Artículo original

Evaluación del plan de seguridad informática diseñado para el Tecnológico de la Universidad Laica Eloy Alfaro de Manabí

Evaluation of the computer security plan designed for the Technological of Laica Eloy Alfaro of Manabí University.

César Arturo del Pino Anchundia
delpino.cesar@hotmail.com
Universidad Laica Eloy Alfaro de Manabí. Ecuador

RESUMEN

Las medidas de seguridad informática diseñadas para usarse en las plataformas de comunicación de datos en la Universidad Laica Eloy Alfaro de "Manabí" representan una de sus mayores vulnerabilidades ya que han sido insuficientes para poder mantener el sitio completamente seguro de ataques de negación de servicios y de acceso a los servidores de datos. Es por esta razón que se propone un plan de seguridad informática para mitigar las vulnerabilidades de la plataforma tecnológica mediante un escaneo inicial y uno final con la utilización de herramientas gratuitas que se encuentran en la web y que permitieron determinar las amenazas críticas, altas, medias y bajas de que se produzcan accesos no autorizados a la red de datos. Según el informe del escaneo inicial, se aplicaron las medidas correctivas necesarias tales como, la adquisición de equipos Cisco y el diseño de una nueva estructura de la red LAN y WAN usando los beneficios que brindan estos equipos en capa 2 y 3, luego de esto, se compararon los niveles de riesgo entre el escaneo inicial y final y se verificó el mejoramiento de la seguridad de datos en el departamento de la Unidad Central de Gestión de la Información, las mismas que resultan necesarias para optimizar el servicio web que se brinda actualmente a la comunidad universitaria de la provincia, el resto del país y el mundo, así como también, fortalecer y mejorar los servicios de las telecomunicaciones en el campus matriz y en las extensiones de la universidad.

PALABRAS CLAVE: Etical Hacking; Seguridad Informática; Denegación de servicios; Técnicas de hackeo.

ABSTRACT

The Computer Security measures designed to be used in data communication platforms at the Laico Eloy Alfaro University in "Manabí" represent one of their greatest vulnerabilities since they have been insufficient to keep the site completely secure from denial of service attacks and Access to data servers. It is for this reason that a computer security plan is proposed to mitigate the vulnerabilities of the technological platform by means of an initial scan and an end using free tools that are in the web it was determined the critical, high and low threats that occur Unauthorized access to the data network, according to the initial scan report, the necessary corrective measures were applied, such as the acquisition of Cisco equipment and the design of a new LAN and WAN network structure using the benefits provided by these layered equipment 2 and 3, after

Recibido: Febrero 2017. **Aceptado:** Abril 2017
Universidad Regional Autónoma de los Andes UNIANDES

this the levels of risk between the initial and final scanning were compared by verifying the improvement of data security in the Central Unit of Information Management, which are necessary to improve the web service Which is currently offered to the university community of the province, the rest of the country and the world, as well as fort Establish and improve telecommunication services in the main campus and in the extensions of the university.
KEYWORDS: Ethical Hacking; Computer security; Denial of services; Vulnerability scan.

INTRODUCCIÓN

En el Ecuador, el tema del hackeo a información confidencial ha ganado notoriedad en estos últimos años debido al apoderamiento de las redes sociales e internet. Como ha sido noticia, los delitos van desde el cambio de notas de algunas universidades hasta la falsificación de títulos de tercer o cuarto nivel, así como también, robo de dinero mediante cuentas electrónicas y estafas, a todo esto se lo conoce como ciberdelincuencia, ciberdelito o delincuencia informática, constituida por un grupo de acciones que se cometen en los medios y recursos informáticos, principalmente dirigidos a la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos cibernéticos, además del abuso de estos (Orejuela, 2017).

Dentro de las iniciativas que se han desarrollado para promover la cooperación internacional en la lucha contra la ciberdelincuencia informática, se deben destacar las medidas adoptadas por el Consejo de Europa, la Unión Europea, el Grupo de los Ocho y la Organización de Cooperación y Desarrollo Económicos (Toledo, 2011), así como también, en Noviembre del 2001 se firmó en Budapest (Hungría) la primera convención sobre ciberdelitos, sin embargo, hasta la fecha estas medidas adoptadas han sido insuficientes.

Es por esta razón que los autores se preguntan cómo es posible que algunas instituciones tengan falencias en sus sistemas de cómputo, esto es debido a que no se realiza un correcto diseño de las redes de comunicaciones basado en normas de seguridad como por ejemplo en la ISO 27001:2005, la cual está orientada a establecer un sistema gerencial que permita minimizar el riesgo y proteger la información (Alexander, 2014). El riesgo de ingresos no autorizados a las redes de datos depende mucho del conocimiento que tenga el intruso, ya que puede utilizar scripts de programación o utilizar otros medios como son versiones completas de herramientas que se encuentran de manera gratuita en la web tal es el caso de Kali Linux la cual es una distribución de Linux avanzada para pruebas de penetración y auditorías de seguridad (Security, 2017), y que recopila las mejores herramientas de ingeniería social, mapeo de vulnerabilidades e infiltración a sistemas.

Para ser un buen hacker se debe tener conocimiento entre otros puntos, de Linux, programación, lenguaje de máquina, bases de datos y configuración de routers; hasta cierto punto podría decirse que el tener un conocimiento básico podría ser el inicio de un manejo de big data, concepto este que, aplica para toda aquella información que no puede ser procesada o analizada al utilizar procesos o herramientas tradicionales de información (Fragoso, 2012).

Recibido: Febrero 2017. **Aceptado:** Abril 2017

Para lograr realizar ingresos no autorizados hay que encontrar una puerta de acceso al mismo, o también llamada puerta trasera, de ahí que los usuarios y las claves de acceso no deben ser demasiados sencillos en su estructura, deben tener una política que contenga letras, números y signos de puntuación que se hace más difícil de obtener por medio de un ataque de fuerza bruta sin que el mismo no sea imposible de realizar, pero sí que represente una dificultad mayor la idea de encriptar la información.

Los protocolos de comunicación utilizados carecen (en su mayoría) de seguridad o ésta ha sido implementada en forma de "parche" tiempo después de su creación. Sea cual sea el ataque, por lo general, cada una de estas intrusiones redundan en importantes pérdidas económicas para las organizaciones, además de la imagen negativa y poco confiable que esta daría ante sus inversionistas y administradores; esto debido a que cada empresa debe garantizar que todos sus recursos informáticos se encuentren debidamente disponibles al momento de requerir cualquier tipo de información y así, poder cumplir con sus propósitos, y para ello no puede haber alteración o manipulación por parte de factores externos (Duque, Silva, & Renteria, 2013).

La seguridad informática actualmente forma parte de los grandes negocios en materia de tecnología y seguridad en las empresas (Suárez & Aldeir Avila, 2013), constituye una disciplina que en la actualidad tiene mayor notoriedad debido a la gran cantidad de delitos informáticos que se generan mediante el uso de la web y a la gran cantidad de automatización de servicios. Resulta numerosa la lista de las diferentes técnicas para poder realizar un ataque cibernético a determinado dominio, la mayoría de ocasiones provocadas por el desconocimiento de los usuarios acerca de las diferentes maneras en que se puede tener acceso a datos confidenciales mediante clonación de páginas o tarjetas, un simple correo electrónico que permite el acceso a claves secretas, e incluso, respuestas a preguntas de seguridad, por tal razón, en la actualidad es de vital importancia tomar las medidas que sean necesarias para minimizar el riesgo de que se presenten estafas electrónicas.

El desarrollo del tema propuesto se desarrolla en la Universidad Laica Eloy Alfaro de “Manabí” concretamente en la Unidad Central de Gestión de la Información (UCGI) o Tecnológico, departamento que se encuentra anexo al Vicerrectorado Académico desde el mes de Junio de 2011, mediante el análisis de su infraestructura tecnológica en el año 2014-2015 (del Pino Anchundia, 2015).

Entre sus actividades principales se encuentran brindar soporte de hardware y software a la comunidad universitaria, así como desarrollar aplicaciones que sirvan para mejorar los procesos académicos de la institución como son el control biométrico de los docentes, asistencia de alumnos y notas, ingreso de horarios de docentes, entre otros, por lo que lo se considera un eje de desarrollo para la institución mediante software de aplicación. Actualmente esta unidad se encuentra integrada en otra localidad y forma parte de un único departamento de Tecnología de la Información y la Comunicación (TIC) el cual se denomina Unidad Central de Información (UCI).

En el Ecuador se presentan denuncias sobre hackeo a cuentas, así como la intercepción de datos, tanto es así, que según los informes de Fiscalía del Ecuador, ocupa el primer

Recibido: Febrero 2017. **Aceptado:** Abril 2017

lugar la clonación de tarjetas. Según la Unidad de Gestión Procesal de la Fiscalía General del Estado, existieron 877 casos de delitos informáticos denunciados en el 2014 (Estado, 2014).

Resulta importante señalar que en el Código Integral Penal se contemplan seis tipos de delitos informáticos entre ellos, revelación ilegal de base de datos, interceptación ilegal de información, entre otros. Para minimizar el riesgo se debe evitar el uso de lugares públicos y de facilitar datos personales a terceras personas como son nombres de usuario y contraseñas de tarjetas y cuentas a través de internet, verificar a su vez la autenticidad del sitio, sea este por medio de un certificado de validez o simplemente verificar el nombre del dominio ya que la mayoría de estafas se dan por esta vía, por ejemplo, la página clonada siempre tendrá una terminación diferente de los sitios autorizados, llegando en su mayoría mensajes falsos de actualización de datos por medio de correos a las cuentas, adicionalmente, hay que tener cuidado en los datos que se publican en páginas sociales ya que también podrían ser usados por terceras personas para realizar ciberdelitos.

A partir de lo planteado, los objetivos del presente trabajo, estuvieron enfocados en revisar los resultados obtenidos en el análisis de vulnerabilidades en el Tecnológico de la Universidad Laica Eloy Alfaro de Manabí y a su vez, constatar la efectividad de las medidas de mitigación a los problemas encontrados.

MÉTODOS

"Una vez detallado el esquema de redes de la Unidad Central de Gestión de la Información se realizó el aplicativo de las diferentes plataformas de vulnerabilidades que puedan ser explotadas, es importante señalar que los dominios donde se realizaron los laboratorios fueron: www.ULEAM.edu.ec y www.academico.ULEAM.edu.ec por ser el primero la puerta de enlace al segundo" (del Pino Anchundia, 2015). Aproximadamente los software escogidos hicieron unos 100000 test a los dominios seleccionados, ya que cada uno cuenta con una base de datos extensa de las vulnerabilidades encontradas hasta la fecha en los sistemas operativos y de programación, entre otros.

Se realizó un estudio de mapeo y análisis de vulnerabilidades mediante el uso de tres programas especializados: *Nessus Cloud, Retina Scanner Vulnerability y OpenVas*, (Astudillo, 2014) mediante el escaneo a la dirección principal de la universidad: www.uleam.edu.ec y la de vicerrectorado académico: www.academico.uleam.edu.ec. Además de estos tres programas, se usaron otras herramientas como son: *maltego, dmitry, nmap, zenmap*, las que permitieron tener una visión global de la plataforma tecnológica en los dominios de la Universidad Laica Eloy Alfaro de Manabí, obteniendo información como, el tipo de servidor de datos y subdominios del dominio principal, y tomando en consideración que al ser información confidencial fueron obviados datos considerados innecesarios.

Para poder instalar y configurar los programas especializados que fueron objeto de estudio en el mapeo de vulnerabilidades, como es el caso de *Nessus*, se debe ingresar a la página del autor del software (https://www.tenable.com/products/nessus-vulnerability-scanner), primeramente se selecciona el lenguaje a utilizar y luego se registra; debido a que este programa tiene algunas versiones, se selecciona usar la

Recibido: Febrero 2017. **Aceptado:** Abril 2017

opción de evaluación de *Nessus Cloud* (nube); para registrase se necesita un mail corporativo ya que no son aceptadas las direcciones de hotmail y yahoo, por ejemplo, ya que las personas que pedían evaluar la aplicación, muchas veces optaban por darle mal uso al programa, es decir, las versiones de evaluación solo son autorizadas para fines educativos o de necesidad por parte de una empresa; luego de esto, aparecerá la siguiente interfaz de registro:

Figura 1. Captura de pantalla de registro *Nessus*
Fuente: página de *Nessus*

Para poder instalar *Retina Scanner Vulnerability* se debe ingresar al siguiente link https://www.beyondtrust.com/products/retina-network-security-scanner/ y dar click en request demo, luego de eso, se pedirá ingresar nombres y apellidos, un email corporativo, teléfono, país y cuántas personas trabajan en la organización, luego de registrarse al correo que se ingresó, llegará una notificación donde, si se hace correctamente, permitirá bajar una aplicación que resulta sencilla instalarla en Windows (también se puede escoger versiones para Linux y Mac OS); la funcionalidad de la interfaz gráfica del programa es similar a la versión de *Nessus*, arroja también un informe basado en qué tipo de vulnerabilidad ha sido encontrada, cómo puede ser explotada dicha vulnerabilidad y la manera también de mitigarla, se cuenta además, con un asesor en línea que puede ayudar a esclarecer cualquier duda que se tenga.

Con respeto a la aplicación *OpenVas,* si bien es cierto que podría usarse directamente mediante un browser de navegación como Mozilla Firefox o Internet Explorer, resulta más eficaz y fácil de instalar subiendo primero una máquina virtual con un sistema operativo especializado en análisis de vulnerabilidades como es Kali Linux, para luego, una vez instalada la máquina virtual, ingresar en la consola de comandos de Kali Linux lo siguiente:

root@kali:~# apt-get update

root@kali:~# apt-get dist-upgrade

root@kali:~# apt-get install openvas

root@kali:~# openvas-setup

root@kali:~# netstat –antp

Recibido: Febrero 2017. **Aceptado:** Abril 2017

root@kali:~# openvas-start

Si la aplicación se instaló correctamente se podrá visualizar el siguiente mensaje:

Starting OpenVas Services

Starting Greenbone Security Assistant: gsad.

Starting OpenVAS Scanner: openvassd.

Starting OpenVAS Manager: openvasmd. (Security, Kalilinux Openvas 8.0, 2015)

Los datos fueron obtenidos en los registros de cada plataforma de escaneo especializadas, al dividir las amenazas en críticas, altas, medias y bajas, y luego fueron resumidos los informes que dan los programas en cuadros estadísticos para hacer la información más comprensible para los lectores.

A continuación una muestra del informe real de *Nessus*:

REPORTE NESSUS CLOUD					
Crítica	**Alta**	**Media**	**Baja**	**Información**	**Total**
3	**9**	**35**	**5**	**34**	**86**
Critical (10.0)			45004	Apache 2.2 < 2.2.15 Multiple Vulnerabilities	
Critical (10.0)			57603	Apache 2.2 < 2.2.13 APR apr_palloc Heap Overflow	
Critical (10.0)			60085	PHP 5.3.x < 5.3.15 Multiple Vulnerabilities	
High (9.3)			67259	PHP 5.3.x < 5.3.27 Multiple Vulnerabilities	
High (8.5)			59529	PHP 5.3.x < 5.3.14 Multiple Vulnerabilities	
High (8.3)			58988	PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution	
High (8.3)			59056	PHP 5.3.x < 5.3.13 CGI Query String Code Execution	
High (7.5)			42052	Apache 2.2 < 2.2.14 Multiple Vulnerabilities	

Tabla 1. Vulnerabilidad UCGI dada por programa _ *Nessus*
Fuente: del Pino Anchundia, 2015

RESULTADOS

Con las pruebas realizadas en la red LAN y WAN de la plataforma tecnológica se llegó a determinar las fallas más comunes, las cuales se detallan en la figura 2.

Recibido: Febrero 2017. **Aceptado:** Abril 2017

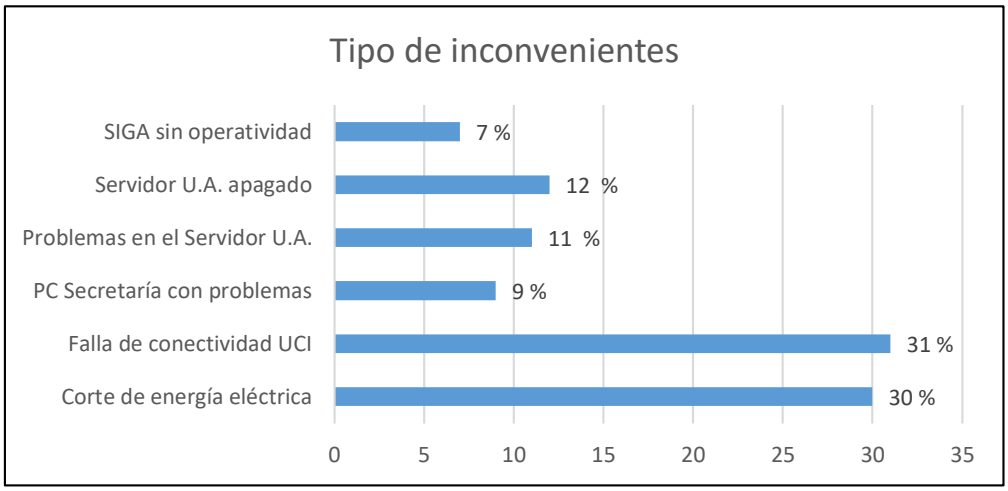

Figura 2. Informe de fallas de sistema
Fuente: base de datos del proyecto

En el año 2015 se reportaron en la unidad una serie de fallas en el sistema del tecnológico de la ULEAM como lo muestra la figura 2, de las cuales, el 31 % correspondió a falla de conectividad, el corte de energía eléctrica representó el 30 % de las fallas registradas en el área, y el 12 % a servidor de la unidad académica apagado.

En primer lugar se usó *Nessus Cloud*, una de las más conocidas y galardonadas a nivel mundial en detección de vulnerabilidades, lo cual generó los siguientes resultados.

Resumen 1 (*Nessus Cloud*)

El resumen de reporte de programa *Nessus* sobre el dominio www.academico.uleam.edu.ec, tal como lo muestra la figura 3, informa que el mismo tiene tres vulnerabilidades críticas, dos se refieren al sistema operativo y una al código de programación *Hypertext Preprocessor* (PHP). Se observa además que, un 6 % corresponde a vulnerabilidad crítica, el 17 % a vulnerabilidad alta, el 67 % a vulnerabilidad media y el 10 % del escaneo realizado muestra un 10 % de vulnerabilidad baja (del Pino Anchundia, 2015).

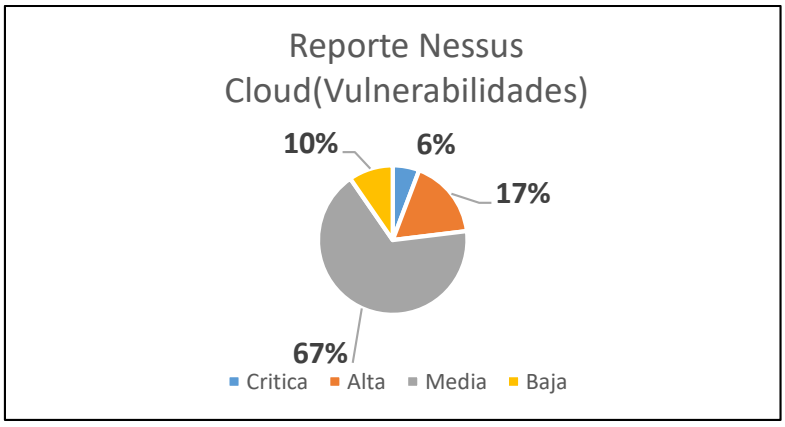

Figura 3. Vulnerabilidades UCGI
Fuente: Base de datos del proyecto

Recibido: Febrero 2017. **Aceptado:** Abril 2017
Universidad Regional Autónoma de los Andes UNIANDES

Resumen 2 (*OpenVas*)

Como se observa en la figura 4, con el reporte principal que ofrece *OpenVas*, se detectaron dos vulnerabilidades medias a través del método de detección de la vulnerabilidad que representa el 100% del muestreo realizado y no se detectaron vulnerabilidades altas ni bajas.

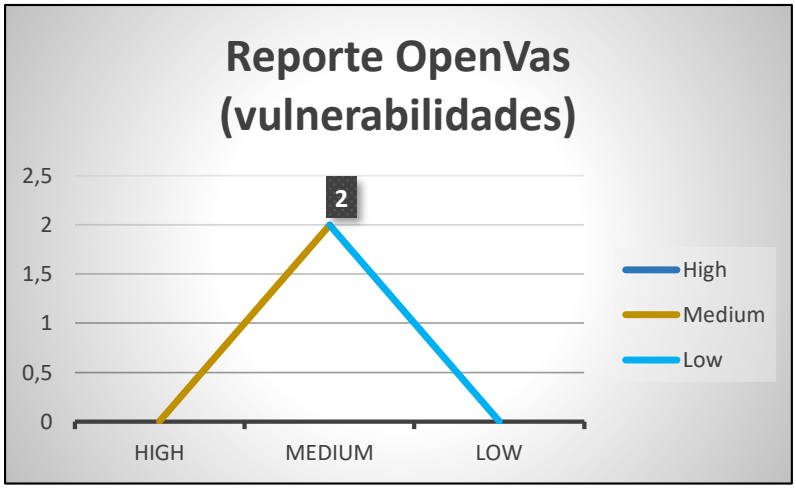

Figura 4. Vulnerabilidades UCGI
Fuente: bases de datos del proyecto

Resumen 3 (*Retina Scanner*)

Al utilizar la versión free de *Retina Scanner* se pudo determinar que el Tecnológico de la ULEAM tiene 91% de vulnerabilidades medias, 7 % de vulnerabilidades altas y un 2 % de vulnerabilidades bajas (del Pino Anchundia, 2015).

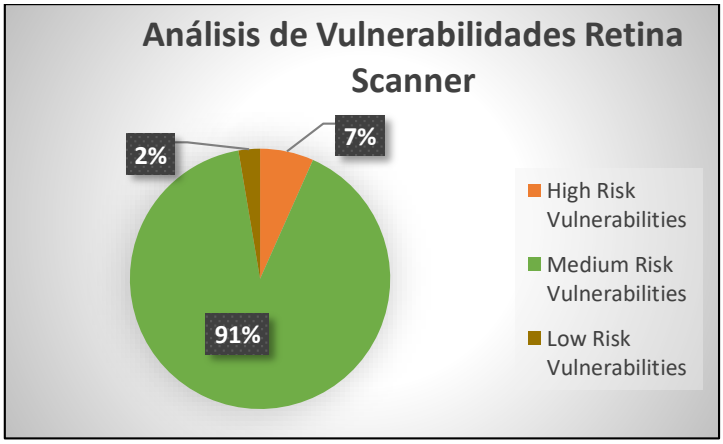

Figura 5. Cuadro Estadístico Vulnerabilidades UCGI
Fuente: base de datos del proyecto

En la tabla 2 de resultados se puede observar que al iniciar se tenía un total de 206 vulnerabilidades encontradas en el servidor de la UCGI en el año 2014-2015 y al revisar el proyecto se tiene ahora apenas 13 vulnerabilidades de acuerdo a un escaneo realizado a principios del 2016, por lo que se puede plantear que las medidas adoptadas en el departamento permitieron mitigar las vulnerabilidades encontradas por los programas usados en el mapeo, sin que esto signifique que se hayan solucionado todas las vulnerabilidades encontradas. Es importante señalar también, que el riesgo bajó de

Recibido: Febrero 2017. **Aceptado:** Abril 2017
Universidad Regional Autónoma de los Andes UNIANDES

70380 a 4433, este proceso se realizó al utilizar una matriz de riesgo que se calcula de acuerdo a las vulnerabilidades encontradas.

Dirección IP	OS Detectado	Exploits	Malware	Totales	Críticas	Altas	Medias	Bajas	Riesgo
RESULTADOS PRELIMINAR DE VULNERABILIDADES DETECTADAS									
184.107.231.202	Linux 2.6.32	1	0	**206**	1	11	183	11	**70380**
201.219.17.48	SuSE Linux 11.0 or 11.1	2	0	57	3	7	41	6	20060
RESULTADOS DESPUES DE REALIZAR LAS CORRECIONES TECNICAS CON LOS PROGRAMADORES DE LA UCGI									
184.107.231.202	Linux 2.6.32	0	0	**13**	0	0	8	5	**4433**
201.219.17.48	SuSE Linux 11.0 or 11.1	0	0	4	0	0	2	2	1364

Tabla 2. Comparación de resultados escaneos inicial y final UGCI
Fuente: del Pino Anchundia, 2015

Propuesta técnica desarrollada

Cabe destacar que algunas de las sugerencias realizadas fueron implementadas para el mejoramiento de la plataforma, entre ellas, la compra de equipos Cisco y la centralización de la información mediante el monitoreo de software que vigilen el tráfico de la información en la red; uno de los puntos más importantes fue el establecer las políticas de uso de los recursos del departamento, faltando algo que hacer en el manual de procesos y establecimiento de planes de contingencia que en el futuro seguramente serán considerados. Adicional a estos correctivos implementados, resulta necesario ejecutar en el futuro algunos puntos adicionales inmersos en el plan de seguridad final siguiendo la norma ISO 27001:2005, los cuales se detallan a continuación:

a) Conformación del comité de seguridad y delegación formal de responsabilidad.
b) Definir los activos de la información de la Unidad Central de Gestión de la Información y delegar responsables formales a cada uno de ellos.
c) Establecer acuerdos de confidencialidad en los activos actuales y en la compra de nuevos.
d) Establecer relaciones con proveedores relaciones en el tema de seguridad de la información.
e) Identificar los riesgos derivados de terceros en el proceso de compras o adquisición.
f) En los contratos de servicio realizado a un tercero, revisar que incluya las cláusulas de seguridad.
g) Realizar el inventario de activos de la Unidad Central de Gestión de la Información e indicar su criticidad dentro del proceso de seguridad de la información.
h) Realizar un procedimiento documentado en el tema de cambios de puesto y devolución de activos al finalizar funciones en el departamento.

Recibido: Febrero 2017. **Aceptado:** Abril 2017

i) Ver la factibilidad del uso de una planta generadora para la continuidad del servicio.
j) Documentar los procesos de operación del departamento.
k) Realizar una separación de los entornos de desarrollos de software y pruebas de explotación.
l) Implementar en la red ruta y reglas de control de acceso filtrado de paquetes.
m) Definir procedimientos claros y documentados sobre: comercio electrónico, transacciones en línea e información con acceso público.
n) Definir procedimiento formal de revisión de los derechos de acceso.
o) Capacitar a los programadores en temas concernientes a la seguridad de la red y servidores.
p) Establecer una política sobre el cumplimiento de las leyes de propiedad intelectual.
q) Cumplir con las leyes de regulación de controles criptográficos.
r) Establecer controles de auditorías paulatinamente en la Unidad Central de Gestión de la Información (del Pino Anchundía, 2015)

DISCUSIÓN

La disciplina de la seguridad informática es muy poco aplicada, debido a que cada cierto tiempo se descubren vulnerabilidades en los núcleos de los sistemas, programación o se desarrollan nuevas técnicas de hackeo; muchas de las instituciones, especialmente las financieras, han recurrido a nuevas estrategias de seguridad por medio de mensajes telefónicos por ejemplo, preguntas de seguridad para evitar que sea mayor el índice de personas perjudicadas por el tema de delitos informáticos. Mediante la implementación del proyecto se intenta dar un nuevo diseño a la red LAN y WAN al utilizar switches de capa 2 y 3; ante todas estas estimaciones se procedió a realizar las políticas de seguridad así como un plan de contingencia en caso de desastres físicos o lógicos.

Después de la ejecución de la revisión sistemática y del análisis de las vulnerabilidades encontradas, se evidencia que se pueden utilizar herramientas que permiten detectar vulnerabilidades para diferentes propósitos, es decir, algunas herramientas cubren desde escaneo de vulnerabilidades en aplicaciones web, hasta escaneo de vulnerabilidades en dispositivos móviles, un ejemplo de este tipo de herramientas es *Nessus Vulnerability Scanner* (Tenable, 2014), además de muchas otras funcionalidades. De igual manera existen herramientas muy específicas para la detección de problemas de seguridad muy específica, como por ejemplo WhatWeb (Morning Start Security, 2014) que solamente se enfoca en el escaneo de sitios web (Hernández Salcedo & Mejía Miranda, 2015).

Tal y como plantean Hernández Salcedo y otros, se debe centrar en realizar el análisis de vulnerabilidades con herramientas globales que abarquen muchos aspectos como lo tiene *Nessus* que divide sus análisis en diferentes campos como: *Basic Network Scan, Host Discovery, Audit Cloud Insfraestructure, Advanced Scan, Mobile Device Scan*, lo que permite cubrir la gran mayoría de técnicas de detección de vulnerabilidades como son: *black-box, white-box*, auditoría de código fuente, análisis dinámico de código, pruebas de penetración, pruebas de caja negra, entre otros. Es por este motivo que antes de realizar el análisis de vulnerabilidades se tiene que determinar cuál es el

Recibido: Febrero 2017. **Aceptado:** Abril 2017

objetivo a escanear, ya que variará de acuerdo a las condiciones y tipo de tecnología que se vaya a analizar.

Una vez detectadas las vulnerabilidades usando los 3 escáneres (*Nessus, Retina y OpenVas*), el siguiente paso consiste en determinar qué vulnerabilidad crítica se ha encontrado, para que, de acuerdo al informe del escáner, utilizar una herramienta de explotación, como por ejemplo, *core impact* que es un programa que mediante una debilidad detectada puede tener acceso al servidor de datos de una red; en el proyecto, la opción *Nessus Cloud* detectó vulnerabilidades críticas tal y como lo muestra la figura 3. Desde el 2015 hasta la fecha, la infraestructura de datos de la ULEAM ha sido atacada por diferentes técnicas de hackeo, una de ellas la denegación de servicio ("tipo de ataque informático especialmente dirigido a redes de computadoras y que tiene como objetivo lograr que un servicio específico o recurso de la red, quede completamente inaccesible a los usuarios legítimos de la red") (www.culturación.com, 2014), lo que ha causado que el servidor de datos web de la Universidad Laica Eloy Alfaro de Manabí quede sin servicio. El proyecto se inició en el año del 2015 y desde esa época la infraestructura ha mejorado ya que se propuso cambios en los servidores y compra de equipos Cisco los cuales permiten realizar un direccionamiento acorde de la información. Además se realizaron correcciones a la programación PHP de la página. Una vez que se implementaron algunas de las sugerencias indicadas en el proyecto, se realizó un nuevo escaneo con las mismas herramientas iniciales obteniendo los resultados ya detallados en la tabla 2.

Estos resultados podrían contrastarse con los que indica el artículo Ethical hacking, una metodología para descubrir fallas de seguridad en sistemas informáticos (Veloz, Alcivar, Salvatierra, & Silva , 2017) que señala mediante la herramienta Kali-Linux el uso de Ethical Hacking en un ambiente virtualizado y controlado. En los Laboratorios de Informática de la Universidad Técnica de Manabí, por ejemplo, se pudo demostrar la presencia de fallas de seguridad en Sistemas Operativos, como Windows y Android, las pruebas se realizaron en máquinas reales, virtuales y dispositivos móviles.

Adicionalmente, con el empleo de la norma ISO 27001:2005 en los procesos que se realizan en la Unidad Central de Gestión de la Información de la ULEAM se puede hacer uso del Modelo de Madurez de Capacidades o Capability Maturity Model (CMM), que es un modelo de evaluación de procesos, para llegar a determinar en qué proceso se encuentra la norma ISO y que se pondera en un orden desde 0 hasta 5 (inicial, repetible, definido, gestionado y optimizado). Con esto, cada cierto tiempo, de acuerdo a lo que determinen las autoridades del departamento, se realice una auditoría de procesos y llegar a determinar el punto del modelo de madurez en que se encuentra el mismo. Esto ayudará a que el departamento pueda acceder en un futuro a una certificación ISO 27001:2005, una vez que el grado de madurez de los procesos se encuentre en estado óptimo.

CONCLUSIONES

1. La plataforma tecnológica de la Unidad Central de Gestión de la Información muestra vulnerabilidades de programación las cuales fueron mitigadas al comparar los primeros análisis al inicio del proyecto
2. Los riesgos de acceso de usuarios no autorizados a la plataforma tecnológica disminuyeron un porcentaje considerable en los dos dominios analizados que

Recibido: Febrero 2017. **Aceptado:** Abril 2017

corresponden a la página principal de la Universidad Laica Eloy Alfaro de "Manabí" y a Vicerrectorado Académico

3. Las vulnerabilidades mitigadas en gran parte corresponden a debilidades de los sistemas operativos (Linux) y a la programación PHP de la página web.
4. Se hace necesario instalar programas y herramientas de rastreo que permitan controlar el tráfico de la red
5. Se debe implementar un plan de continuidad del negocio o plan de contingencias en caso de desastres.

REFERENCIAS

Alberto G. Alexander, P. (2014). *Iso 2700*. Obtenido de Centrum (Pontificia Universidad Católica del Perú): http://www.iso27000.es/download/Implantacion_del_ISO_27001_2005.pdf

Astudillo, K. (2014). *Hacking Etico 101.* Guayaquil: Amazon.

del Pino Anchundia, C. (2015). *Desarrollar e implementar un Plan de Seguridad Informática para el Tecnológico de la Uleam (Título de maestría).* Guayaquil, Ecuador: ESPOL.

Details, C. (12 de Febrero de 2017). *CVEdetails.com the ultimate security vulnerability data source*. Obtenido de http://www.cvedetails.com/cve/CVE-2001-1013/

Duque, J., Silva, L. A., & Renteria, E. D. (2013). Análisis Comparativo de las principales técnicas de Hacking Empresarial. *ISSN 0122-1701*.

Estado, F. G. (2014). *Fiscalia*. Obtenido de Fiscalia de Ecuador: http://www.fiscalia.gob.ec/index.php/sala-de-prensa/2421-el-coip-contempla-una-pena-de-tres-a-cinco-a%C3%B1os-de-prisi%C3%B3n-por-robos-de-cuentas-bancarias.html

Fragoso, R. B. (18 de 06 de 2012). *IBM*. Obtenido de IBM DeveloperWorks: https://www.ibm.com/developerworks/ssa/local/im/que-es-big-data/

Hernández Salcedo, A. L., & Mejía Miranda, J. (2015). *Guía de ataques, vulnerabilidades, técnicas y herramientas para aplicaciones Web* (Vols. ReCIBE, Año 4 No. 1, Febrero 2015). Zacatecas, México: Recibe(Revista Electrónica de Computación, Informática, Biomedia y Electrónica.

Orejuela, N. T. (2017). *Ciberdelicuencia*. Obtenido de Instituto Tecnico Industrial de Facatativa: https://ciberdelincuencia.wikispaces.com/

Security, O. (27 de Abril de 2015). *Kalilinux Openvas 8.0*, 8.0 Update. (Offensive Security) Recuperado el 18 de Abril de 2017, de https://www.kali.org/penetration-testing/openvas-vulnerability-scanning/

Security, O. (2017). *Kali Linux Official Documentation*. Obtenido de http://es.docs.kali.org/introduction-es/que-es-kali-linux

Suárez, D., & Aldeir Avila, F. (2013). Una forma de interpretar la seguridad Informática. *Journal of Engineering and Technology*, 16.

Recibido: Febrero 2017. **Aceptado:** Abril 2017

Toledo, R. B. (2011). Los Delitos en Internet: Un enfoque desde la pornografía infantil en la red. *Versión en Línea ISSN 0718-4018*(Número 13 Semestre 2011).

Veloz, J., Alcivar, A., Salvatierra, G., & Silva , C. (2017). Ethical hacking, una metodología para descubrir fallas de seguridad en sistemas informáticos mediante la herramienta Kali-linux. *Revista de Tecnologías de la Informática y las Comunicaciones, Vol.1 N.1 Año 1 (2017)*, 5.

www.culturación.com. (15 de Mayo de 2014). *Culturación*. Obtenido de http://culturacion.com/que-es-una-denegacion-de-servicio/

Recibido: Febrero 2017. **Aceptado:** Abril 2017