1ez) presenta una combinación de números y letras, pero el análisis demuestra que es una contraseña débil ya que como mínimo debe estar compuesta por 8 dígitos. Lo recomendable es que se combinen caracteres entre números, letras y signos intercalando mayúsculas y minúsculas cumpliendo con los protocolos de seguridad.

Ilustración 6: Resultados de seguridad en contraseñas

Elaborado por: Jonathan Delgado Basurto

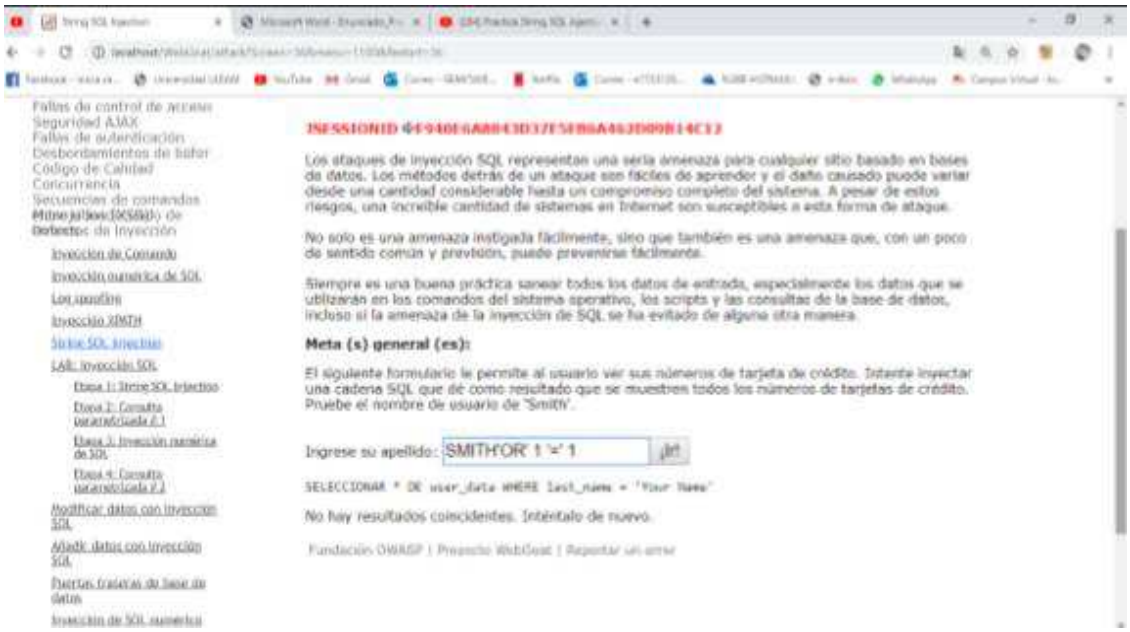


Ilustración 7: Ataque de inyección
Elaborado por: Jonathan Delgado Basurto

Interpretación. A continuación, se muestra un intento de inyección en código SQL a través de la herramienta WebGoat, tratando de insertar una búsqueda en bases de datos con la sentencia SELECT, se obtuvo como respuesta un acceso denegado, es decir que fue bloqueado el ataque de inyección SQL por parte de los protocolos de seguridad que se implementan en la universidad.

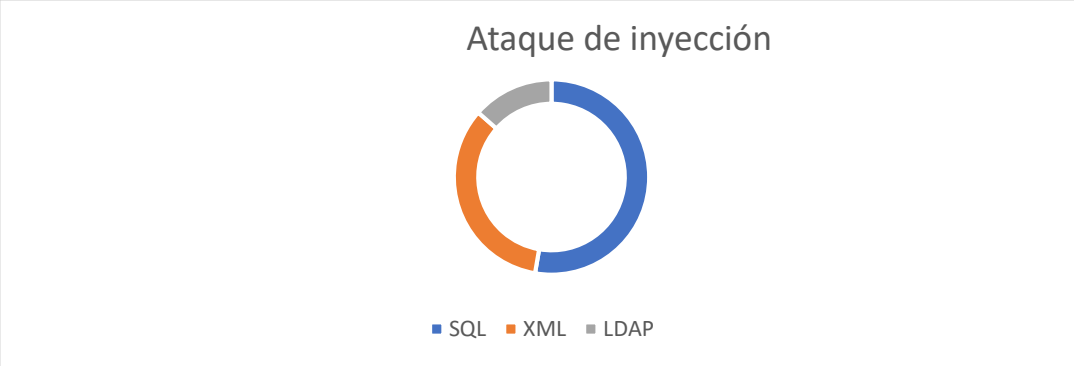


Ilustración 8: Análisis de ataques
Elaborado por: Jonathan Delgado Basurto

Interpretación. En el análisis realizado se puede interpretar que cualquier fuente que almacene datos puede ser atacado por la inyección de código malicioso, entre ellos los entornos web, la cual puede causar divulgación de información o denegación de acceso cuya solución más equivalente es evitar el uso de intérpretes con el uso de herramientas de mapeo relacional de objetos (ORMs).

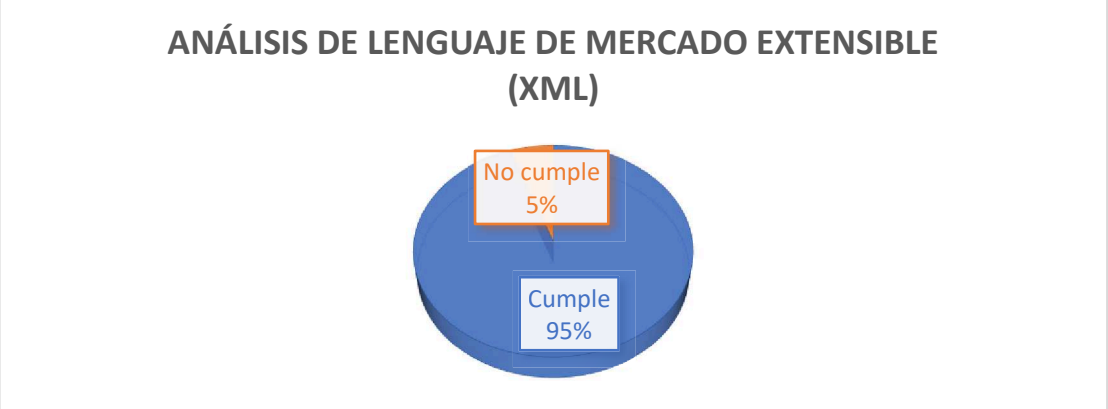


Ilustración 9: Análisis XML
Elaborado por: Jonathan Delgado Basurto

Interpretación. Se puede visualizar en el gráfico que el nivel de seguridad para los ataques de este tipo a las aplicaciones web, presentan una efectividad del 95%, las vulnerabilidades de este tipo se pueden utilizar para extraer datos de un almacenamiento, aplicar sentencias o solicitudes a servidores como también para el escaneo de sistemas internos. Una de las soluciones de mayor eficiencia es deshabilitar entidades de tipo XML externas y analizadores sintácticos adyacentes en las aplicaciones que utiliza.

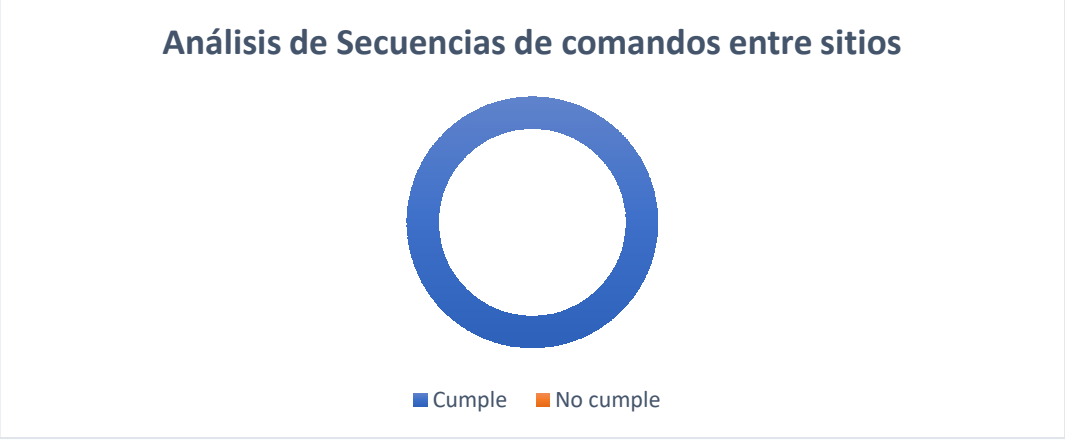


Ilustración 10: Análisis XSS
Elaborado por: Jonathan Delgado Basurto

Interpretación. Con la efectividad del 100% se demuestra que las vulnerabilidades de java Script están controladas en su totalidad en las aplicaciones web de la ULEAM Extensión en El Carmen, bloqueando todo tipo solicitud maliciosa que pretenda materializar ataques de este tipo.

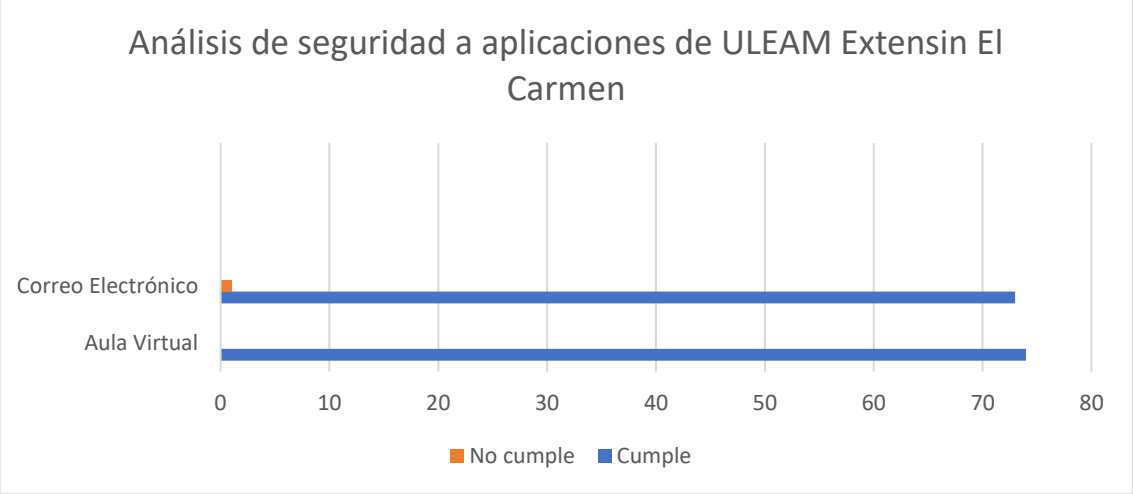


Ilustración 11: Resultados de análisis
Elaborado por: Jonathan Delgado Basurto

Interpretación. El análisis de seguridad que se realizó refleja que el aula virtual de la universidad es un sitio protegido que cumple con los protocolos de seguridad por la cual circulan tráficos de información sensible, como notas, documentos, informes, artículos, entre otros. En lo que respecta al correo electrónico de los usuarios (estudiantes) en su mayoría presentan vulnerabilidades en las contraseñas.

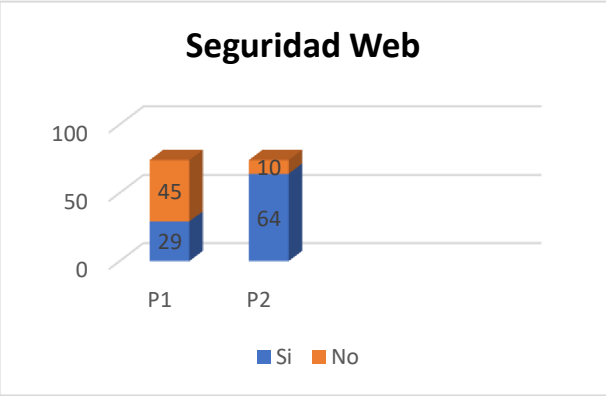


Ilustración 12: Control de seguridad web y cumplimiento de políticas.
Autor: Jonathan Delgado Basurto

Interpretación. En los resultados que se han obtenido mediante la aplicación del cuestionario a los estudiantes de la universidad se puede demostrar que en ciertas ocasiones han ingresado datos importantes en sitios web clonados que capturan información ingresada por teclado manejándose en un rango de baja magnitud mientras utilizan el internet de la Extensión universitaria, por otra parte, hacen referencia que mientras utilizan las redes inalámbricas se puede

evidenciar publicidad no deseada en sus sitios web. Uno de los principales inconvenientes que se presentan en cuanto a la seguridad de una aplicación, son los datos suministrados por el usuario siendo estos de forma errónea o se duplica la información mediante el método de inyección, mientras que su inmediata solución es la de utilizar API segura que monitoree, escanee y minimice a los intérpretes de datos además de realizar validaciones al ingreso de datos a los servidores.

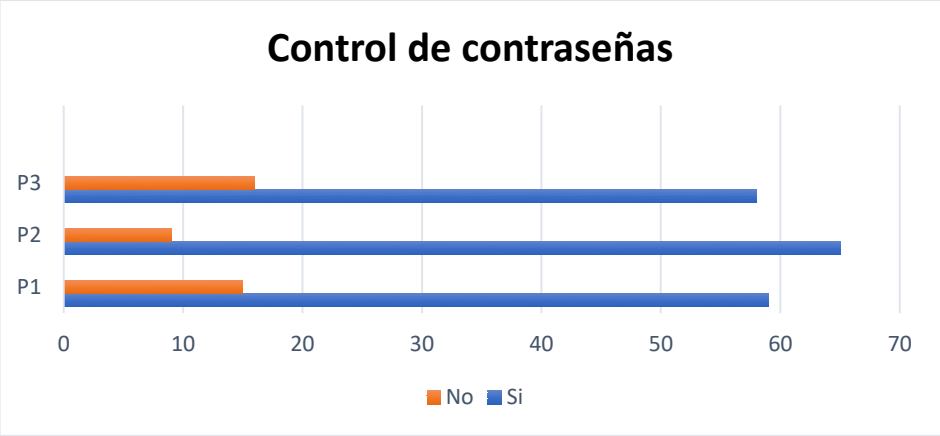


Ilustración 13: Seguridad en contraseñas de sitios Web
Autor: Jonathan Delgado Basurto

Interpretación. Con la aplicación de los cuestionarios se puede identificar que algunas personas almacenan sus contraseñas en los sitios web que utilizan para que de esta manera al momento de abrir la página el usuario no tenga la necesidad de ingresar usuario y contraseñas, se puede deducir que existe un incumplimiento en la seguridad de sus sitios web ya que cualquier persona que tenga acceso a sus dispositivos personales podrían manipular la información que contenga almacenada.

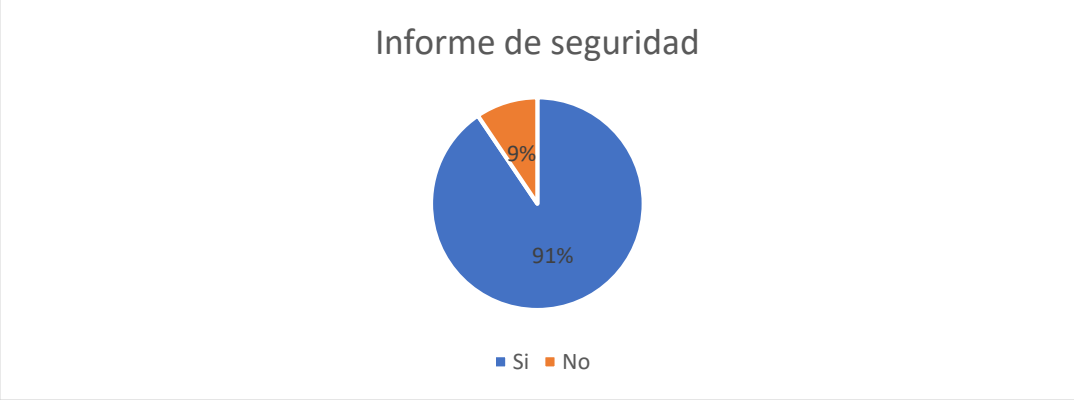


Ilustración 14: Informe de control se seguridad
Autor: Jonathan Delgado Basurto

Interpretación. Como se observa en el gráfico en mayoría los encuestados mencionan que la protección que brindan los sitios web, como correo electrónico aplican medidas de seguridad que les notifica si alguien intenta acceder desde otro dispositivo además de bloquearse si es necesario hasta que el propietario de dicha cuenta la habilite, mientras que otros sitios experimentan una falta mínima de seguridad en cuanto a acceso y bloqueo de ingreso.

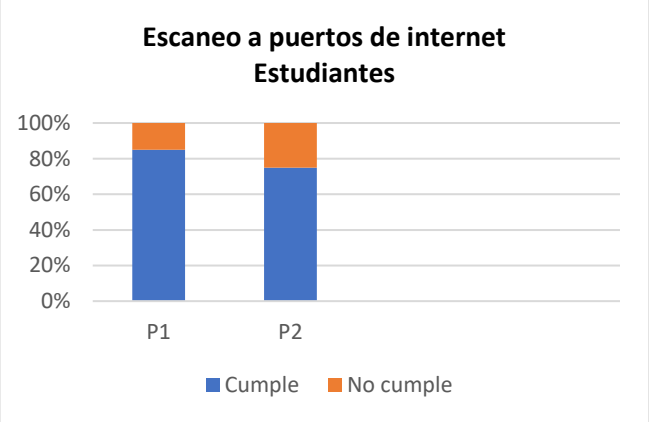


Ilustración 15: Análisis de red básico mediante Nessus
Autor: Jonathan Delgado Basurto

Interpretación. Con la aplicación de la herramienta Nessus se ha podido determinar que existen riesgos de seguridad de baja magnitud en ciertos puertos de internet mencionados en la tabla de observación (número uno), ya que solo consistía en información que la herramienta brindaba al usuario junto con las posibles soluciones que se podía aplicar para solventar el riesgo encontrado.

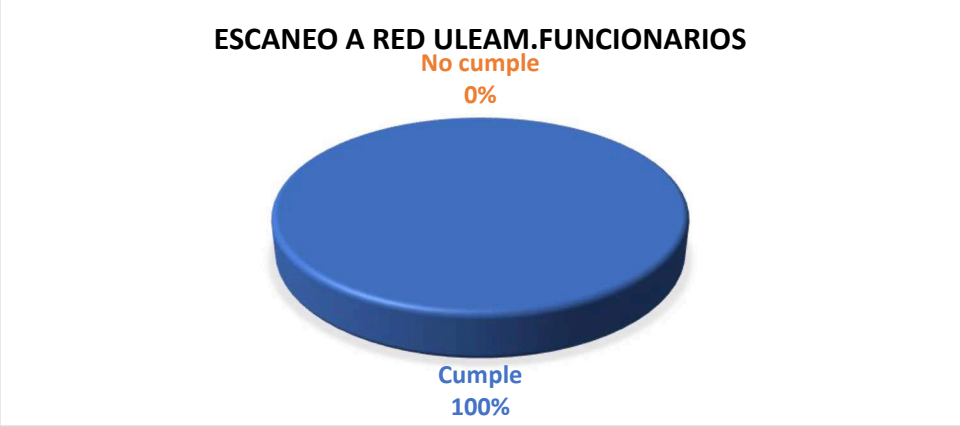


Ilustración 16: Análisis Nessus de re Uleam.Funvionarios
Autor: Jonathan Delgado Basurto

Interpretación. En el análisis aplicado a la red inalámbrica Uleam.Funcionarios, se puede constatar que no existe algún tipo de riesgo, la herramienta Nessus mediante escaneos básicos y avanzados a la red, no ha determinado problemas de vulnerabilidad y posibilidad de riesgo ya que utiliza seguridad de puerto cautivo cuya función es vigilar el tráfico de HTTP, obligando a cada usuario de esta red a pasar por filtros de vigilancia negando la navegación de internet hasta que el mismo se autentifique, el mismo sistema de seguridad hará que se caduque la sesión después de un periodo de tiempo.

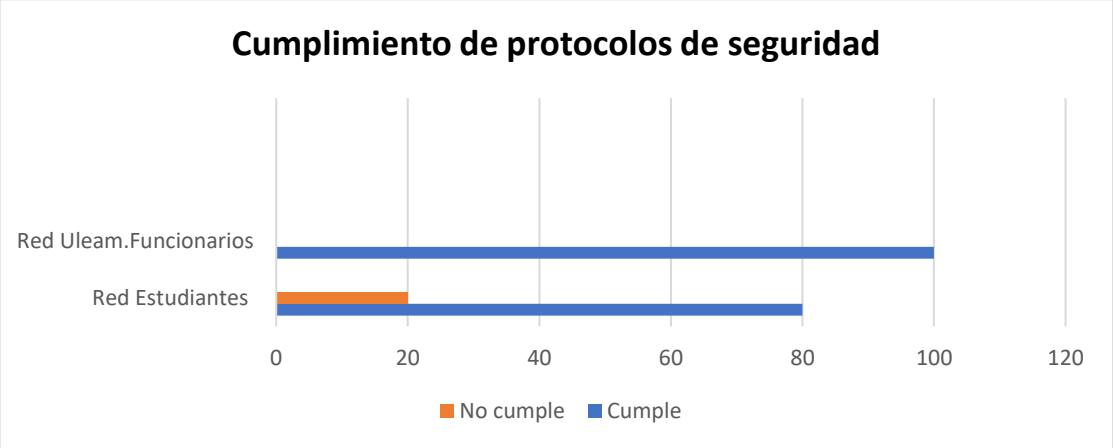


Ilustración 17: Cumplimiento de protocolos de seguridad
Autor: Jonathan Delgado Basurto

Interpretación. Con la ejecución de la herramienta Nessus se pudo constatar que la red utilizada por los docentes de la universidad denominada Uleam.Funcionarios cumple con los protocolos de seguridad, mientras que la red denominada Estudiantes la cual es de uso público presenta riesgos de menor grado.

3.7.7 Opinión

Después de analizar cada una de las pruebas realizada mediante la herramienta Nessus se ha llegado a la conclusión que algunos de los test aplicados a las redes inalámbricas de la universidad fueron de categoría nulo, es decir que no presentaron vulnerabilidades en cuanto a seguridad lógica se refiere obteniendo resultados en cero acerca de algún tipo de riesgo que puedan facilitar el ingreso de intrusos a la red y cometer actos delictivos.

Opinión objetivo uno.

Con la ejecución de la herramienta WebGoat perteneciente a la metodología OWASP, se puede concluir que los ataques llevados a cabo fueron bloqueados satisfactoriamente por los protocolos de seguridad que rigen en la universidad, mientras que los análisis de seguridad en contraseñas arrojaron en sus informes algunos inconvenientes, el más común de todas contraseñas débiles que los usuarios utilizan en sus sitios web. En fin, el análisis de seguridad en aplicaciones web cumplen en un 90% los protocolos de seguridad.

Opinión objetivo dos.

Se puede concluir que la red inalámbrica de la ULEAM Extensión en El Carmen llamada Uleam.Funcionarios no presenta vulnerabilidades, mientras que la red llamada Estudiantes presenta ciertos tipos de inconvenientes menores que pueden ser corregidos como indican las fichas de observación, gracias a la herramienta Nessus se pudo detectar los riesgos a las que se exponen las redes y las soluciones tanto correctivas como preventivas que se pueden implementar para resolver las inseguridades encontradas.

Conclusiones de informe de auditoría.

- Finalizada la auditoría en análisis de seguridad a aplicaciones web y a redes inalámbricas de ULEAM Extensión en El Carmen se puede constatar que en promedio de seguridad se cumple con un 90%, basados en sistemas como puerto cautivo, firewall, y antivirus que bloquean intentos sospechosos dentro de la universidad.

- Basados en las herramientas utilizadas para llevar a cabo el análisis de seguridad y con los hallazgos encontrados, se puede concluir que la Extensión universitaria en cuestiones de vulnerabilidades y riesgos informáticos se encuentra protegida.

Recomendaciones de informe de auditoría.

- Con el evidenciado avance de la tecnología en la época actual se debe tener en consideración los resultados obtenidos en los análisis de seguridad y en las soluciones planteadas en las fichas de observación para que así exista un control total de los riesgos y vulnerabilidades a las que se encuentra expuesta las aplicaciones web y las redes inalámbricas de la ULEAM Extensión en El Carmen

CONCLUSIONES

- La auditoría informática de seguridad web es de vital importancia en estos tiempos para las empresas cuya visión sea crecer en el futuro, ya que tiende a proveer métodos y técnicas de control de riesgos, además de ofrecer respaldos de información, en este mundo globalizado los ataques informáticos son muy comunes en la vida diaria, cada uno de ellos van dirigidos a los sitios donde los usuarios son mayormente vulnerables, la web.
- Controlar y evaluar de forma permanente la seguridad en aplicaciones web ya que son ellas lo medios por el cual se envían miles de información y datos esenciales para una organización, los atacantes dependen en su gran mayoría de la falta de monitoreo y respuesta inmediata para lograr su objetivo final sin dejar ningún tipo de rastro o señal del acto ilícito materializado.
- Utilizando herramientas como WebGoat se pudo verificar los protocolos de seguridad en el aula virtual que utiliza la universidad, mientras que Nessus cumplió la función de analizar las redes inalámbricas (Estudiantes, y Uleam.Funcionarios) obteniendo resultados beneficiosos en cuanto a las soluciones a seguir que proporciona la herramienta.
- Cada uno de los instrumentos utilizados para esta auditoría fueron de vital importancia, cuyas herramientas permitieron conocer resultados acerca del análisis de riesgos y vulnerabilidades, llegando a concluir que s e mantiene un estricto control de seguridad en las redes inalámbricas y aplicaciones web desde la matriz de la universidad en la ciudad de Manta.

RECOMENDACIONES

- Teniendo en cuenta el avance de la tecnología que se visualiza en estos tiempos modernos es correcto que las empresas e instituciones apliquen métodos y técnicas que le permitan mantener segura la información que poseen, para ello deben incluir herramientas de análisis estático como también aplicar pruebas dinámicas para identificar las vulnerabilidades a las que se exponen con sus sitios web.
- Es necesario tomar medidas de seguridad relacionados con la autenticación ya que poseer procesos de controles débiles exponen de forma significativa las credenciales de seguimiento a vulnerabilidades, para ello es necesario utilizar la autenticación multifactor que brinde la protección ante ataques no autorizados, además se debe utilizar un gestor de inicios de sesión al servidor generando ID dinámicos que se invaliden una vez cerrada la sesión.
- Teniendo en cuenta que se debe habilitar una política de seguridad de contenido ya que se trata de una defensa de manera segura en los actos de mitigación y minimización de vulnerabilidades encontradas, controlando la inyección de códigos maliciosos.
- Se debe verificar que se cumpla con los controles y normas de seguridad adecuadas, cuya finalidad sea garantizar la integridad y disponibilidad de la información, además de minimizar las vulnerabilidades que se presenten en clasificación de datos sensibles que no estén cifrados por la ausencia de controles de acceso en los servidores.
- Se deben realizar constantes evaluaciones en los sistemas de la universidad ya que la tecnología cambia, y a medida como avanza pueden aparecer nuevas herramientas para vulnerar la seguridad implementada.

BIBLIOGRAFÍA

Acevedo Ibáñez, , A., & López Martín, A. (2004). *El proceso de la entrevista: conceptos y modelos.* México: Limusa.

Aguilera López , P. (2010). *Seguridad informática.* Madrid: Editex.

Aguilera López, P. (2011). *Seguridad del hardware (Seguridad informática).* Editorial Editex.

Alegre Ramos, M., García , A., & Hurtado, C. (2011). *Seguridad Informática.* Madrid: Paraninfo S.A.

Andreu Gómez, J. (2011). *Redes inalámbricas (Servicios en red).* España: Editex.

Andreu, J. (2011). *Despliegue de cableado (Redes locales).* Editorial Editex.

Baca Urbina, G. (2016). *Introducción a la seguridad informática.* México: Grupo Editorial Patria.

Benchimol, D. (2012). *Hacking.* Buenos Aires: Users.

Broy de la Cruz, H. (2013). *HACKING & CRACKING.* Lima-Perú: Macro.

Cabello García, J. M. (2014). *Operaciones auxiliares con Tecnologías de la Información y la Comunicación .* IC Editorial.

Castro Gil, M., Díaz Orueta, G., Alzórriz Armendáriz , I., & Sancristobal Ruíz , E. (2014). *PROCESOS Y HERRAMIENTAS PARA LA SEGURIDAD DE REDES.* Madrid: Editorial UNED.

Cegarra Sánchez, J. (2012). *Los métodos de investigación.* Ediciones Díaz de Santos: Madrid.

Corral González, P. (2016). *Simulación de técnicas de diversidad y filtrado Kalman en redes inalámbricas.* España: Universidad Miguel Hernández.

Costas Santos, J. (2011). *Seguridad Informática (GRADO MEDIO).* RA-MA.

Del Peso Navarro, E. (2003). *Manual de outsourcing informático: (análisis y contratación).* Madrid: Ediciones Díaz de Santos.

Díaz Uretra , G., & Alonso Castro, M. (2014). *PROCESOS Y HERRAMIENTAS PARA LA SEGURIDAD DE REDES.* Madrid-España: Editorial UNED.

Domínguez, F. (2014). *Introducción a la Informática Forense.* Madrid: RA-Ma.

Dordoigne, J. (2015). *Redes informáticas - Nociones fundamentales.* Barcelona: Ediciones ENI.

Gallego, J. (2015). *Instalación y mantenimiento de redes para transmisión de datos.* Editex.

Gómez Vieites, Á. (2011). *Enciclopedia de la Seguridad Informática. 2ª edición.* Madrid: RA-MA.

González Río, M. D. (2016). *Tecnologías de Virtualización: 2ª Edición.* Campus Academy.

Hertzog, R., & Mas, R. (2016). *El manual del Administrador de Debian.* Barcelona: LULU.com.

Huaman Valencia , H. (2005). *MANUAL DE TECNICAS DE INVESTIGACION Conceptos y Aplicaciones.* Lima Perú: IPLADEES S.A.C.

Landean, R. (2007). *Elaboración de trabajos de investigación.* Caracas-Venezuela: Alfa.

Latorre Estrada, E. (1996). *Teoría general de sistemas aplicada a la solución integral de problemas.* Santiago de Cali: Universidad del Valle.

Marco Galindo, M., & Marco Simó, J. (2010). *Escaneando la informática.* Barcelona: Editorial UOC.

Marroquín, N. (2010). *Tras los pasos de un... Hacker.* Quito: NMC Research Cía Ltda.

Mora Pérez, P. (2017). *UF1347 - Instalación y configuración de los nodos de interconexión de redes privadas con publicas.* España: Editorial Elearning, S.L.

Moreno Pérez, J. C. (2014). *Mantenimiento del Subsistema Físico de Sistemas Informáticos.* Madrid: RA-MA.

Navarro Lacoba, R. (2014). *La guía exprés de redes.*

Rault, R., Schalkwijk, L., Agé, M., Crocfer, N., Crocfer, R., Dumas, D., . . . Lasson, S. (2015). *Seguridad informática - Hacking Ético.* Barcelona: Ediciones ENI.

Raya Cabrera , J. (2014). *Sistemas Informáticos (GRADO SUPERIOR).* Madrid: RA-MA.

Robles, F. J. (2014). *Redes locales.* RA-MA Editorial.

Rodríguez Ávila, A. (2007). *Iniciación a la Red de Internet.* Ideaspropias Editorial S.L.

Rodríguez Moguel, E. (2005). *Metodología de la Investigación.* México: Univ. J. Autónoma de Tabasco.

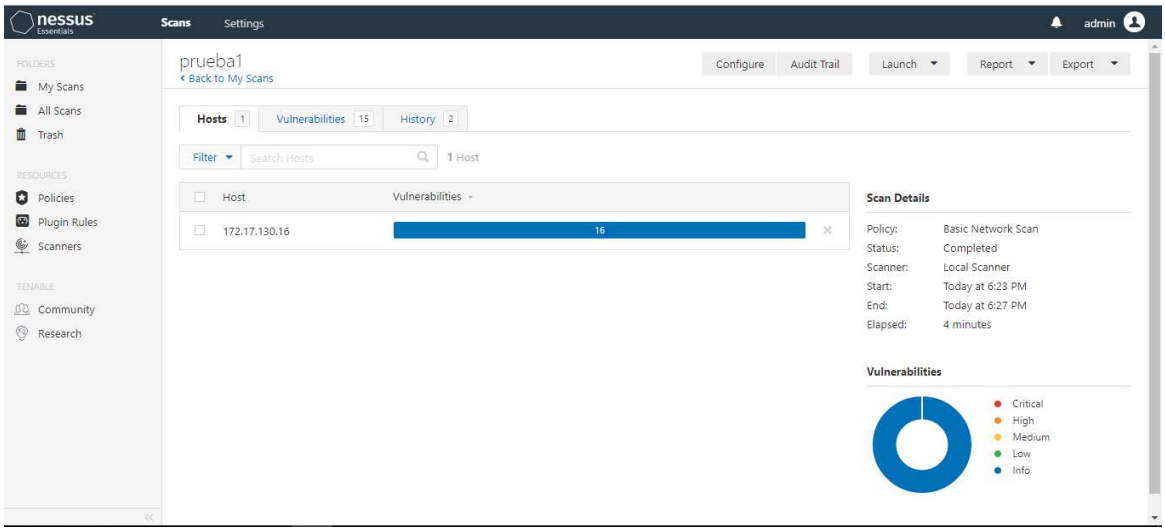
Romero Castro, M., & Figueroa Morán, G. (2018). *INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES.* Alicate-España: 3Ciencias.

Romero, M., & Barbancho Consejero , J. (2010). *Servicios en Red.* Madrid-España: Editorial Paraninfo.

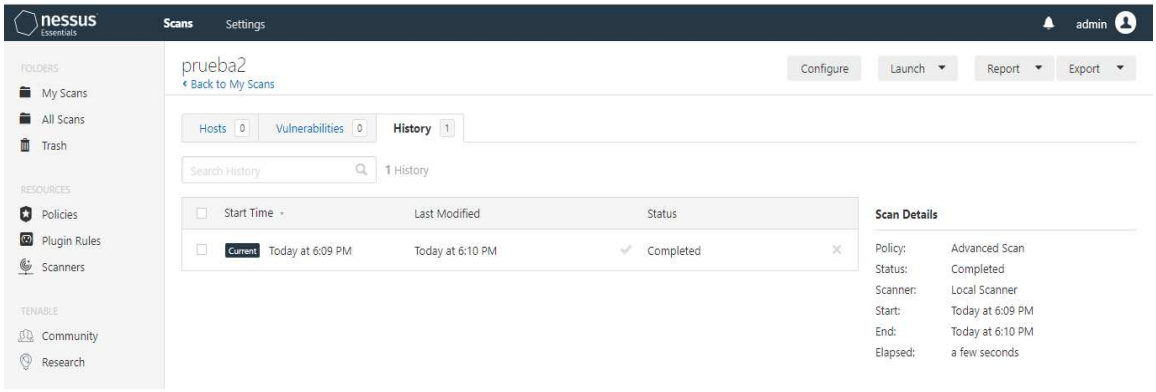
www.uleam.edu.ec. (2019). Obtenido de http://www.uleam.edu.ec/

Zabía de la Mata, J., & Agúndez Lería, I. (2008). *Protección de datos: comentarios al reglamento.* Valladolid: Lex Nova.

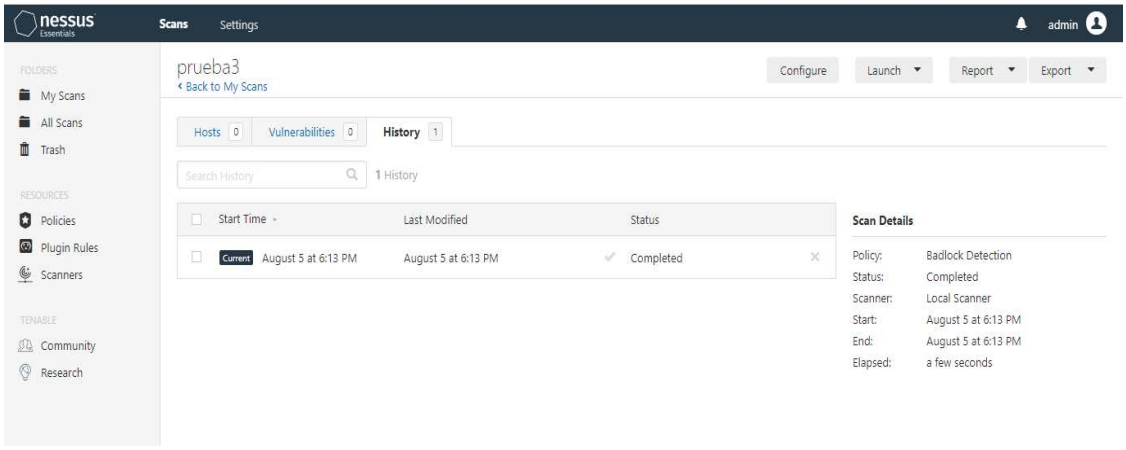
ANEXOS



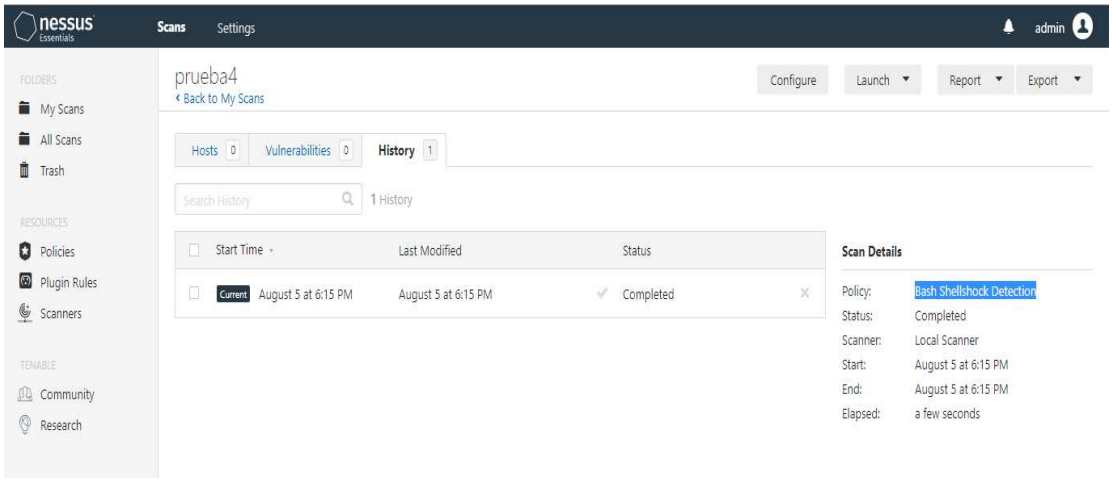
Anexo 1: Test - Prueba 1



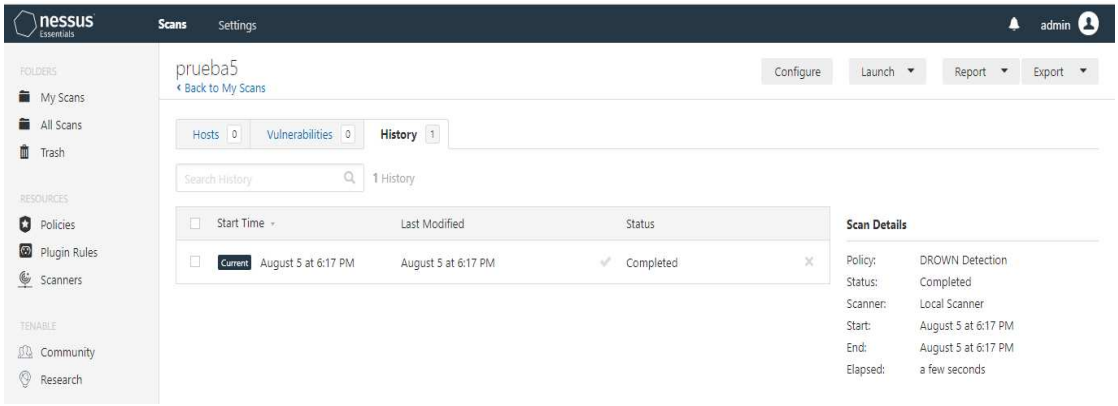
Anexo 2: Test - Prueba 2



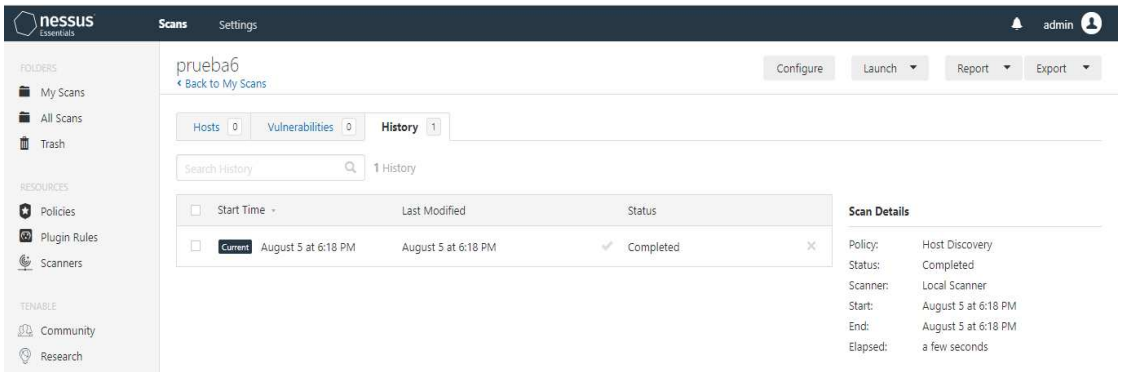
Anexo 3: Test - Prueba 3



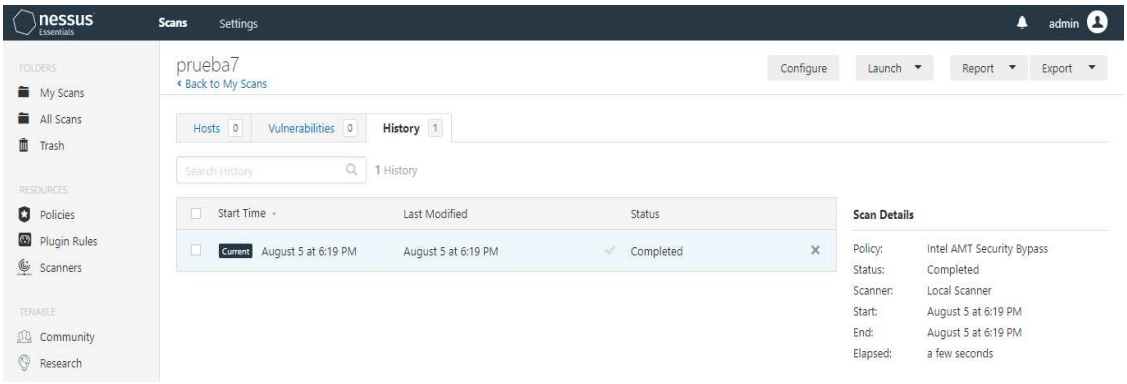
Anexo: Test - Prueba 4



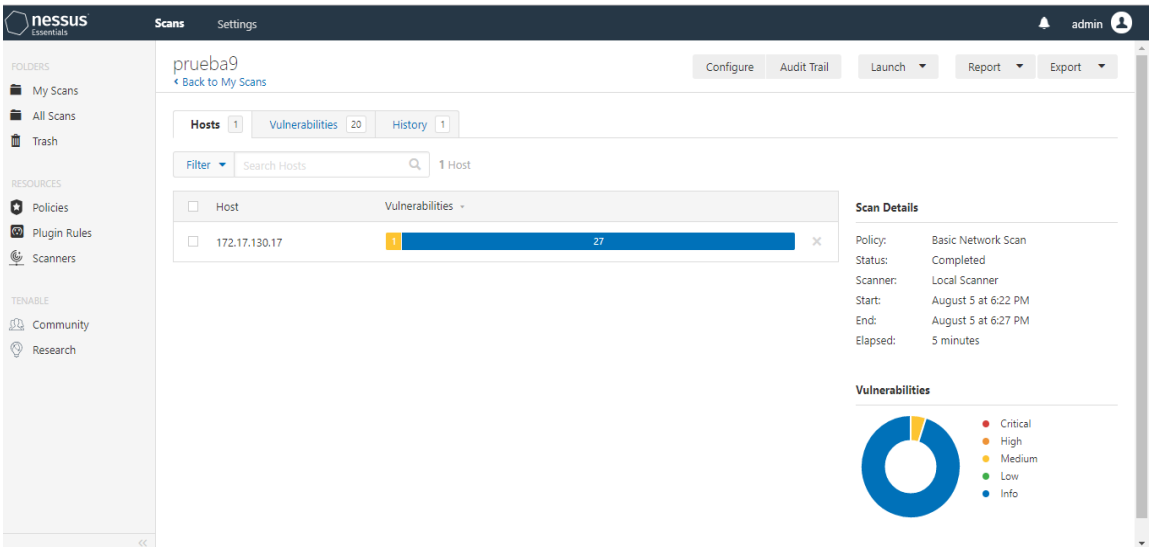
Anexo 5: Test - Prueba 5



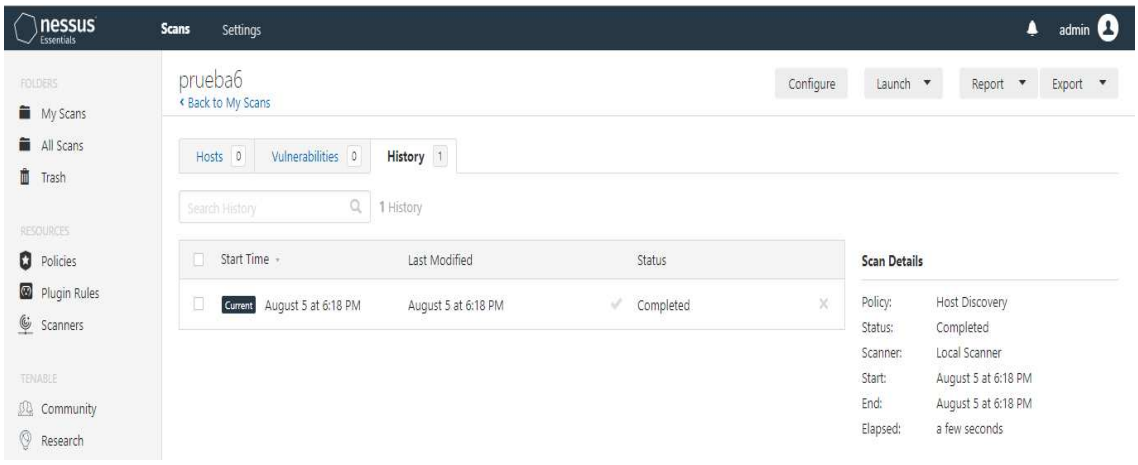
Anexo 6: Test - Prueba 6



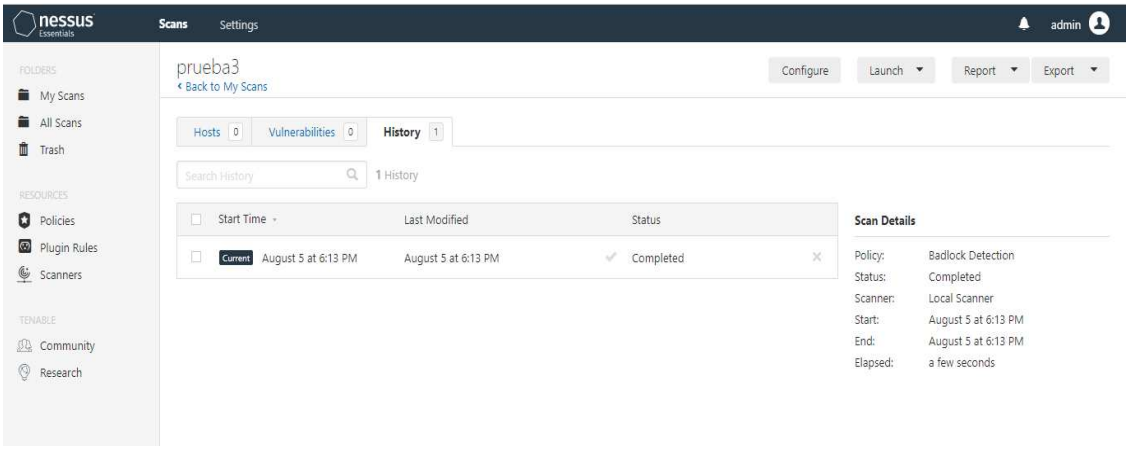
Anexo 7: Test - Prueba 7



Anexo 8: Test - Prueba 8



Anexo 9: Test - Prueba 9



Anexo 10: Test - Prueba 10

Uleam — UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ

Objetivo: Realizar entrevista sobre la seguridad en redes inalámbricas al administrador del área informática de la "Universidad Laica Eloy Alfaro de Manabí Extensión en El Carmen"

1. **¿Quién es el proveedor que presta servicios de internet a la universidad?**
2. **¿Por qué medio llega el internet a la universidad?**
3. **¿Existen tipos de redes WIFI, y cuales se implementan en las redes de la universidad?**
4. **¿Qué tipo de seguridad se implementan en las redes inalámbricas de la universidad?**
5. **¿Existe algún control en la navegación de internet en la universidad?**
6. **¿Los estudiantes tienen libre acceso a todo tipo de sitios web cuando utiliza las redes inalámbricas de la universidad?**
7. **¿Los sitios web de la universidad se encuentran protegidos, de qué manera?**
8. **¿Cómo gestiona el proveedor los riesgos de seguridad de la información?**
9. **¿Qué tipo de incidentes de seguridad son mitigados por usted?**
10. **¿Utiliza un Firewall para que la organización pueda identificar las susceptibilidades del sistema y también prevenir una invasión de hackers??**
11. **¿Ante un ataque informático llevado a cabo por hackers cuales son las primeras acciones que se toman?**
12. **¿Cuenta con las soluciones de seguridad adecuadas?**

Anexo 11: Entrevista dirigida al encargado del sistema informático

UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ

Objetivo: Realizar el diagnóstico sobre la seguridad en redes inalámbricas a los estudiantes, personal docente y administrativos de la "Universidad Laica Eloy Alfaro de Manabí Extensión en El Carmen"

1. **¿Utiliza usted las redes inalámbricas de la universidad?**
   SI ☐ **No** ☐

   Observación: Si su respuesta es no finalice, caso contrario continúe.
2. **¿Con que frecuencia utiliza las redes inalámbricas de la universidad?**
   1 a 2 horas ☐
   3 a 4 horas ☐
   Más de 5 horas ☐
3. **¿Usted cree que las redes inalámbricas de la universidad son seguras?**
   SI ☐ **No** ☐
4. **¿Ha ingresado a la banca móvil utilizando la red de la universidad?**
   SI ☐ **No** ☐
5. **¿Ingresa contraseñas importantes utilizando la red de la universidad?**
   SI ☐ **No** ☐
6. **¿Con que fin utiliza las redes inalámbricas de la universidad?**
   Estudios ☐
   Entretenimiento ☐
   Redes sociales ☐
   Otros, especifique: _____
7. **¿Qué tipo de aplicaciones utiliza cuando está en la universidad?**
   Correo ☐
   Aula virtual ☐
   Páginas webs informativas ☐
   Otros, especifique: _____
8. **¿Tiene libre acceso a todo tipo de páginas cuando utiliza las redes inalámbricas de la universidad?**
   SI ☐ **No** ☐
9. **¿Existe algún control en la navegación en la universidad?**
   SI ☐ **No** ☐
10. **¿Le gustaría contar con sistemas que protejan la información que usted envía mientras utiliza las redes de la universidad?**
    SI ☐ **No** ☐

Anexo 12: Encuesta dirigida a los Estudiantes

Ficha de observación

Nombre de la empresa:			
Nro. De observación	**Periodo sujeto a revisión**		
Nombre del informe de auditoria			
Calificación de la observación	**Alta( )**	**Media( )**	**Baja( )**
Descripción de la observación:			
Fundamento específico legal y/o técnico:			
Causas:			
Efectos:			
Recomendaciones Correctivas: **Preventivas:**			

Anexo 13: Formato ficha de observación

UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ

Cuestionario sobre políticas de seguridad				
Recuperación de datos				
Nro.	**PREGUNTA**	**SI**	**NO**	**OBSERVACIÓN**
1	¿Recupera usted contraseñas de acceso a sitios webs?			
2	¿Indica a los estudiantes como recuperar sus contraseñas?			
3	¿Monitorea inicios de sesión inadecuados?			
4	¿Almacena sus contraseñas de administrador en su pc personal?			
5	¿Almacena sus contraseñas de administrador en agendas?			
6	¿Actualiza constantemente sus contraseñas?			
7	¿Sus contraseñas tienen 8 caracteres o más?			
8	¿Combina letras, números y caracteres en sus contraseñas?			
9	¿Personas particulares tienen acceso a su pc personal?			
10	¿Su pc personal tiene usuarios de invitado para personas particulares?			
11	¿Su pc personal cuanta con usuario y contraseña para inicio de sesión?			
12	¿Administra servidores de la universidad?			
13	¿Escanea puertos de acceso a internet?			
14	¿Minimiza vulnerabilidades en los puertos de internet?			
15	¿Configura bloqueos de acceso a puertos de internet?			
16	¿Monitorea uso indebido de navegación en internet?			
17	¿Capacita a estudiantes para que no sean víctimas de ataques informáticos?			
18	¿Tiene medidas de seguridad que protegen la información de los servidores?			
19	¿Cuenta con antivirus para los servidores?			
20	¿Cuenta con informe en tiempo real si está siendo víctima de un ataque informático?			
21	¿Bloquea cuentas sospechosas?			
Realizado por: Delgado Basurto Jonathan				
Fecha: 30/07/2019				

Anexo 14: Instrumento aplicado al encargado de sistema informático

Cuestionario sobre políticas de seguridad				
Uso de aplicaciones webs				
Si utiliza las redes inalámbricas de la universidad responda lo siguiente:				
Nro.	PREGUNTA	SI	NO	OBSERVACIÓN
1	¿Se conecta de forma fácil al Wifi de la universidad?			
2	¿Ha suministrado datos correctos en aplicaciones web, y al momento de cargar regresan al mismo lugar de ingreso de datos?			
3	¿Dentro de los parámetros de búsqueda ha experimentado pérdida de información?			
4	¿Divisa publicidad indebida al intentar acceder a una aplicación web?			
5	¿Ha experimentado algún tipo de filtración en sus sitios web privados?			
6	¿Tiene registradas automáticamente las contraseñas de sus sitios webs?			
7	¿Usa contraseñas fuertes en sus sitios webs?			
8	¿Sus contraseñas están cifradas al momento de ser ingresadas?			
9	¿Ha perdido acceso a sus sitios webs después de ser víctima de hackers?			
10	¿Almacena información sensible como datos personales en la web?			
11	¿Utiliza datos de tarjetas de crédito en sitios webs?			
12	¿Realiza compras en línea por medio de portales webs?			
13	¿Ha Experimentado descargas de documentos no confiables en sitios webs?			
14	¿Tiene servicio en la nube?			
15	¿Realiza configuraciones adecuadas en los servicios que le ofrece la nube?			
16	¿Experimenta fallos en inicio de sesión a sus sitios webs?			
17	¿Su correo electrónico le informa sobre un intento de vulnerabilidad?			
18	¿Utiliza métodos de seguridad que le permita identificar actividades sospechosas?			
19	¿Los sitios webs que utiliza le informa en tiempo real sobre un ataque realizado?			
20	¿Los sitios webs que utiliza detectan cuentas sospechosas?			
21	¿Las aplicaciones que utiliza se bloquean momentáneamente si intentan acceder de manera inadecuada?			
22	¿Han eliminado o modificado información importante compartida en sus sitios webs?			
23	¿Los sitios webs que utiliza son seguros?			
24	¿Sus sitios webs utilizan estándares de verificación de seguridad?			
25	¿Ha recibido información dañina por medio de sus sitios webs?			
26	¿Ha descargado documentos de sospechosa procedencia de sitios webs?			
27	¿Utiliza rotación de contraseñas en sus sitios webs?			
28	¿Los sitios webs que utiliza le informa si su contraseña es fuerte o débil?			
29	¿Los sitios webs que utiliza, gestiona protección de seguridad automática?			
30	¿Mantiene sesión iniciada de sus sitios web en computadores personales?			
31	¿Sus equipos informáticos están en constante uso?			
32	¿Sus equipos informáticos tienen usuario y contraseña de inicio de sesión?			
33	¿Sus equipos cuentan con antivirus instalados?			
34	¿Tiene contraseñas grabadas en sus computadores en documentos de texto?			
35	¿Las sesiones en su navegador tienen tiempo de caducidad?			
36	¿Ha cambiado, o deshabilitado, las contraseñas de sus cuentas predeterminadas?			
37	¿Permiten que personas particulares utilicen sus equipos informáticos?			
38	¿Verifica la identidad digital del remitente de una comunicación?			
39	¿Verifica que las sesiones se invalidan cuando cierra la sesión?			
40	¿Posee cuentas en sitios webs que ya no utilice?			
41	¿Ha sido víctima de robo de cuentas en redes sociales?			
42	¿Comparte claves de sitios webs con otras personas?			
43	¿Ha cambiado su contraseña en los sitios webs que utiliza?			
44	¿Con que frecuencia cambia sus contraseñas?			
45	¿Su contraseña tiene 8 caracteres o más?			
46	¿Combina letras, números y caracteres en sus contraseñas?			
47	¿Ha perdido la contraseña de acceso a sus sitios webs?			
48	¿Recuperó con facilidad la contraseña de acceso a sus sitios webs?			
Realizado por: Delgado Basurto Jonathan				
Fecha: 30/07/2019				

Anexo 15: Instrumento aplicado a los estudiantes