UNIDAD ACADÉMICA:

OFICINA DE POSTGRADOS

TEMA:

MODELO PARA LA MITIGACIÓN DE VULNERABILIDADES INFORMÁTICAS EN LOS SERVICIOS WEB DE LA PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR AMBATO

Proyecto de Investigación y Desarrollo previo a la obtención del título de Magister en Gerencia Informática

Línea de Investigación, Innovación y Desarrollo principal:

Sistemas de Información y/o Nuevas Tecnologías de la Información y Comunicación y sus aplicaciones

Caracterización técnica del trabajo:

Aplicación

Autor:

Eduardo Marcelo Remache Rubio

Director:

Alberto Leopoldo Arellano Aucancela, MsC.

Ambato – Ecuador

Julio 2018

Modelo para la mitigación de vulnerabilidades informáticas en los servicios web de la Pontificia Universidad Católica del Ecuador Ambato

Informe de Trabajo de Titulación presentado
ante la Pontificia Universidad Católica del
Ecuador
Sede Ambato por

Eduardo Marcelo Remache Rubio

En cumplimiento parcial de
los requisitos para el Grado de
Magister en Gerencia Informática

Oficina de Postgrados

Julio 2018

Modelo para la mitigación de vulnerabilidades informáticas en los servicios web de la Pontificia Universidad Católica del Ecuador Ambato

Aprobado por:

María Fernanda San Lucas, Mg.
Presidente del Comité Calificador
Coordinadora de la Oficina de Postgrados

José Marcelo Balseca Manzano, Mg.
Miembro Calificador

Alberto Leopoldo Arellano Aucancela, MSc .
Miembro Calificador
Director de Proyecto

Hugo Rogelio Altamirano Villarroel, Dr.
Secretario General

Pontificia Universidad Católica del Ecuador
SECRETARÍA GENERAL
PROCURADURÍA

Dennis Vinicio Chicaiza Castillo, Mg.
Miembro Calificador

Fecha de aprobación:
Julio 2018

Ficha Técnica

Programa: Magister en Gerencia Informática

Tema: Modelo para la mitigación de vulnerabilidades informáticas en los servicios *web* de la Pontificia Universidad Católica del Ecuador Ambato

Tipo de trabajo: Proyecto de Investigación y Desarrollo

Clasificación técnica del trabajo: Aplicación

Autor: Eduardo Marcelo Remache Rubio

Director: Alberto Leopoldo Arellano Aucancela, Ing. MsC.

Líneas de Investigación, Innovación y Desarrollo

Principal: Sistemas de Información y/o Nuevas Tecnologías de la Información y Comunicación y sus aplicaciones

Resumen Ejecutivo

Con una tecnología cambiante, con vulnerabilidades que se descubren día a día que permiten nuevas formas de ataques cibernéticos, se hace imprescindible el tener los servicios *web* de la institución asegurados y evitar daños futuros.

Es así que, con la ayuda de la metodología de gestión de riesgos Magerit V3, se definió como un modelo acoplado que permite mitigar las vulnerabilidades informáticas en los servicios *web* de la Pontificia Universidad Católica del Ecuador Ambato, para la toma de decisiones y prevenir que los servicios sean atacados o vulnerados.

El modelo propuesto inicia con la identificación de los servicios y activos informáticos, para luego hacer un análisis de los riesgos y determinar el daño que causarían a la organización.

DECLARACIÓN Y AUTORIZACIÓN

Yo: EDUARDO MARCELO REMACHE RUBIO, con CC. 050239743-3, autor del trabajo de graduación intitulado: "MODELO PARA LA MITIGACIÓN DE VULNERABILIDADES INFORMÁTICAS EN LOS SERVICIOS WEB DE LA PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR AMBATO", previa a la obtención del título profesional de Magister en Gerencia Informática, en la oficina de Postgrados.

1.- Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través de sitio web de la Biblioteca de la PUCE Ambato, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de Universidad

Ambato, julio 2018

EDUARDO MARCELO REMACHE RUBIO

CC. 050239743-3

Dedicatoria

El presente proyecto lo dedico a mi padre, con quien iniciamos éste viaje, pero Dios lo llamo repentinamente; quien, con su ejemplo de perseverancia y superación personal como profesional dejó un legado a la familia; a mi madre, gracias por su comprensión y paciencia durante éste proceso, han permitido culminarlo con éxito.

Reconocimientos

A la Pontificia Universidad Católica del Ecuador Ambato, por haberme permitido ser parte del programa de maestría y poder superarme profesionalmente, como a todos los Docentes que impartieron sus conocimientos.

Al Departamento de Tecnología de la PUCE Ambato, por la apertura brindada de todo su personal para el desarrollo del presente proyecto.

Al Ing. MSc. Alberto Arellano, por su apoyo incondicional, su ayuda desinteresada y su guía acertada han permitido culminar con éxito la investigación propuesta.

A todas las personas que, de forma desinteresada me apoyaron con sus concejos y sugerencias para alcanzar profesionalmente los objetivos propuestos.

Resumen

El presente trabajo de investigación tiene por objeto proponer un modelo para la mitigación de vulnerabilidades informáticas en los servicios *web* de la Pontificia Universidad Católica del Ecuador Ambato, con la finalidad de dar a conocer al personal que administra los sistemas informáticos la existencia de riesgos, la necesidad de mitigarlos a tiempo y evitar daños que pueden ser catastróficos para la institución.

La recolección de información se realiza mediante los métodos deductivo, inductivo y exploratorio que por medio de entrevistas ayudan a recopilar información para el desarrollo del presente modelo, además, como metodología para la gestión y análisis de riesgos informáticos se toma como base Magerit Versión 3, la cual permite identificar los activos relevantes de la organización y el valor que poseen.

El análisis de resultados evidencia los riesgos a los que están expuestos los activos, las vulnerabilidades que poseen los aplicativos *web*, así como el impacto que tendrían si llegasen a materializarse, bajo la aplicación de salvaguardas que puedan mitigar el impacto siempre y cuando se considere que existen debilidades residuales. Las acciones propuestas promueven la mejora continua de los riesgos y vulnerabilidades de los aplicativos, y la posibilidad de aprender de eventos propios o ajenos que generan oportunidad de crecimiento.

Palabras Clave: seguridad informática, servicios *web*, sistema de gestión de riesgos, vulnerabilidades, riesgos.

Abstract

The aim of this study is to propose a model for the mitigation of cyber susceptibilities in the web services of the Pontifical Catholic University of Ecuador in Ambato in order to indicate to the staff who manage the computer systems the existence of risks, the need to mitigate them on time, and avoid damage that can be catastrophic for the institution.

The data is collected with the deductive, inductive and exploratory methods, which through interviews, help to collect information for the development of this model. In addition, Magerit Version 3 is taken as the methodology for cyber risk management and analysis making it possible to identify the organization's relevant assets and the value that they have.

The analysis of the results show the risk that the assets are exposed to, the susceptibilities that web applications have, as well as the impact that they would have if they became a reality. This is done with the safeguard application that can mitigate the impact provided it is considered that there will always be residual weaknesses. The proposed actions foster continuous improvement of the risks and vulnerabilities of the applications as well as the possibility to learn from one's own events, or those of others, which create opportunities of growth.

Key words: cyber security, web services, risk management system, susceptibilities, risks.

Tabla de Contenidos

Lista de Gráficos

Lista de Figuras

Lista de Cuadros

Lista de Esquemas

Lista de Tablas

Capítulo 1

Introducción

Las instituciones educativas en el Ecuador han crecido tecnológicamente en los últimos años, es así que, la mayoría de los procesos administrativos y académicos se han automatizado mediante la implementación de sistemas informáticos, con la finalidad de brindar al cliente un servicio rápido, oportuno y de calidad. Con lo cual, se ha hecho imprescindible la creación de un departamento de tecnología, el que se debe alinear a los objetivos institucionales.

Sin embargo, se ha obviado un problema muy importante y que actualmente se ha convertido en un pilar fundamental, no solo en las instituciones educativas sino en toda organización pública o privada, como es la seguridad de los sistemas informáticos pues el valor más preciado es la información, la que es apetecida por personas externas o internas que desean lucrar económicamente o modificarla para bien personal. Por ésta razón, el modelo para mitigar las vulnerabilidades en aplicativos *web* que se propone, analiza los puntos en los que un desarrollo *web* es débil, desde los componentes físicos que permiten su ejecución hasta su mismo funcionamiento.

A su vez, se identifican todos los activos informáticos, las amenazas a las que están expuestos, la probabilidad de que una amenaza llegue a ocurrir y el impacto que tendría en la organización la pérdida de la información. Igualmente, se detectan las vulnerabilidades en los sistemas informáticos *web*, las que son mitigadas con la adopción de contramedidas que ayudan a reducir el impacto que los fallos del sistema pudiesen tener.

1.1 Presentación del trabajo

La investigación, establece un modelo que permite analizar las vulnerabilidades en los servicios *web* que una institución ofrece a los clientes, como también se define las salvaguardas a aplicarse para mejorar la seguridad y evitar que una amenaza llegase a materializarse.

Una vez determinados los riesgos y vulnerabilidades a los que están expuestos los activos informáticos, se evidencia la falta de procedimientos de control en la seguridad de los aplicativos desarrollados como en los adquiridos, así como tampoco existe un análisis periódico de vulnerabilidades en los sistemas informáticos en producción.

Es así que, se propone un modelo para mejorar la seguridad en los aplicativos *web* de la PUCE Ambato, tanto en los desarrollados como en los adquiridos, también se establecen memorias para las vulnerabilidades detectadas y mitigadas, las que pueden ser utilizadas en futuras detecciones; de tal manera, que se minimice el impacto de un ataque.

1.2 Descripción del documento

En el primer capítulo, se realiza una visión global sobre el trabajo realizado y lo alcanzado con la misma. El segundo capítulo, describe el problema encontrado en los aplicativos *web* de la PUCE Ambato y los objetivos planteados para la investigación. El tercer capítulo, presenta definiciones que respaldan el desarrollo del proyecto. El cuarto capítulo, muestra el diagnóstico y el modelo a ser aplicado para la mitigación de vulnerabilidades *web*. El quinto capítulo, describe la ejecución de la propuesta y los resultados obtenidos. El sexto capítulo, presenta las conclusiones y recomendaciones de la investigación.

Capítulo 2

Planteamiento de la Propuesta de Trabajo

2.1 Información técnica básica

Tema: Modelo para la mitigación de vulnerabilidades informáticas en los servicios *web* de la Pontificia Universidad Católica del Ecuador Ambato.

Tipo de trabajo: Proyecto de Investigación.

Clasificación técnica del trabajo: Investigación.

Líneas de investigación: Seguridad Informática en Aplicativos *web*, Metodología de seguridad *web*.

2.2 Descripción del Problema

La seguridad en los servicios *web* que contienen información sensible, ha crecido de una manera exponencial con el internet, tal es así, que uno de los puntos más críticos en una infraestructura de comunicación empresarial, es la seguridad de los aplicativos *web* que interactúan de forma directa con el usuario. La falta de medidas de prevención adecuadas, puede provocar que un atacante utilice una variedad de medios para ingresar de forma no autorizada a la infraestructura de comunicación y obtener información de manera ilícita, pueden llegar hasta su alteración.

En este sentido, el problema científico se centra en el desarrollo de una metodología para mitigar las vulnerabilidades informáticas en los servicios *web* de la Pontificia Universidad Católica del Ecuador Ambato.

2.3 Preguntas Básicas

¿Cómo aparece el problema que se pretende solucionar? No aplica.

¿Por qué se origina? La falta de control de los administradores para detectar y reducir el impacto de las vulnerabilidades.

¿Qué lo origina? La presencia de amenazas de seguridad intrínsecas que una aplicación o sistema puede tener en su desarrollo y/o implementación.

¿Cuándo se origina? Cuando usuarios mal intencionadas desean acceder a la información de manera ilegal.

¿Dónde se origina? No aplica.

¿Dónde se detecta? En los servicios *web* brindados por la Pontificia Universidad Católica del Ecuador Ambato.

2.4 Formulación de la meta

Reducir el impacto de las vulnerabilidades en los servicios *web* de la Pontificia Universidad Católica del Ecuador Ambato, para mejorar el nivel en la seguridad.

2.5 Objetivos

Objetivo General

Desarrollar un modelo para la mitigación de vulnerabilidades informáticas en los servicios *web* de la Pontificia Universidad Católica del Ecuador Ambato.

Objetivos Específicos

Fundamentar técnicamente los riesgos de seguridad en los aplicativos *web* de la Pontificia Universidad Católica del Ecuador Ambato

Diagnosticar los tipos de vulnerabilidades en los servicios *web* de la Pontificia Universidad Católica del Ecuador Ambato, para el mejoramiento de los niveles de seguridad.

Desarrollar un *benchmarking* de los resultados obtenidos en la prueba parcial del modelo de mitigación de vulnerabilidades para la medición de su grado de efectividad.

2.6 Delimitación Funcional

¿Qué será capaz de hacer el producto final del proyecto de titulación?

Dar a conocer las vulnerabilidades que los servicios *web* poseen y que deben ser corregidas en el menor tiempo posible para evitar que personas ajenas puedan tener acceso a la información.

Dividir los activos de la organización y determinar los que se encuentren más vulnerables.

¿Qué no será capaz de hacer el producto final del proyecto de titulación?

Reportar automáticamente la detección de vulnerabilidades.

Capítulo 3

Marco Teórico

3.1 Historia y evolución de la Seguridad Informática

El sitio *web* Definicion.de (2018), indica que: "la palabra seguridad viene del latín seguritas, que significa libre de peligro, daño o riesgo"; es así que, Anderson (1980) elabora el primer escrito relacionado a la seguridad informática, "*Computer Security Threat Monitoring and Surveillance";* donde por primera vez, se conoce palabras como: riesgo, amenaza, vulnerabilidad y penetración, las que hoy en día son usadas en un mundo digitalizado; cabe mencionar, que con los primeros computadores, los esfuerzos se centraban en evitar que se presenten fallas del sistema operativo o infecciones de virus (grupocontrol, 2010), pero con el uso de internet, los esfuerzos se enfocaron en proteger los datos mediante la creación de políticas de seguridad y la implementación de sistemas de seguridad perimetral.

Es así que en los inicios, el objetivo de un atacante era ingresar a un sistema e infectarlo de virus, sin intención de réditos económicos. Actualmente, el atacante se enfoca en los datos, por lo que el concepto de Seguridad Informática ha cambiado, es así que, actualmente se habla de Seguridad de la Información cuyo principal objetivo es alinear la seguridad con los objetivos y estrategias del negocio de las empresas. Es por este motivo, que se enfocan en proteger la información y evitar extorsiones para la recuperación de la información.

3.2 Estudio de conceptos y definiciones de aplicaciones *web*

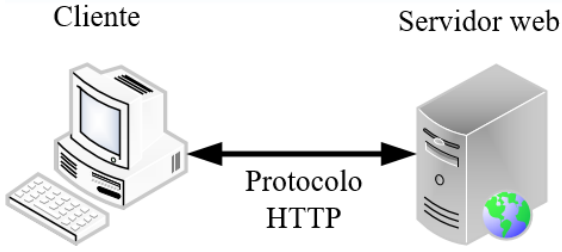
Las aplicaciones *web* son utilizadas por la mayoría de organizaciones, para brindar un servicio a sus clientes internos o externos, y que se extienden rápidamente a través de redes públicas y privadas. Para los *hackers,* la probabilidad de encontrar una aplicación *web* vulnerable es cada vez mayor (Salazar Carpió, 2013), al considerar que una aplicación es un sistema que se accede desde internet o intranet y conforman una clase especial de aplicación de *software* que se construye con ciertas tecnologías y estándares.

De lo indicado anteriormente, Oliveros, Danyans, & Mastropietro (2014) las clasifican en: "*web* documentales, *web* interactivas, *web* transaccionales, *web* basadas en flujos de trabajos, *web* colaborativas y *web* social", cada tipo de aplicación *web* debe tener un grado de aseguramiento en su desarrollo, ya que con los avances de la tecnología, son un blanco de ataque para quien desea obtener información de manera fraudulenta mediante la búsqueda de debilidades en su diseño o desarrollo para luego solicitar grandes cantidades de dinero en recuperar la información secuestrada, caso contrario es destruida sin poder recuperarla, lo que genera pérdidas para la organización.

También, considerar que las debilidades en el desarrollo no pueden ser mitigadas en su totalidad, sino que deben ser gestionadas por medio de políticas y buenas prácticas de uso (Kamlofsky, Colombo, Sliafertas, & Pedernera, 2015). Con el avance de la tecnología se descubren nuevas vulnerabilidades y se analizan las salvaguardas a ser aplicadas, por lo que un sistema siempre se verá afectado por una debilidad.

En tal sentido, Luján (2002) define que una aplicación *web* es un tipo especial de aplicación cliente-servidor, en el que, el cliente, el servidor y el protocolo mediante el que se comunican, están estandarizados y no han de ser creados por el programador de aplicaciones, como se muestra en la siguiente figura.

Figura 1.- Comunicación básica de una aplicación *web*



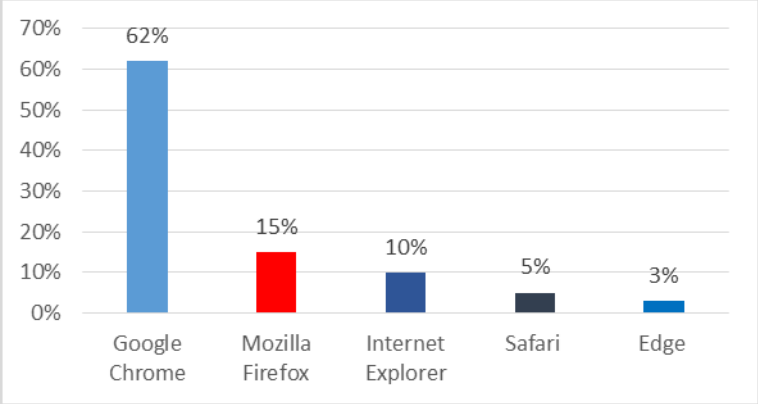
Fuente: tomado de (Lujan, 2002)

En la figura anterior, se aprecia que el Protocolo de Transferencia de Hipertextos (HTTP) permite la comunicación entre el cliente y el servidor, lo que facilita el intercambio de información.

Sin embargo, Pressman (2010) menciona que: con el avance de la tecnología las aplicaciones *web* han evolucionado hacia ambientes integrados con bases de datos corporativas y aplicaciones de negocio; es por ello, que las aplicaciones *web* se fundamentan en la arquitectura cliente/servidor, cuyos componentes son la capa de presentación, la capa de negocio y la capa de datos, con lo que se facilita el mantenimiento del aplicativo y se brinda mejor seguridad a los datos, ya que no están expuestos directamente al mundo exterior; en éste punto se debe considerar que los elementos principales para que una aplicación *web* funcione son el cliente *web* y el servidor *web*, los que se describen a continuación:

El cliente *web*.- Es definido por Lujan (2002) como un programa con el que interacciona el usuario para solicitar a un servidor *web*, el envío de los recursos que desea obtener mediante una consulta HTTP, dentro de los clientes *web* se encuentran aplicativos diseñados para consumir recursos de servidores *web*, navegadores o visualizadores (*Internet Explorer, Firefox, Opera, Safari, Google Chrome*), es así que Iteracy (2017) en su publicación realizada, da a conocer las estadísticas de uso de los clientes *web* de escritorio a nivel mundial, como se muestra en el gráfico siguiente:

Gráfico 1.- Estadísticas de uso de navegadores en equipos de escritorio

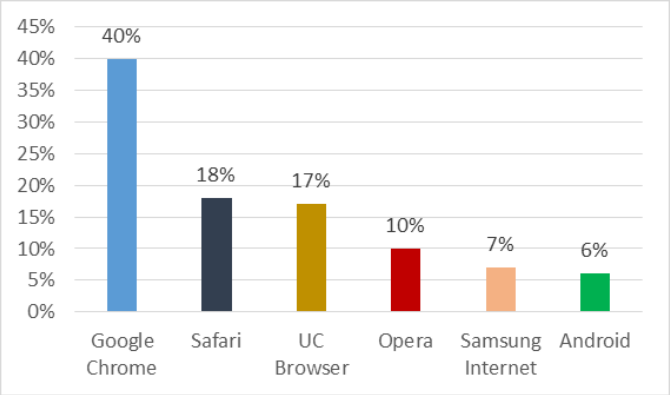


Fuente: tomado de (Iteracy, 2017)

En el gráfico anterior, se aprecia que el navegador *web* de escritorio más usado es *Google Chrome* con el 62%, debido a que las búsquedas realizadas son más rápidas y el consumo de memoria es

mucho menor que sus competidores, lo que también se corrobora en los clientes *web* para dispositivos móviles, como se muestra en el siguiente gráfico:

Gráfico 2.- Estadísticas de uso de navegadores en equipos móviles

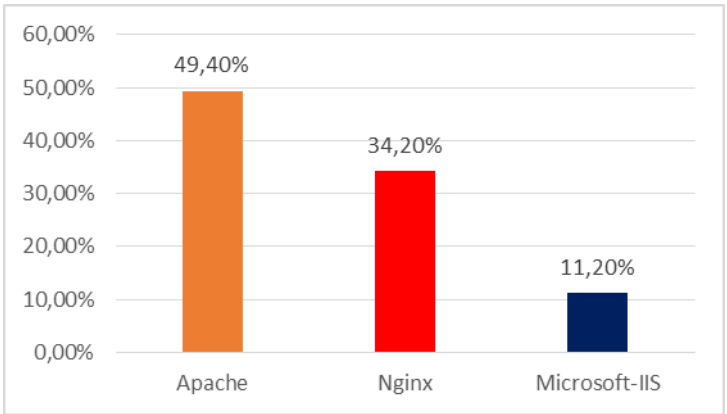


Fuente: tomado de (Iteracy, 2017)

En el gráfico anterior se observa que el navegador más utilizado en dispositivos móviles es *Google Chrome* con el 40% y en segundo lugar, se encuentra *Safari* con el 18% de aceptación.

El servidor *web*.- Es un programa que espera permanentemente las solicitudes de conexión mediante el protocolo HTTP (Medina, 2014), los más utilizados a nivel mundial tenemos *Apache*, *Internet Information Services y Nginx*, a lo que W3Techs (2017) indica que, de los tres servidores *web* más utilizados en la actualidad, *Apache* es el de mayor uso, como se muestra en el gráfico siguiente:

Gráfico 3.- Estadísticas de uso de servidores *web*



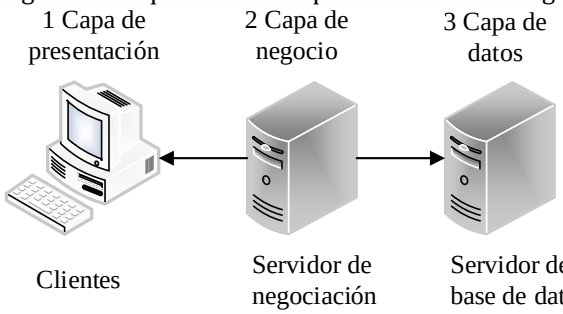
Fuente: tomado de (W3Techs, 2017, p. 3)

En el gráfico anterior, se observa que actualmente *Apache* lidera el mercado con el 49.40% y su competidor, *Nginx*, alcanza el 34.20%; pero cabe mencionar, que a julio de 2014 *Apache* lideraba con un 60.40% mientras que *Nginx* alcanzaba un 21% e IIS llegaba al 13%. Sin embargo actualmente el servidor *web Nginx* posee un 34.20% de uso, ha ganado terreno frente a su competidor *Apache*, debido al mejor rendimiento que presenta frente al resto de sus competidores.

También, un punto importante al momento de diseñar aplicaciones *web*, es la segmentación por capas y la distribución por niveles, entre los que destacan:

a) La segmentación por capas, en donde Alfsan (2012) menciona que el término capa, hace referencia a la forma en que una aplicación *web* es dividida desde el punto de vista lógico; es decir, que se divide a la aplicación en una capa de presentación que se encarga de la entrada y salida de información con el usuario, la capa de negocio se encarga de gestionar y procesar los datos proporcionados por el usuario y la capa de datos se ocupa de almacenar los datos en un sistema de base de datos, como se muestra en la siguiente figura.

Figura 2.- Arquitectura de aplicaciones *web* – Segmentación por capas

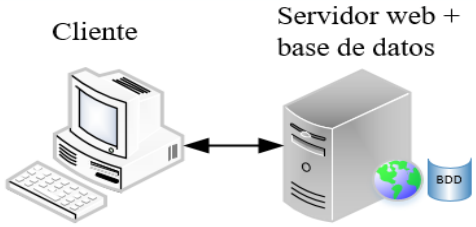


Fuente: elaboración propia a partir de literatura revisada

b) La distribución por niveles, indica la manera en que las capas lógicas de la aplicación *web* se encuentran distribuidas físicamente en los servidores (Alfsan, 2012), existen varias maneras de distribuir, entre las cuales se tiene:

- Un nivel: se aloja en un solo servidor todas las capas lógicas del aplicativo *web*; es decir, que: el servicio *web*, el servicio de aplicaciones y el servicio de base de datos se despliegan en un mismo equipo, como se indica en la siguiente figura.

Figura 3.- Arquitectura de aplicaciones *web* – un nivel



Fuente: elaboración propia a partir de literatura revisada

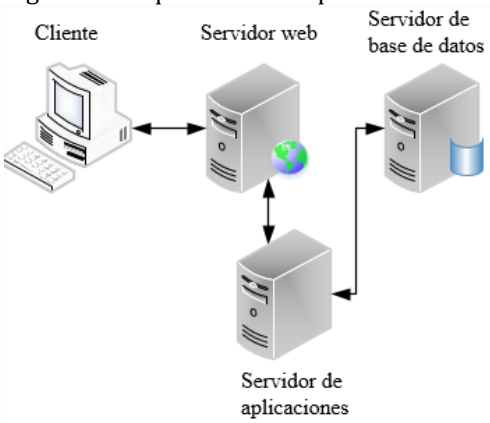
- Dos Niveles: se aloja el servicio *web* y el servicio de aplicaciones en un equipo y el servicio de bases de datos en un equipo diferente, como se indica en la figura siguiente.

Figura 4.- Arquitectura de aplicaciones *web* – dos niveles

Fuente: elaboración propia a partir de literatura revisada

- Tres Niveles: Se dispone de equipos independientes para cada servicio, como se indica a continuación.

Figura 5.- Arquitectura de aplicaciones *web* – tres niveles



Fuente: elaboración propia a partir de literatura revisada

La ventaja de tener separado los servicios por niveles, es incrementar la escalabilidad del sistema de cara a un mayor rendimiento y seguridad de la información (Lujan, 2002). Como se puede observar, en las imágenes, una separación en dos o tres niveles ofrecen mayor seguridad, al tener únicamente al servidor *web* expuesto al internet, en caso de sufrir ataque o daño alguno, los datos están salvaguardados en otro servidor, lo que reduce el Tiempo de Recuperación del Servicio (RTO) en caso de requerir la restitución del servicio.

3.3 Elementos del análisis de riesgos informáticos

El proceso de análisis de riesgos informáticos recoge información sobre los activos que posee la empresa, identifica las amenazas sobre los activos, determina qué salvaguardas se aplican para minimizar las amenazas, estima el impacto que tiene una amenaza e interpreta el significado del impacto (Sotelo, Torres, & Rivera, 2012), a lo que también Duque (2010) cita que, la gestión de riesgos informáticos es la estructuración lógica de las acciones a tomar para minimizar las debilidades o problemas detectados en el análisis.

De acuerdo a lo anterior, Pérez (2014) indica que, la mayoría de organizaciones con profesionales de seguridad, no tienen claro el cómo un riesgo informático puede convertirse en una falla organizacional, por lo que deben acogerse a las mejores prácticas de seguridad informática para evitar los riesgos y mantener o mejorar los tiempos de disponibilidad de los aplicativos *web*. Dentro de los elementos que intervienen en un análisis de riesgos, se

encuentran: los activos, riesgos, vulnerabilidad, amenaza, salvaguarda e impacto, los que se interrelacionan entre sí, como se indica en el esquema siguiente.

Esquema 1.- Elementos del análisis de riesgos potenciales

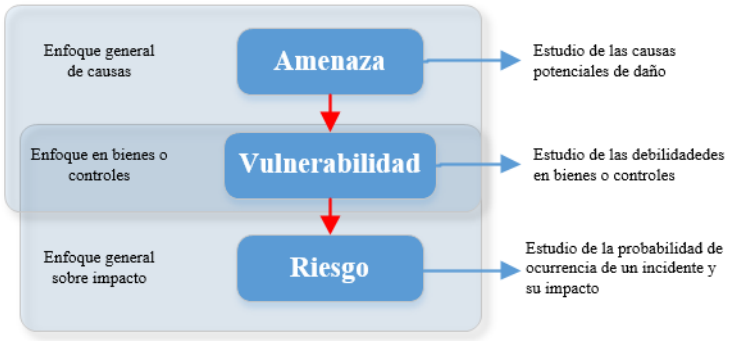
Fuente: tomado de Consejo Superior de Administración Electrónica de España (2012)

En el esquema se evidencia, que los activos de una organización están expuestos a amenazas, y que su valor es el principal interés de quienes lo desean, también que las amenazas generan degradación al activo con una cierta frecuencia lo que logra un impacto negativo y un riesgo para las instituciones.

Activo.- Es un bien que tiene valor para la organización al tener en cuenta la utilidad que presta para la consecución de las operaciones comerciales (Vanegas & Pardo, 2014), es por eso que, un activo necesita de las seguridades necesarias para garantizar que la organización logre los objetivos planteados. Como activos se puede encontrar: *software*, *hardware*, comunicaciones, infraestructura, información o datos, recursos administrativos, recursos humanos, servicios, entre otros.

Riesgo.- Es la posibilidad de que algo ocurra o impacte negativamente sobre un activo, al existir una relación estrecha entre amenaza, vulnerabilidad y riesgo, como se muestra en la figura siguiente, la amenaza puede causar un impacto negativo sobre el activo de la organización, siempre y cuando posean vulnerabilidades o un fallo en los controles que lo administran, en este sentido, Prandini & Pallero (2013) mencionan que una vulnerabilidad al ser explotada por una amenaza, pone en riesgo a una organización, al generar un impacto negativo en su credibilidad.

Figura 6.- Conceptos involucrados y su relación



Fuente: tomado de Prandini & Pallero (2013)

Vulnerabilidad.- Es la falta de controles en el diseño de un proceso o de un bien, que puede ser aprovechada por una amenaza (Prandini & Pallero, 2013), por lo que, en el campo de la seguridad de la información, las vulnerabilidades obligan a los administradores de seguridad a tomar nuevos retos a mejorar las soluciones implementadas para proteger todos los activos de acuerdo a la importancia que la institución los clasifique, es así que *Open web Application Security Project* (OWASP, 2013) organización que se dedica a determinar y combatir los problemas de seguridad de las aplicaciones *web*, da a conocer las diez vulnerabilidades más peligrosas identificadas:

- **A1 Inyección.** Las fallas de inyección, tales como SQL, OS, y LDAP, ocurren cuando datos que provienen de fuentes no confiables son enviados como parte de un comando o consulta real.
- **A2 Pérdida de autenticación y gestión de sesiones**. Permite a los atacantes secuestrar, claves, *token* de sesiones, o explotar otras fallas de implementación al hacerse pasar por un usuario identificado en el sistema.
- **A3 Secuencia de comandos entre sitios (XSS).** Las fallas XSS permite a los atacantes ejecutar secuencia de comandos en el navegador de la víctima los cuales pueden secuestrar las sesiones del usuario, destruir sitios *web* o dirigir al usuario hacia un sitio malicioso.

- **A4 Referencia directa insegura a objetos.** Una referencia directa a objetos ocurre cuando un desarrollador expone una referencia a un objeto de implementación interno sin un chequeo de control de acceso u otra protección.
- **A5 Configuración de seguridad incorrecta.** Una buena seguridad requiere definir e implementar una configuración segura para la aplicación, esto incluye mantener todo el *software* actualizado, incluidas las librerías de código utilizadas por la aplicación.
- **A6 Exposición de datos sensibles.** Los datos sensibles requieren de métodos de protección adicionales tales como el cifrado de datos y tener las precauciones especiales en un intercambio de datos con el navegador.
- **A7 Ausencia de control de acceso a funciones.** Las solicitudes de acceso a recursos no se verifica, los atacantes pueden realizar peticiones sin la autorización apropiada.
- **A8 Falsificación de peticiones entre sitios (CSRF).** Esto permite al atacante forzar al navegador de la víctima para generar pedidos que la aplicación vulnerable piensa que son peticiones reales realizadas por la víctima.
- **A9 Utilización de componentes con vulnerabilidades conocidas.** La utilización de componentes con vulnerabilidades, debilitan las defensas de la aplicación y permiten ampliar el rango de posibles ataques e impactos.
- **A10 Redirecciones y reenvíos no validados.** Sin una validación apropiada, los atacantes pueden redirigir a las víctimas hacia sitios de *phishing* o *malware*, o utilizar reenvíos a páginas no autorizadas.

Amenaza.- Según el sitio *web* definicionabc.com (2018) describe a la amenaza como: la posibilidad de que un peligro se haga realidad, el cual puede generar daños sobre los activos de una institución por la falta de previsiones.

Según Erb (2009), la seguridad informática tiene como propósito garantizar la confidencialidad de la información al evitar que personas no autorizadas accedan a la información, la integridad

asegura que la información no sea alterada o modificada desde su emisor hacia su receptor, la disponibilidad garantiza que la información esté disponible en todo momento, y la autenticidad al garantizar que los datos provengan de fuentes confiables.

Como indica Mieres (2009), es necesario que los usuarios opten por buenas costumbres para proteger la información, con lo cual se garantiza que las personas ajenas no puedan sacar provecho de las debilidades humanas, para ello se debe conocer los peligros latentes, y cómo detenerlos a través de mecanismos de prevención, es así que el Consejo Superior de Administración Electrónica de España (2012) identifica las amenazas según su origen en:

- De origen natural.- Cuando son provocados por la naturaleza, sin intervención del hombre.
- De origen industrial.- Cuando tienen como origen acciones realizadas por el hombre.
- Errores no intencionados.- Cuando son provocados por el hombre, pero no tiene intención de generar daños.
- Ataques Intencionados.- Cuando son provocados por el hombre, pero con clara intención de causar daños.

Salvaguardas informáticas.- Son controles que se aplican a los activos de una organización para minimizar las vulnerabilidades, limitar el impacto y reducir el riesgo. También se puede citar la definición que da el Consejo Superior de Administración Electrónica de España (2012), como las medidas que se toman a nivel técnico para proteger los activos y reducir el riesgo, al cumplir funciones específicas, como las indicadas en el cuadro siguiente.

Cuadro 1.- Funciones de las Salvaguardas

Función	**Detalle**
Detección	Informa que el ataque está en ejecución mediante alertas de seguridad, con lo que se permite que entren en operación otras medidas que detengan el avance del ataque.
Disuasión	Actúan antes del incidente, reduciendo las probabilidades de que ocurra.

Prevención	Reduce las oportunidades de que un incidente ocurra. Si la salvaguarda falla y el incidente llega a ocurrir, los daños son los mismos.
Limitación del impacto	Cuando se reduce las consecuencias de un incidente.
Corrección	Se aplican luego un incidente para reducir los daños.
Recuperación	Permite regresar al estado anterior al incidente. Lo que permite reducir el daño en un período de tiempo.
Monitorización	Monitorean para detectar ataques en tiempo real, lo que permite reaccionar sobre el incidente para limitar el impacto.
Concienciación	Son las actividades de formación de las personas anexas al sistema que pueden tener una influencia sobre él.

Fuente: tomado de Consejo Superior de Administración Electrónica de España (2012)

Impacto de los ataques informáticos.- Es la materialización de una amenaza sobre un activo, puede generar la destrucción de un activo, incrementa el peligro en la integridad del sistema de información, la pérdida de autenticidad, de confidencialidad o de disponibilidad de un servicio (Areitio, 2008), es así que la revista digital Economiadigital (2017) da a conocer los mayores ataques informáticos de 2016, entre los cuales está el robo de información bancaria, la publicación de información personal de los usuarios, el robo de cuentas de correo electrónico y ataques de denegación de servicio, los que tuvieron un impacto costoso para las empresas atacadas, al pagar millonarias sumas de dinero para que la información sea devuelta, el tener degradación o pérdida de uno o más servicios informáticos y el afrontar su credibilidad ante el resto de usuarios o clientes.

3.4 Computación en la Nube

La computación en la nube hace referencia a los servicios que son ofrecidos por un proveedor y son consumidos por medio de internet (Ávila, 2011); es decir, que el cliente no conoce de la infraestructura desplegada para ofrecer el servicio. Existen tres maneras principales de ofrecer un servicio en la nube, los que se detallan a continuación:

- ***Software* como servicio (SaaS**).- El proveedor entrega una infraestructura completa de aplicaciones, las que están listas para ser usadas, el cliente no tiene acceso a los servidores, pero si a la administración del *software*.
- **Plataforma como servicio (PaaS***).*- El proveedor proporciona toda la infraestructura necesaria para que el cliente despliegue sus servicios, en el caso de necesitar más recursos, el proveedor es el encargado de incrementarlos, el cliente tiene acceso a los entornos contratados pero no a la infraestructura.
- **Infraestructura como servicio (IaaS).-** El proveedor proporciona al cliente acceso a la infraestructura contratada, los que son pagados según su consumo, en éste caso el cliente configura todos los recursos necesarios para desplegar sus aplicaciones.

Es así que, con el crecimiento vertiginoso que ha tenido en los últimos años la adopción de los nuevos modelos de prestación de servicios en las empresas, Márquez Alcañiz, Rosado, Mellado, & Fernández-Medina Patón (2014), afirman que: la migración hacia la nube trae nuevos desafíos en la gestión de seguridad de la información, debido a que el proveedor es quien gestiona la seguridad de la infraestructura y deben acogerse a la manera en que éste lo administra, pero en la seguridad de las aplicaciones *web* el proveedor no garantiza la mitigación de vulnerabilidades, pues esto depende de las seguridades que el cliente aplique.

3.5 Estado del Arte

Se debe aclarar que la seguridad informática debe ser tratada como un proceso de importancia para la consecución de los objetivos institucionales, al estar alineada al negocio en el apoyo a la toma de decisiones tecnológicas, a pesar de que, en muchas organizaciones el personal de tecnología no cuenta con el respaldo de la dirección para implementar medidas de seguridad necesarias, al no tener el tiempo suficiente para su gestión, las que son vistas como tiempo improductivo por los directivos.

Las metodologías de análisis de riesgo son fundamentales en la gestión de riesgos informáticos, ayudan a identificar las fortalezas y debilidades con las que cuenta una organización en cada uno

de los activos informáticos que posee, con el propósito de valorar el nivel de protección de la información, evaluar e identificar los riesgos y sus vulnerabilidades y estimar el impacto que tendrían al materializarse una amenaza.

En el análisis realizado por Alemán & Rodríguez (2015), se indica que las metodologías *Construct a platform for Risk Analysis of Security Critical System* (Coras) elaborada a partir de 2001 por un grupo de investigación noruego, la Metodología de Análisis y Gestión de Riesgos de IT (Magerit), creada en 1997 y actualizada a la versión 3 en 2012 por el Consejo Superior de Administración Electrónica de España *y Operationally Critical Threat, Asset and Vulnerability Evaluation* (Octave), diseñada por la Universidad Carnegie Mellon de Estados Unidos en el año 2001, poseen un procedimiento sistematizado para el análisis de riesgos al planificar las salvaguardas que se apliquen para minimizar su impacto y también hacen uso de herramientas de apoyo para el análisis de la seguridad informática de la organización. Si bien las metodologías ayudan a detectar los fallos de seguridad, también es importante indicar que, para que un programa informático sea seguro no basta con utilizarlo correctamente, hace falta que esté libre de fallos, que no tenga puertas traseras y que toda su funcionalidad esté documentada (de Bustos Pérez, 2002).

Para analizar la seguridad informática en las organizaciones, existen empresas que se dedican a éste fin, entre ellas Acunetix (2016) afirma que: de las páginas *web* analizadas en los últimos 12 meses, existe un 55% de sitios que tienen al menos una vulnerabilidad de alta peligrosidad en comparación del 46% del año anterior y que el 84% de los sitios analizados presentan vulnerabilidades de grado medio, encontrándose una reducción en las vulnerabilidades de tipo inyección SQL (*Structured Query Language*), debido a que los motores de bases de datos poseen medidas de seguridad propias y no dependen únicamente del aplicativo.

En el estudio realizado por Abril, Pulido, & Bohada (2014), se menciona que los incidentes relacionados con seguridad informática comprometen los activos de las empresas, lo que genera la necesidad de implementar sistemas de seguridad para que se minimicen las consecuencias no deseadas, se debe considerar que, para mejorar la seguridad no basta con la implementación de nuevos equipos de seguridad, sino que depende en gran medida de un compromiso de los altos

directivos en implementar políticas de seguridad que protejan el activo más valioso, la información (Sullivan, 2016).

Así también, en el estudio realizado por *Verizon Business RISK Team* (2008) a más de 500 incidentes relacionados con seguridad informática en el período comprendido entre los años 2004 y 2007, se evidencia que el 73% de los incidentes tienen origen externo, al comprometer 30.000 registros mientras que el 39% tienen originen en los socios, los que comprometieron 187.000 registros y el 18% son de origen interno pero que tienen un mayor impacto, al comprometer 375.000 registros, como conclusión se tiene que: los incidentes por el personal interno son más peligrosos que los originados por personas externas, a pesar de que son en menor cantidad, el nivel de impacto es mayor, mientras que los externos son en mayor número pero el nivel de impacto es menor.

También se considera lo realizado por *Haystax Technology* (2017), en el estudio a más de 300.000 miembros de la comunidad de seguridad informática, encuentra que el 74% de las empresas se siente vulnerable a ataques internos, de éstos el 60% del riesgo es representado por usuarios con acceso a información confidencial, seguido por los socios con un 57% y con un 51% por usuarios regulares.

De los análisis de seguridad informática realizados en América Latina, cabe mencionar la investigación sobre ciberseguridad realizada por el Banco Interamericano de Desarrollo (2016), donde se revela que cuatro de cada cinco países de América Latina no tienen estrategias de seguridad o planes de protección de la infraestructura crítica, entre estos se encuentra Ecuador, del que se manifiesta que, a pesar de que no ha desarrollado una estrategia nacional de seguridad cibernética, ha hecho avances en los últimos años para fortalecer su capacidad de abordar las amenazas informáticas, añade además que, los ataques cibernéticos se incrementaron significativamente en los últimos años pero la mayoría de los afectados no conocían los medios más eficaces para poder denunciar los incidentes.

Para mitigar la problemática detallada en el párrafo anterior, el Estado ecuatoriano, por medio de la Secretaría Nacional de Inteligencia del Ecuador (SENAIN), promueve la socialización de los

organismos de inteligencia, cómo funcionan y cuál es su labor en el mantenimiento de la seguridad integral atreves de la academia.

Es así que, en el Ecuador se crea la Corporación Ecuatoriana para el Desarrollo de la Investigación y la Academia (CEDIA), que agrupa a las universidades del Ecuador para ofrecer servicios relacionados con tecnología, como es el caso del Equipo de Respuesta a Incidentes (*CSIRT)*, el servicio que monitorea todos los eventos de seguridad informática. En la primera encuesta de seguridad realizada por la RED CEDIA (2014), los resultados indican que: el 46% de las universidades miembro no realizan ningún tipo de revisión de seguridad a sus sistemas, mientras que el 36% los evalúa una vez al año y, apenas un 18% lo hacen más de tres veces al año.

Es así que, en base a la información recabada, el presente proyecto de investigación utiliza las mejores prácticas para analizar los servicios *web* de la PUCE Ambato alojados localmente o en la nube, identificar vulnerabilidades informáticas, proponer contramedidas que minimicen el impacto para que los servicios ofrecidos sean seguros y confiables.

Capítulo 4

Metodología

4.1 Diagnóstico

La investigación se enfoca en los servicios *web* que la Pontificia Universidad Católica del Ecuador Ambato ofrece a sus clientes internos o externos, con el propósito de mitigar las vulnerabilidades detectadas, igualmente se aplica una investigación cuantitativa y no experimental longitudinal, ya que se miden los resultados obtenidos antes y después de aplicar las medidas de mitigación a las vulnerabilidades detectadas en los servicios *web*, con la finalidad de lograr una mejor caracterización.

4.2 Métodos Aplicados

Se utiliza el método de investigación inductivo, que permite generar observaciones generales de las vulnerabilidades a partir de las más específicas y el método deductivo, que permite identificar las vulnerabilidades desde las más generales hasta las más específicas, adicional se mantienen entrevistas con el personal del Departamento de Tecnología de la institución, Apéndice A, para conocer los servicios prestados, su estructura y procedimientos que posee la dependencia para tratar incidentes de seguridad, también se ejecutan tareas de campo que permiten obtener información referente a la infraestructura física de los activos, que son relevantes para el desarrollo de la investigación.

Además se debe indicar que, la población seleccionada es de 8 servicios *web*, los que son analizados con una aplicación especializada en seguridad informática que permita encontrar todas las debilidades que posean.

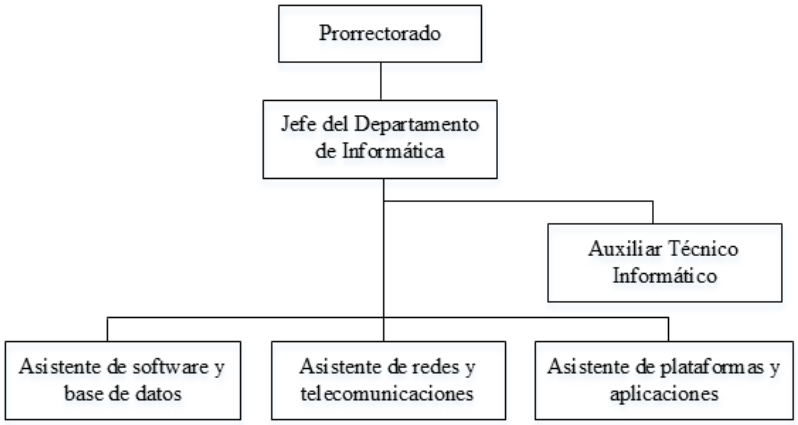
Para iniciar es importante describir la estructura actual del Departamento de Informática con la finalidad de comprender su accionar en la administración de los servicios *web* de la PUCE Ambato.

4.3 Caracterización del Departamento de Informática de la PUCE Ambato

Generalidades

El Departamento de Informática de la PUCE Ambato, fue creado para satisfacer las necesidades de tecnología de la institución, es decir que, es el encargado de la administración de la infraestructura tecnológica existente, dar asesoría en la adquisición de nuevas tecnologías que se deseen implementar. Actualmente, posee cinco colaboradores, los que tienen definidas sus funciones en base a cargos establecidos, como se muestra en el esquema siguiente.

Esquema 2.- Organigrama estructural Departamento de Informática



Fuente: tomado de http://www.pucesa.edu.ec (2016)

La PUCE Ambato, cuenta con servicios informáticos para la gestión académica, financiera y administrativa, para lo cual posee desarrollos *web* internos con arquitectura cliente/servidor, desarrollados en lenguajes PHP, *Visual Studio* 2010 (ASP.NET v4.0), también posee desarrollos adquiridos, entre los principales se tiene:

- Gestión académica, cuenta con el sistema *Academics*, desarrollado en su totalidad en la PUCE Ambato.
- Gestión administrativa, cuenta con el sistema *Squarenet*, es un sistema adquirido.
- Gestión financiera, se cuenta con el sistema Saci, que es un desarrollo adquirido, consta de módulos para la gestión de activos y facturación electrónica.
- Gestión de biblioteca, cuenta con el sistema Siabuc, es una aplicación adquirida, consta de módulos para préstamos de libros, consulta interna de bibliografía,

también cuenta con un módulo *OPAC,* que permite la consulta de bibliografía por medio de un servicio *web*.

- Gestión de trabajos de titulación, cuenta con el sistema *Dspace*, que es *software* libre.
- Administración de impresiones, cuenta con el sistema *Papaercut*, que es un sistema adquirido.
- Gestión de requerimientos de tecnología, cuenta con *Spiceworks,* que es *software* libre.
- Administración de aulas virtuales, cuenta con *Moodle,* que es *software* libre.
- Administración de planes operativos, cuenta con el Tablero de Control, que es un trabajo de titulación donado a la universidad.

La PUCE Ambato, cuenta con 10 servidores virtuales y 11 servidores físicos, con varias versiones de sistema operativo, como: *Linux Centos, Oracle Solaris* y *Windows Server,* cuya administración está a cargo del administrador de red e infraestructura. Además, cuenta con una infraestructura en la nube, cuyo proveedor y administrador es *Amazon web Services*, dentro de éste servicio se mantiene dos servidores, uno de base de datos y otro para el servicio *web*.

En las instalaciones de la Universidad, se encuentra su cuarto de datos que está ubicado en el Bloque I, Departamento de Informática, el que alberga los servidores y equipos de comunicación, cuyo acceso físico es permitido únicamente para el Jede del Departamento y el administrador de red e infraestructura, cualquier acceso adicional debe ser autorizado por los responsables.

4.4 Selección de la metodología para el análisis de riesgos

"Una metodología es un conjunto de acciones que ayudan a controlar de manera eficiente y eficaz los procesos que se dan para alcanzar los objetivos propuestos" (Cortés & Iglesias, 2004), mientras que en el campo de la seguridad informática. Alemán & Rodríguez (2015) citan a las metodologías, como: "la disciplina que se articula en las organizaciones para proponer una forma más segura de cuidar la información y los recursos tecnológicos", para

proteger la infraestructura tecnológica se necesita de procedimientos que determinen las mejores prácticas para identificar las amenazas a los que están expuestos y tomar las mejores decisiones.

En el estudio realizado por Molina-Miranda (2017) indica que, las metodologías más destacadas para el análisis de gestión de riesgos informáticos son *Coras*, *Magerit* y *Octave*; es así que, en el siguiente cuadro se realiza una comparación de las metodologías indicadas.

Cuadro 2.-Comparación Metodologías Coras, Magerit y Octave

Metodología	***Coras***	***Magerit***	***Octave***
Definición	Metodología desarrollada por un grupo de investigación noruego, tomándose como base modelos de estimación de seguridad informática.	Es creada en España en 1997 y actualizada en 2012 a la versión 3, ayuda a que las instituciones estén preparadas para procesos de certificación.	Desarrollado en EEUU en el año 2001 por la Universidad *Carnegie Mellon*, analiza información que permita diseñar planes de protección.
Características	Es adecuada para el desarrollo, mantenimiento y mejora de sistemas heredados. Permite la creación de los modelos por medio del lenguaje unificado de modelado. Permite la reutilización de bibliotecas. Para la comunicación de los integrantes del grupo de trabajo, posee formatos estándares.	Concientiza a los responsables de las organizaciones de la existencia de riesgos informáticos y de la necesidad de gestionarlos. Permite planificar, identificar y mitigar los riesgos de los activos. Permite que la organización esté lista para procesos de certificación.	Estudia los riesgos organizacionales, principalmente en los aspectos relacionados con el día a día de las empresas. Construye los perfiles de amenazas informáticas, basado en activos. A partir de los criterios de *Octave*, se pueden desarrollar nuevas metodologías.
Fases de la Metodología	**Presentación:** da a conocer los objetivos y alcance del análisis. **Análisis:** determina las entrevistas que se utilizan para validar la información recabada. **Aprobación:** el interesado aprueba el alcance y objetivos del análisis de riesgos. **Identificación de riesgos:** identifica las amenazas, vulnerabilidades, escenarios e incidentes. **Estimación de riesgo:** estima las probabilidades e impactos de los incidentes identificados. **Evaluación de riesgo:** se elabora el informe de riesgos para su revisión. **Tratamiento del riesgo:** permite determinar las salvaguardas a aplicar.	**Identificar activos:** obtiene el inventario de activos y su valoración. **Identificar amenazas:** permite determinar los peligros que pueden afectar a los activos. **Determinar las salvaguardas:** encontrar las mitigaciones a los riesgos de los activos. **Estimar el impacto:** determina el posible daño que tendría un activo si una amenaza se materializa. **Estimar el riesgo:** determina la posibilidad de que un activo sufra daños.	**Evaluación de la organización**: se identifican los acticos, se determina las amenazas, se establecen las medidas de seguridad aplicadas a los activos. **Identifican las vulnerabilidades:** se identifica las vulnerabilidades que afectan a los activos informáticos. **Desarrollo de un plan y una estrategia de seguridad**: se analizan los riesgos para determinar el impacto que puede tener la organización.

Ventajas	Utiliza herramientas de apoyo para el análisis de riesgos, un editor gráfico par el modelado basado en Microsoft Visio y utiliza lenguaje gráfico basado en *Unified Modelling Language* (UML). La visión general de como diferentes amenazas interaccionan entre sí para materializarse en riesgos concretos. Es una metodología muy útil para identificar vulnerabilidades y amenazas que afectan a los activos de la organización.	Posee un extenso archivo de inventarios en lo referente a recursos de información, amenazas y tipo de activos. Permite un análisis completo, cualitativo y cuantitativo. Información en idioma español, de acceso público sin tener que solicitar su uso. Es una metodología líder con buenos referentes de aplicación en Europa. Usa la herramienta PILAR para el análisis de riesgos.	Cada método aplicado puede ser adaptado a cada organización en un único entorno de riesgo. Involucra a todos los miembros de la organización. Posee una visión clara sobre la seguridad de la información de la organización.
Desventajas	No realiza un análisis de riesgo cuantitativo. No contempla los procesos y las dependencias de la organización. Acceso a información restringida, se necesita comprar la documentación para su uso. No reconocida en Ecuador.	No involucra a los procesos, recursos ni vulnerabilidades. No posee un inventario completo de políticas. Es una metodología conocida pero poco utilizada en Ecuador.	Utiliza muchos documentos en el proceso de análisis de riesgos. Se requiere de amplios conocimientos técnicos para su implementación. No define de forma clara los activos de la información. Se requiere de autorización para su uso. Poco reconocida en Ecuador. La documentación está en idioma inglés.

Fuente: tomado de Forigua & Ballesteros (2006), Huerta (2012), Urrutia (2014), Alemán & Rodríguez (2015)

Con la finalidad de seleccionar la metodología a ser utilizada en el análisis de vulnerabilidades, se evalúan 6 factores de las metodologías *Coras, Magerit* y *Octave*.

Cuadro 3.- Factores Selección Metodología

Factor Comparativo	***Coras***	***Magerit***	***Octave***
Documentación en Español	No	Sí	No
Documentación de libre acceso	No	Sí	No
Realiza inventario completo de activos	No	Sí	No
Posee herramientas informáticas de apoyo	Sí	Sí	Sí
Realiza análisis cuantitativo y cualitativo	No	Sí	No
Ideal para organizaciones principiantes en seguridad	Sí	Sí	No
Posee gestión completa de riesgos	Sí	Sí	Sí

Fuente: elaboración propia a partir de literatura revisada

Del análisis realizado, las metodologías *Coras* y *Octave* no permiten tener un análisis cualitativo y/o cuantitativo de los riesgos, y no consideran el riesgo residual, pero permiten realizar mejoras sobre una salvaguarda aplicada hasta minimizar en lo posible el impacto que pueda darse.

La metodología *Magerit* cumple con todos los parámetros evaluados, es ideal para organizaciones que inician un proceso de seguridad informática, además, mantiene un amplio inventario de activos al dividir en grupos, a la vez, posee mayor granularidad en la detección de riesgos y poder tomar las contramedidas necesarias para mitigarlos. Cuenta con una buena base documental dividida en tres obras, el método, catálogo de elementos y la guía de técnicas, las que están disponibles para su uso de manera pública, y la documentación se encuentra en idioma español.

Por lo que, la metodología *Magerit* es la seleccionada para el presente proyecto; ya que, por medio de las herramientas informáticas y la documentación disponible para su uso, se acopla para cumplir el objetivo propuesto, que es mitigar las vulnerabilidades informáticas en los servicios *web* de la PUCE Ambato.

4.5 Análisis de modelos aplicados al Sistema de Gestión de Seguridad de la Información

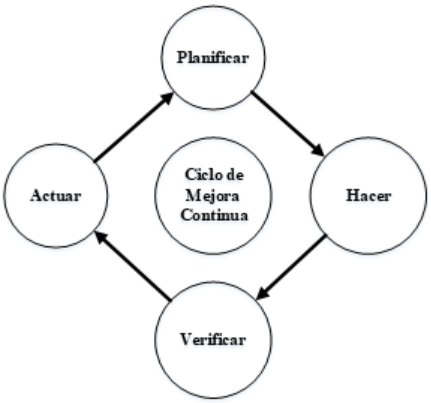
En éste apartado, se analizan los diferentes modelos que pueden ser aplicados en un sistema de gestión de riesgos informáticos, los modelos propuesto ayudan a la toma de decisiones, generan el involucramiento de los administradores de los servicios en las actividades de seguridad que

permita la toma de decisiones acordes a los nuevos avances tecnológicos, es así que se detallan los modelos que son aplicables al análisis de riesgos informáticos.

Modelo de Deming

El modelo fue creado a mediados del siglo XX por el profesor Edwards Deming, con el objetivo de mantener la mejora continua en las áreas fuertes que se debe mantener y los puntos de mejora en los que se debe actuar.

Figura 7.- Ciclo de mejora continua



Fuente: elaboración propia a partir de literatura revisada

Como se observa en la figura anterior, el modelo de Deming consta de cuatro etapas que son evaluadas en busca de la mejora continua, el sitio *web* pmg-ssi.com (2015), describe cada etapa como:

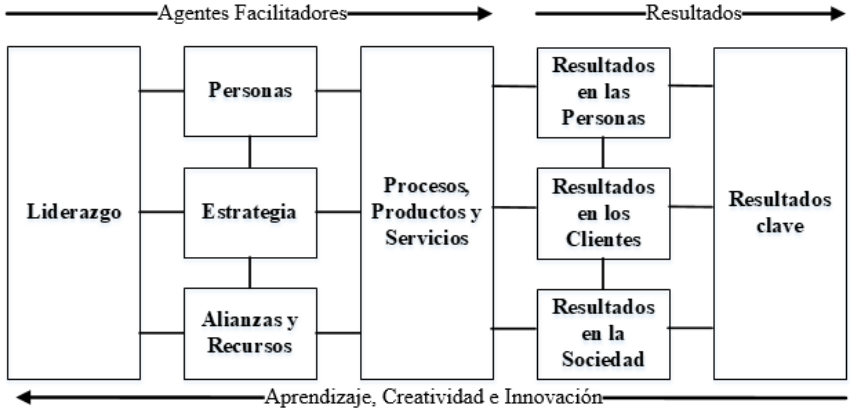
- Planificar.- propone la metodología a utilizar para el Sistema de Gestión de Seguridad de la Información; es decir, se define los objetivos, el alcance, el responsabilidades del personal, la estructura de la organización, los activos tecnológicos con que cuenta, además se debe establecer exclusiones si existiesen.
- Hacer.- Se define el tratamiento de los riesgos que se identifiquen, las salvaguardas y las prioridades durante la gestión de riesgos. También se define las métricas que permitan comparar los resultados obtenidos en cada medición, ya que pueden existir nuevos hallazgos en mitigaciones ya establecidas.
- Verificar.- Se debe llevar a efecto los procedimientos de monitorización y revisión de los errores generados en los resultados obtenidos en el procesamiento de la información, también debe verificar si todas las salvaguardas establecidas para mitigar los riesgos fueron efectivas.

- Actuar.- Se debe implementar todas las mejoras establecidas, y establecer la periodicidad con la que se llevarán a efecto, con la finalidad de establecer que todas las salvaguardas están bien definidas y cumplan el objetivo.

Modelo EFQM

El modelo fue diseñado en 1989 por la "*European Foundation for Quality Management"*, con el objetivo de ayudar a las empresas a posicionar su calidad como factor estratégico.

Figura 8.- Modelo EFQM



Fuente: tomado de www.efqm.es

Como se muestra en la figura anterior, el modelo EFQM, posee nueve criterios, cinco de criterios de agentes facilitadores y cuatro de criterios de resultados. Carrión García (2006), los describe como:

Agentes:

- Liderazgo: hace referencia al estilo en que la Gerencia logra los objetivos organizacionales.
- Estrategia y Planificación: se refleja la calidad en la estrategia dirigida hacia los grupos de interés.
- Gestión del personal: permite que el personal libere todo su potencial individual como grupal en bien de la empresa.
- Recursos: gestiona los procesos para el cumplimiento de las políticas de la organización.

Resultados:

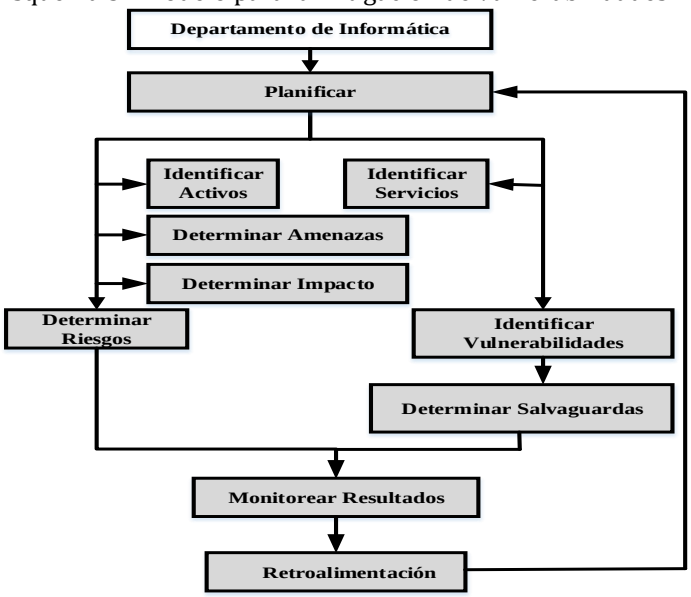
- Satisfacción del cliente: permite medir el grado de aceptación de los clientes a la calidad de los productos y servicios.
- Satisfacción del personal: mide el grado de satisfacción de los trabajadores de la empresa.
- Impacto de la sociedad: mide el grado de cumplimiento de la organización con la sociedad.
- Resultado del negocio: permite medir el grado de cumplimiento de los objetivos económicos previstos.

El modelo EFQM tiene un enfoque global, el que se aplica a procesos organizativos ya establecidos; con lo que, se mejora la satisfacción del cliente al ofrecer servicios de mejor calidad. En cambio, el modelo de *Deming* tiene un enfoque más técnico, centrado en el control estadístico de resolución de problemas, de lo expuesto cabe indicar que el modelo de *Deming* es el que se aplicara conjuntamente con la metodología *Magerit*.

4.6 Definición del modelo para la mitigación de vulnerabilidades informáticas en los servicios web de la Pontificia Universidad Católica del Ecuador Ambato

El modelo de mitigación de vulnerabilidades propuesto en la presente investigación, se enfoca en analizar las vulnerabilidades de los servicios *web* de la PUCE Ambato, alojados local o remotamente. Asimismo, se determinan los riesgos a los que están expuestos los activos informáticos; los que, por medio de una revisión continua y una retroalimentación sobre incidentes anteriores, se reduce al máximo las deficiencias encontradas.

Esquema 3.- Modelo para la mitigación de vulnerabilidades PUCE Ambato



Fuente: elaboración propia

El modelo descrito en el esquema 3, se basa en el modelo de mejora continua de *Deming*; el que, conjuntamente con la metodología *Magerit* dan paso a la definición del modelo para la mitigación de vulnerabilidades de la PUCE Ambato.

Las tareas del modelo propuesto en el presente estudio, se indica a continuación:

- Planificar
  - Análisis de la situación actual
  - Plan de Acción
  - Identificar Servicios
  - Identificar Activos
- Hacer
  - Determinar Amenazas
  - Determinar Impacto
  - Determinar Salvaguardas
  - Determinar Riesgos
  - Identificar Vulnerabilidades
- Verificar
  - Monitorear Resultados
- Actuar
  - Retroalimentación.

Planificar

La planificación según el modelo de *Deming*, determina la situación actual de la organización, el objetivo del análisis, los responsables, las estrategias, las actividades y las métricas del análisis.

Análisis de la situación actual.- Efectuada la revisión de las seguridades aplicadas a los servicios web de la PUCE Ambato, se ha observado que no existe un modelo que permita detectar las vulnerabilidades y aplicar controles para mitigar los mismos.

Dentro de los distintos aspectos a considerar en la seguridad de la información, se ha observado que; para la publicación de servicios web, no existe un procedimiento previo para detectar vulnerabilidades, si bien se ha observado que existen normas para los desarrollos propios no existe un procedimiento para los aplicativos adquiridos.

En cuanto a la seguridad física, se observa que existen controles para el acceso a los sitios en los que se alojan los activos como también se mantienen las seguridades a nivel lógico, al evitar el acceso a los servidores que brindan los servicios desde la red local de la institución.

Plan de acción.- Luego del análisis se ha identificado el proceso de mejora, al realizar un plan de acción que se muestra en el cuadro siguiente:

Cuadro 4.- Plan de acción modelo Deming

Objetivo	Estrategia	Actividades	Responsable	Indicador
Minimizar las vulnerabilidades en los servicios web de la PUCE Ambato, para mejorar los niveles de seguridad.	Utilizar aplicativos que permitan determinar las debilidades en los aplicativos web.	Determinar Riesgos. Identificar Activos. Determinar Amenazas. Determinar Impacto. Identificar Vulnerabilidades. Identificar Servicios. Determinar Salvaguardas.	Administrador de Infraestructura	Porcentaje de vulnerabilidades mitigadas. PVM=((NVI-NVF)/NVI)*100% Donde: PVM=Porcentaje de Vulnerabilidades Mitigadas. NVI= Número de Vulnerabilidades Iniciales. NVF=Número de Vulnerabilidades Finales.

Fuente: elaboración propia

Identificar Servicios.- Se identifican todos los servicios *web* que la institución ofrece a sus clientes; de los que, en base a su criticidad, se obtiene los siguientes:

- *Academics*.- Gestiona el sistema académico, éste servicio es un desarrollo de la Institución, de mantenimiento fácil.
- *Moodle*.- Plataforma *web* que se encuentra alojada en la nube, bajo la modalidad de IaaS en *Amazon web Services,* ésta plataforma ayuda a que los docentes, creen entornos virtuales de aprendizaje, esta plataforma de *software* libre, es desarrollada por terceros, no posee soporte personalizado, actualmente se encuentra instalada la versión 3.2.
- Mesa de Ayuda.- Sistema que viabiliza la solicitud de requerimientos informáticos, es un sistema de *software* libre, desarrollado por terceros, no posee soporte específico, por lo que se hace difícil el aplicar remediaciones, la versión del producto es la 7.5.
- Tablero de Control.- Aplicación que permite la gestión de los planes operativos anuales institucionales, es un sistema desarrollado como parte de un plan de tesis, por lo que no se posee soporte en el caso de requerir remediaciones, existe una única versión y no ha recibido mantenimiento desde su desarrollo.
- Impresión *web*.- Plataforma que permite la impresión *web* dentro de las inmediaciones universitarias, aplicativo desarrollado por terceros, se posee licenciamiento del producto para la versión 13, pero al momento se encuentra en la versión 16.
- Repositorio Digital.- Repositorio para la gestión de contenido bibliográfico institucional, es *software* libre, desarrollado por terceros, no posee un licenciamiento para soporte, lo que se hace difícil el poder realizar remediaciones, actualmente se encuentra instalada la versión 5.5.
- Catalogo en Línea.- Aplicación *web* que permite el acceso a los recursos de la biblioteca institucional, el que cuenta con licenciamiento de soporte y en caso de requerir remediaciones no se tendría inconvenientes.
- Reserva Laboratorios.- Plataforma *web* que permite la administración de reservas de los laboratorios del Departamento de Informática, es una plataforma de *software* libre, no posee soporte, lo que se hace difícil el poder aplicar remediaciones.

Identificar Activos.- Identificar todos los activos que intervienen en la operatividad de los servicios *web* y registrarlos según su clasificación en las fichas que se detallan a continuación.

[D] Datos o Información

Los datos son valiosos para personas ajenas, pues la pérdida de información afecta directamente a las operaciones que se ejecutan en la organización, en el cuadro se determina el activo en base al tipo de información.

Cuadro 5.- Ficha levantamiento de activos - datos

[D] Datos			
Código:	Código del activo	**Nombre:**	Nombre del activo
Descripción:	Descripción del activo		
Responsable:	Responsable del activo		
Tipo			
Nomenclatura	**Descripción**		
[files]	Ficheros		
[backup]	Copias de respaldo		
[conf]	Datos de configuración		
[int]	Datos de gestión interna		
[password]	Contraseñas		
[auth]	Datos de validación de credenciales		
[acl]	Datos de control de acceso		
[log]	Registro de actividad		
[source]	Código fuente		
[exe]	Código ejecutable		
[test]	Datos de prueba		

Fuente: adaptado de Consejo Superior de Administración Electrónica de España (2012)

[S] Servicios

Los servicios cubren las necesidades de los usuarios, en el siguiente cuadro se indica la ficha para levantar la información del activo.

Cuadro 6.- Ficha levantamiento de activos - servicios

[S] Servicios			
Código:	Código del activo	**Nombre:**	Nombre del activo
Descripción:	Descripción del activo		
Responsable:	Responsable del activo		
Tipo			
Nomenclatura	**Descripción**		
[anon]	Anónimo (sin requerir identificación del usuario)		
[pub]	Público en general (sin relación contractual)		
[ext]	Usuarios externos (bajo una relación contractual)		
[int]	Usuarios internos (a usuarios de la propia organización)		
[www]	*World wide web*		
[telnet]	Acceso remoto a cuenta local		
[email]	Correo electrónico		
[file]	Almacenamiento de ficheros		
[ftp]	Transferencia de ficheros		
[edi]	Intercambio electrónico de datos		
[dir]	Servicio de directorio		
[idm]	Gestión de identidades		
[ipm]	Gestión de privilegios		
[pki]	PKI - infraestructura de clave pública		

Fuente: adaptado de Consejo Superior de Administración Electrónica de España (2012)

[SW] Software

El *software* hace referencia a todas aquellas aplicaciones creadas para automatizar los procesos, en el siguiente cuadro se muestra la ficha para levantar la información del activo.

Cuadro 7.- Ficha levantamiento de activos - *software*

[SW] Aplicaciones (*software*)			
Código:	Código del activo	**Nombre:**	Nombre del activo
Descripción:	Descripción del activo		
Responsable:	Responsable del activo		
Tipo			
Nomenclatura	**Descripción**		
[prp]	Desarrollo propio (*in house*)		
[sub]	Desarrollo a medida (subcontratado)		
[std]	Estándar (*off the shelf*)		
[browser]	Navegador *web*		
[www]	Servidor de presentación		
[app]	Servidor de aplicaciones		
[email_client]	Cliente de correo electrónico		
[email_server]	Servidor de correo electrónico		
[file]	Servidor de ficheros		
[dbms]	Sistema de gestión de bases de datos		
[tm]	Monitor transaccional		
[office]	Ofimática		
[av]	Anti virus		
[os]	Sistema operativo		
[hypervisor]	Gestor de máquinas virtuales		
[ts]	Servidor de terminales		
[backup]	Sistema de *backup*		

Fuente: adaptado de Consejo Superior de Administración Electrónica de España (2012)

[HW] Equipos informáticos (hardware)

Los equipos informáticos son los medios físicos que alojan los servicios que presta una organización a sus usuarios, en el siguiente cuadro se detallan la ficha para levantar la información de éste activo.

Cuadro 8.- Ficha levantamiento de activos - *hardware*

[HW] Equipos informáticos (*hardware*)			
Código:	Código del activo	**Nombre:**	Nombre del activo
Descripción:	Descripción del activo		
Responsable:	Responsable del activo		
Ubicación:	Ubicación del activo		
Número:	Número de activos existentes del mismo tipo		
Tipo			
Nomenclatura	**Descripción**		
[host]	Grandes equipos		
[mid]	Equipos medios		
[pc]	Informática personal		
[mobile]	Informática móvil		
[pda]	Agendas electrónicas		
[vhost]	Equipo virtual		
[backup]	Equipamiento de respaldo		
[peripheral]	Periféricos		
[print]	Medios de impresión		
[scan]	Escáneres		
[crypto]	Dispositivos criptográficos		
[bp]	Dispositivo de frontera		
[network]	Soporte de la red		
[modem]	*Módems*		
[hub]	Concentradores		
[switch]	Conmutadores		
[router]	Encaminadores		
[bridge]	Pasarelas		
[firewall]	Cortafuegos		
[wap]	Punto de acceso inalámbrico		
[pabx]	Centralita telefónica		
[ipphone]	Teléfono IP		

Fuente: adaptado de Consejo Superior de Administración Electrónica de España (2012)

[COM] Redes de comunicaciones

Permiten que la información fluya de un lugar a otro, en el siguiente cuadro se indica la ficha para levantar la información de éste activo.

Cuadro 9.- Ficha levantamiento de activos - comunicación

[COM] Redes de comunicaciones			
Código:	Código del activo	**Nombre:**	Nombre del activo
Descripción:	Descripción del activo		
Responsable:	Responsable del activo		
Ubicación	Ubicación del activo		
Número	Número de activos existentes del mismo tipo		
Tipo			
Nomenclatura	**Descripción**		
[pstn]	Red telefónica		
[isdn]	Rdsi (red digital)		
[x25]	X25 (red de datos)		
[adsl]	ADSL		
[pp]	Punto a punto		
[radio]	Comunicaciones radio		
[wifi]	Red inalámbrica		
[mobile]	Telefonía móvil		
[sat]	Por satélite		
[lan]	Red local		
[man]	Red metropolitana		
[Internet]	Internet		

Fuente: adaptado de Consejo Superior de Administración Electrónica de España (2012)

[AUX] Equipamiento auxiliar

Son equipos que no se relacionan con datos, pero sirven de soporte para los sistemas de información, en el siguiente cuadro se muestra la ficha para levantar la información del activo.

Cuadro 10.- Ficha levantamiento de activos - equipamiento auxiliar

[AUX] Equipamiento auxiliar			
Código:	Código del activo	**Nombre:**	Nombre del activo
Descripción:	Descripción del activo		
Responsable:	Responsable del activo		
Ubicación	Ubicación del activo		
Número	Número de activos existentes del mismo tipo		
TIPO:			
Nomenclatura	**Descripción**		
[power]	Fuentes de alimentación		
[ups]	Sistemas de alimentación ininterrumpida		
[gen]	Generadores eléctricos		
[ac]	Equipos de climatización		
[cabling]	Cableado		
[wire]	Cable eléctrico		
[fiber]	Fibra óptica		
[robot]	Robots		
[tape]	Cintas		
[disk]	Discos		
[supply]	Suministros esenciales		
[destroy]	Equipos de destrucción de soportes de información		
[furniture]	Mobiliario: armarios, entre otros.		
[safe]	Cajas fuertes		

Fuente: adaptado de Consejo Superior de Administración Electrónica de España (2012)

[L] Instalaciones

Son los espacios físicos que albergan los equipos de comunicación y de cómputo, la ficha para levantar la información de éste activo se indica en el siguiente cuadro.

Cuadro 11.- Ficha levantamiento de activos - instalaciones

[L] Instalaciones			
Código:	Código del activo	**Nombre:**	Nombre del activo
Descripción:	Descripción del activo		
Responsable:	Responsable del activo		
Ubicación	Ubicación del activo		
Número	Número de activos existentes del mismo tipo		
TIPO:			
Nomenclatura	**Descripción**		
[site]	Recinto		
[building]	Edificio		
[local]	Cuarto		
[car]	Vehículo terrestre: coche, camión, etc.		
[plane]	Vehículo aéreo: avión, etc.		
[shelter]	Contenedores		
[channel]	Canalización		
[backup]	Instalaciones de respaldo		

Fuente: adaptado de Consejo Superior de Administración Electrónica de España (2012)

[P] Personal

Se refiere al personal encargado de la administración de los servicios brindados, la ficha para levantar la información de éste activo se indica en el siguiente cuadro.

Cuadro 12.- Ficha levantamiento de activos - personal

[P] Personal			
Código:	Código del activo	**Nombre:**	Nombre del activo
Descripción:	Descripción del activo		
Ubicación	Ubicación del activo		
Número	Número de activos existentes del mismo tipo		
Tipo			
Nomenclatura	**Descripción**		
[ue]	Usuarios externos		
[ui]	Usuarios internos		
[adm]	Administradores de sistemas		
[com]	Administradores de comunicaciones		
[dba]	Administradores de BBDD		
[sec]	Administradores de seguridad		
[des]	Desarrolladores / programadores		
[sub]	Subcontratas		
[prov]	Proveedores		

Fuente: adaptado de Consejo Superior de Administración Electrónica de España (2012)

Para determinar los activos que abarcan los servicios identificados, se mantiene reuniones con el responsable del área de Infraestructura Informática, con el que, se revisa y clasifica todos los activos a ser analizados, de lo que se obtiene los indicados en el cuadro siguiente.

Cuadro 13.- Identificación de activos informáticos.

Capa	Activo	Responsable
[s] Servicios internos		
	[srv_academics] *Academics*	Desarrollador
	[srv_moodle] *Moodle*	Administrador de plataformas
	[srv_spiceworks] Mesa de ayuda	Administrador de red
	[srv_tablero de control] Tablero de Control	Desarrollador
	[srv_papercut] Impresión *web*	Administrador de red
	[srv_repositorio] Repositorio digital	Administrador de red
	[srv_catalogo en Línea] Catalogo en línea	Administrador de red
	[srv_laboratorios] Reserva Laboratorios	Administrador de plataformas
[e] Equipamiento		
[hw] Equipos		
	[hw_servidor_dl380g6] Servidor hp dl380g6	Administrador de red
	[hw_maq_virtuales] Máquinas virtuales	Administrador de red
	[hw_maq_virtuales] Vpc_aws	Administrador de red
	[hw_servidor hp smf5600] Servidor hp smf5600	Administrador de red
	[hw_servidor *sunfire*] Servidor *sunfire*	Administrador de red
	[hw_switch] *Switch*	Administrador de red
	[hw_router] *Router*	Administrador de red
	[hw_almacenamiento] Almacenamiento emc	Administrador de red
[com] Comunicaciones		
	[com_internet] Internet	Administrador de red
	[com_lan] Red local	Administrador de red
[aux] Elementos auxiliares		
	[aux_aire] Aire acondicionado	Administrador de red
	[aux_generador] Generador eléctrico	Administrador de red
	[aux_ups] Sistemas de respaldo de energía	Administrador de red
[l] Instalaciones		
	[l_datacenter] Cuarto de datos	Administrador de red
[p] Personal		
	[p_admin_red] Administrador de red	
	[p_admin_plataformas] Administrador de plataformas	
	[p_desarrollador] Desarrollador	
	[p_prov] Proveedor	

Fuente: elaboración propia

La valoración de activos, indica cuán importante es para la organización el activo y en qué grado se degrada si sufriera un daño, todas las valoraciones se realizan en base a criterios comunes para

obtener resultados acordes a la realidad, en la siguiente tabla se muestra las escalas a utilizar para valorar el activo en su dimensión correspondiente:

Tabla 1.- Escala de valoración de activos

Valor	Grado	Criterio
10	Extremo	Daño extremadamente grave
9	Muy alto	Daño muy grave
6 – 8	Alto	Daño grave
3 – 5	Medio	Daño importante
1 – 2	Bajo	Daño menor
0	Despreciable	Irrelevante a efectos prácticos

Fuente: tomado de Consejo Superior de Administración Electrónica de España (2012)

Las dimensiones en las que son valorados los activos, son:

- La confidencialidad, parte de la información que no debe ser revelada al personal no autorizado de la organización.
- La integridad, puede ser vulnerada si el activo o información fuese alterado por alguien no autorizado.
- Trazabilidad de los datos, permite conocer de manera proactiva el manejo de la información por parte de diversas personas. O sea, identifica a las personas que modifiquen determinada información o datos que no les compete.
- Autenticidad de los datos, se reconoce cuando la información es confiable y produce un impacto positivo en la toma de decisiones en la organización.
- La disponibilidad, se reconoce cuando un servicio está activo, al generar un impacto positivo en la organización.

La valoración de los activos se realiza con el personal responsable del activo, a fin de establecer correctamente su valoración en cada dimensión, de lo que se obtiene lo resumido en la tabla siguiente.

Tabla 2.- Valoración activos PUCE Ambato

Capa	Activo	[D]	[I]	[C]	[A]	[T]
[is] Servicios internos						
	[srv_academics] *Academics*	[9]			[8]	[8]
	[srv_juridicos] *Moodle*	[9]			[8]	[8]
	[srv_tablero de control] Tablero de control	[8]			[8]	[8]
	[srv_papercut] Impresión *web*	[5]			[5]	[8]
	[srv_catalogo en línea] Catalogo en línea	[9]			[6]	[8]
	[srv_repositorio] Repositorio digital	[8]			[8]	[8]
	[srv_spiceworks] Mesa de ayuda	[8]			[8]	[8]
	[srv_laboratorios] Reserva laboratorios	[5]			[6]	[8]
[e] Equipamiento						
	[sw] Aplicaciones					
	[hw] Equipos					
	[hw_servidor_dl380g6] Servidor hp dl380g6	[9]				[8]
	[hw_maq_virtuales] Máquinas virtuales	[8]				[8]
	[hw_maq_virtuales] Vpc_aws	[9]				[8]
	[hw_servidor hp smf5600] Servidor hp smf5600	[7]				[7]
	[hw_servidor *sunfire*] Servidor *sunfire*	[5]				[7]
	[hw_switch] *Switch*	[9]				[9]
	[hw_router] *Router*	[9]				[9]
	[hw_almacenamiento] Almacenamiento emc	[9]	[8]			[9]
	[com] Comunicaciones					
	[com_internet] Internet	[9]				
	[com_lan] Red local	[9]		[9]		[7]
	[aux] Elementos auxiliares					
	[aux_aire] Aire acondicionado	[8]				
	[aux_generador] Generador eléctrico	[8]				
	[aux_ups] Sistemas de respaldo de energía	[7]				
[l] Instalaciones						
	[l_datacenter] Cuarto de datos			[7]		
[p] Personal						
	[p_administrador_red] Administrador de red			[8]		
	[p_adm_plataformas] Administrador de plataformas			[8]		
	[p_desarrollador] Desarrollador			[8]		
	[p_prov] Proveedor			[8]		

Fuente: elaboración propia

De la valoración realizada, los servicios de *Moodle* y *Academics* son los más importantes, ya que manejan toda la información académica de los estudiantes, que estén o que hayan pertenecido a la institución, aspectos que se requieren en auditorías internas efectuadas por la PUCE Quito, en cuanto a equipamiento, se concluye que el equipo de almacenamiento, de comunicación, servidores

de virtualización locales y servidores en la nube son los que presentan mayor degradación, al igual que los de comunicación, ya que están disponibles los 365 días del año.

Hacer

Según el modelo de *Deming,* se identifican las amenazas, riegos y vulnerabilidades, como la prioridad en su tratamiento.

Determinar Amenazas.- Se debe determinar conjuntamente con el personal responsable del activo, las amenazas más comunes que los afectan en cada una de las dimensiones a valorar, agrupadas por su origen, como se muestra en el siguiente cuadro.

Cuadro 14.- Listado de amenazas comunes

Origen	Tipo	Descripción	[D]	[I]	[C]	[A]	[T]
Desastres naturales							
De origen industrial							
Errores y fallos no intencionados							
Ataques intencionados							

Fuente: elaboración propia

De acuerdo a experiencias recogidas, se establece un conjunto de amenazas más comunes, agrupadas por su origen y con su respectiva dimensión a valorar, como se muestra en el cuadro siguiente.

Cuadro 15.- Identificación de amenazas por su origen

Origen	Tipo	Descripción	[D]	[I]	[C]	[A]	[T]
[N] Desastres naturales							
Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.	[N.1] Fuego	Posibilidad de que el fuego acabe con recursos del sistema.	X				
	[N.2] Daños por agua	Inundaciones: posibilidad de que el agua acabe con recursos del sistema.	X				
	[N.*] Desastres naturales	Posibilidad de rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras.	X				
[I] De origen industrial							
Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.	[I.1] Fuego	Incendio: posibilidad de que el fuego acabe con los recursos del sistema.	X				
	[I.2] Daños por agua	Escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.	X				
	[I.*] Desastres industriales	Explosiones, derrumbes, contaminación química, sobrecarga eléctrica, fluctuaciones eléctricas.	X				
	[I.3] Contaminación mecánica	Vibraciones, polvo, suciedad.	X				
	[I.4] Contaminación electromagnética	Interferencias de radio, campos magnéticos, luz ultravioleta.	X				
	[I.5] Avería de origen físico o lógico	Fallos en los equipos y/o fallos en los programas.	X				

	[I.6] Corte del suministro eléctrico	Cese de la alimentación de potencia.	X				
	[I.7] Condiciones inadecuadas de temperatura o humedad	Excesivo calor, excesivo frío, exceso de humedad.	X				
	[I.8] Fallo de servicios de comunicaciones	Cese de la capacidad de transmitir datos de un sitio a otro.	X				
	[I.9] Interrupción de otros servicios y suministros esenciales	Otros servicios o recursos de los que depende la operación de los equipos; por ejemplo, papel para las impresoras, tóner, refrigerante.	X				
	[I.10] Degradación de los soportes de almacenamiento de la información	Degradación como consecuencia del paso del tiempo.	X				
	[I.11] Emanaciones electromagnéticas	Hecho de poner vía radio datos internos a disposición de terceros.			X		
[E] Errores y fallos no intencionados							
Fallos no intencionales causados por las personas.	[E.1] Errores de los usuarios	Equivocaciones de las personas cuando usan los servicios, datos.	X	X	X		
	[E.2] Errores del administrador	Equivocaciones de personas con responsabilidades de instalación y operación.	X	X	X		
	[E.3] Errores de monitorización (log)	Inadecuado registro de actividades.		X		X	
	[E.4] Errores de configuración	Introducción de datos de configuración erróneos.		X			
	[E.7] Deficiencias en la organización	Cuando no está claro quién tiene que hacer exactamente qué y cuándo.	X				
	[E.8] Difusión de *software* dañino	Propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas.	X	X	X		
	[E.9] Errores de re encaminamiento	Envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información a donde o por donde no es debido.			X		
	[E.10] Errores de secuencia	Alteración accidental del orden de los mensajes transmitidos.		X			
	[E.14] Escapes de información	La información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella.			X		
	[E.15] Alteración accidental de la información	Alteración accidental de la información.		X			
	[E.18] Destrucción de información	Pérdida accidental de información.	X				
	[E.19] Fugas de información	Revelación por indiscreción.			X		
	[E.20] Vulnerabilidades de los programas (*software*)	Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario.	X	X	X		
	[E.21] Errores de mantenimiento / actualización de programas (*software*)	Defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.	X	X			

	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.	X				
	[E.24] Caída del sistema por agotamiento de recursos	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.	X				
	[E.25] Pérdida de equipos	La pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios.	X		X		
	[E.28] Indisponibilidad del personal	Ausencia accidental del puesto de trabajo.	X				
[A] Ataques intencionados							
Fallos deliberados causados por las personas	[A.3] Manipulación de los registros de actividad (log)	Manejo indebido de registros de actividad.		X		X	
	[A.4] Manipulación de la configuración	Manejo de los archivos de configuración del activo.		X	X	X	
	[A.5] Suplantación de la identidad del usuario	Cuando un atacante consigue hacerse pasar por un usuario autorizado.		X	X	X	
	[A.6] Abuso de privilegios de acceso	Cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia.	X	X	X		
	[A.7] Uso no previsto	Utilización de los recursos del sistema para fines no previstos.	X	X	X		
	[A.8] Difusión de *software* dañino	Propagación intencionada de virus, espías, gusanos, troyanos, bombas lógicas.	X	X	X		
	[A.9] re encaminamiento de mensajes	Envío de información a un destino incorrecto a través de un sistema o una red.			X		
	[A.10] Alteración de secuencia	Alteración del orden de los mensajes transmitidos.		X			
	[A.11] Acceso no autorizado	El atacante consigue acceder a los recursos del sistema sin tener autorización.		X	X		
	[A.12] Análisis de tráfico	El atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios.			X		
	[A.13] Repudio	Negación a posteriori de actuaciones o compromisos adquiridos en el pasado.		X			X
	[A.14] Interceptación de información (escucha)	El atacante llega a tener acceso a información que no le corresponde.			X		
	[A.15] Modificación deliberada de la información	Alteración intencional de la información.		X			
	[A.18] Destrucción de información	Eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.	X				
	[A.19] Divulgación de información	Revelación de información.			X		
	[A.22] Manipulación de programas	Alteración intencionada del funcionamiento de los programas.	X	X	X		

	[A.23] Manipulación de los equipos	Alteración intencionada del funcionamiento de los equipos.	X		X		
	[A.24] Denegación de servicio	La carencia de recursos suficientes.	X				
	[A.25] Robo	La sustracción de equipamiento.	X		X		
	[A.26] Ataque destructivo	Vandalismo, terrorismo, acción militar.	X				
	[A.27] Ocupación enemiga	Cuando los locales han sido invadidos.	X		X		
	[A.28] Indisponibilidad del personal	Ausencia deliberada del puesto de trabajo.	X				
	[A.29] Extorsión	Presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido.	X	X	X		
	[A.30] Ingeniería social	Abuso de la buena fe de las personas.	X	X	X		

Fuente: tomado de Consejo Superior de Administración Electrónica de España (2012)

Del listado de amenazas propuestas, asignar las que afecten al activo, en base al análisis realizado, se debe tener la matriz propuesta en el cuadro siguiente.

Cuadro 16.- Formulario para identificar amenazas

Activo	**Amenaza**
Activo 1	Amenaza 1
	Amenaza 2
	Amenaza 3

Fuente: elaboración propia

Para determinar las amenazas que podrían afectar a los activos, se definen las siguientes:

Cuadro 17.- Listado de amenazas por activo

Activo	**Amenaza**
[hw_servidor_dl380g6] Servidor hp dl380g6	[N.1] Fuego
	[N.2] Daños por agua
	[N.*] Desastres naturales
	[I.5] Avería de origen físico o lógico
	[I.6] Corte del suministro eléctrico
	[I.7] Condiciones inadecuadas de temperatura o humedad
	[E.4] Errores de configuración
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)
	[E.24] Caída del sistema por agotamiento de recursos
	[A.11] Acceso no autorizado
	[A.23] Manipulación del *hardware*
	[A.25] Robo de equipos
[hw_maq_virtuales] Máquinas virtuales	[I.5] Avería de origen físico o lógico
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)
	[E.24] Caída del sistema por agotamiento de recursos
	[A.11] Acceso no autorizado
	[A.23] Manipulación del *hardware*
[hw_maq_virtuales] Vpc_aws	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)
	[A.11] Acceso no autorizado

[hw_servidor hp smf5600] Servidor hp smf5600	[N.1] Fuego
	[N.2] Daños por agua
	[N.*] Desastres naturales
	[I.5] Avería de origen físico o lógico
	[I.6] Corte del suministro eléctrico
	[I.7] Condiciones inadecuadas de temperatura o humedad
	[E.4] Errores de configuración
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)
	[E.24] Caída del sistema por agotamiento de recursos
	[A.11] Acceso no autorizado
	[A.23] Manipulación del *hardware*
	[A.25] Robo de equipos
[hw_servidor sun fire] Servidor *sunfire*	[N.1] Fuego
	[N.2] Daños por agua
	[N.*] Desastres naturales
	[I.5] Avería de origen físico o lógico
	[I.6] Corte del suministro eléctrico
	[I.7] Condiciones inadecuadas de temperatura o humedad
	[E.4] Errores de configuración
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)
	[E.24] Caída del sistema por agotamiento de recursos
	[A.11] Acceso no autorizado
	[A.23] Manipulación del *hardware*
	[A.25] Robo de equipos
[hw_switch] *Switch*	[N.1] Fuego
	[N.2] Daños por agua
	[N.*] Desastres naturales
	[I.5] Avería de origen físico o lógico
	[I.6] Corte del suministro eléctrico
	[I.7] Condiciones inadecuadas de temperatura o humedad
	[E.4] Errores de configuración
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)
	[E.24] Caída del sistema por agotamiento de recursos
	[A.11] Acceso no autorizado
	[A.23] Manipulación del *hardware*
	[A.25] Robo de equipos
[hw_router] *Router*	[N.1] Fuego
	[N.2] Daños por agua
	[N.*] Desastres naturales
	[I.5] Avería de origen físico o lógico
	[I.6] Corte del suministro eléctrico
	[I.7] Condiciones inadecuadas de temperatura o humedad
	[E.4] Errores de configuración
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)
	[E.24] Caída del sistema por agotamiento de recursos
	[A.11] Acceso no autorizado
	[A.23] Manipulación del *hardware*
	[A.25] Robo de equipos
[hw_almacenamiento] Almacenamiento emc	[N.1] Fuego
	[N.2] Daños por agua
	[N.*] Desastres naturales
	[I.5] Avería de origen físico o lógico

	[I.6] Corte del suministro eléctrico
	[I.7] Condiciones inadecuadas de temperatura o humedad
	[I.10] Degradación de los soportes de almacenamiento de la información
	[E.1] Errores de los usuarios
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)
	[E.24] Caída del sistema por agotamiento de recursos
	[A.11] Acceso no autorizado
	[A.23] Manipulación del *hardware*
	[A.25] Robo de equipos
[com_internet] Internet	[I.8] Fallo de servicios de comunicaciones
	[E.2] Errores del administrador del sistema / de la seguridad
	[E.24] Caída del sistema por agotamiento de recursos
	[A.11] Acceso no autorizado
	[A.24] Denegación de servicio
[com_lan] Red local	[I.8] Fallo de servicios de comunicaciones
	[E.2] Errores del administrador del sistema / de la seguridad
	[E.9] Errores de re encaminamiento
	[E.19] Fugas de información
	[E.24] Caída del sistema por agotamiento de recursos
	[A.11] Acceso no autorizado
	[A.14] Interceptación de información (escucha)
	[A.24] Denegación de servicio
[aux_aire] Aire acondicionado	[N.1] Fuego
	[N.2] Daños por agua
	[N.*] Desastres naturales
	[I.6] Corte del suministro eléctrico
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)
	[A.23] Manipulación del *hardware*
[aux_generador] Generador eléctrico	[N.1] Fuego
	[N.2] Daños por agua
	[N.*] Desastres naturales
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)
	[A.23] Manipulación del *hardware*
	[A.25] Robo de equipos
[aux_ups] Sistemas de respaldo de energía	[N.1] Fuego
	[N.2] Daños por agua
	[N.*] Desastres naturales
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)
	[A.23] Manipulación del *hardware*
	[A.25] Robo de equipos
[l_datacenter] Cuarto de datos	[N.1] Fuego
	[N.2] Daños por agua
	[N.*] Desastres naturales
	[A.6] Abuso de privilegios de acceso
[p_administrador_red] Administrador de red	[E.19] Fugas de información
	[E.28] Indisponibilidad del personal
	[A.19] Revelación de información
	[A.30] Ingeniería social (picaresca)
[p_adm_plataformas] Administrador de plataformas	[E.19] Fugas de información
	[E.28] Indisponibilidad del personal
	[A.19] Revelación de información
	[A.30] Ingeniería social (picaresca)

[p_desarrollador] Desarrollador	[E.19] Fugas de información
	[E.28] Indisponibilidad del personal
	[A.19] Revelación de información
	[A.30] Ingeniería social (picaresca)
[p_prov] Proveedor	[E.4] Errores de configuración
	[E.18] Destrucción de la información
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)
	[E.28] Indisponibilidad del personal
	[E.29] Extorción

Fuente: basado en el Consejo Superior de Administración Electrónica de España (2012)

Se valoran las amenazas en base a la frecuencia de ocurrencia y la degradación del activo, al considerar que:

Degradación.- Es la pérdida de valor del activo causado por un incidente.

Tabla 3. Escala de degradación

Nivel	Degradación		Peso
100%	Muy Alto	MA	5
75%	Alto	A	4
50%	Medio	M	3
25%	Bajo	B	2
1%	Despreciable	MB	1

Fuente: tomado de Consejo Superior de Administración Electrónica de España (2012)

Frecuencia.- Indica cada que tiempo se materializa la amenaza, periodo anual.

Tabla 4.- Escala de frecuencia

Periodicidad	Frecuencia		Peso
360	A diario	MA	5
12	Una vez al mes	A	4
2	Dos veces al año	M	3
1	Una vez al año	B	2
1/12	Cada varios años	MB	1

Fuente: tomado de Consejo Superior de Administración Electrónica de España (2012)

La valoración a las amenazas, se indica en el cuadro siguiente.

Cuadro 18.- Identificación y valoración de amenazas

Activo	Amenaza	Frecuencia	Degradación				
			[D]	[I]	[C]	[A]	[T]
[hw_servidor_dl380g6] Servidor hp dl380g6	[N.1] Fuego	MB	A				
	[N.2] Daños por agua	MB	A				
	[N.*] Desastres naturales	MB	MA				
	[I.5] Avería de origen físico o lógico	B	A				
	[I.6] Corte del suministro eléctrico	M	B				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M	A				
	[E.4] Errores de configuración	M		M			
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	B	B				
	[E.24] Caída del sistema por agotamiento de recursos	B	A				
	[A.11] Acceso no autorizado	MB		B	B		
	[A.23] Manipulación del *hardware*	MB	A		B		
	[A.25] Robo de equipos	MB	MA		A		
[hw_maq_virtuales] Máquinas virtuales	[I.5] Avería de origen físico o lógico	B	A				
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	B	B				
	[E.24] Caída del sistema por agotamiento de recursos	B	A				
	[A.11] Acceso no autorizado	MB		B	B		
	[A.23] Manipulación del *hardware*	MB	A		B		
[hw_maq_virtuales] Vpc_aws	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	MB	A				
	[A.11] Acceso no autorizado	MB		A	A		
[hw_servidor hp smf5600] Servidor hp smf5600	[N.1] Fuego	MB	A				
	[N.2] Daños por agua	MB	A				
	[N.*] Desastres naturales	MB	MA				
	[I.5] Avería de origen físico o lógico	B	A				
	[I.6] Corte del suministro eléctrico	M	B				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M	A				
	[E.4] Errores de configuración	B		M			
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	B	B				
	[E.24] Caída del sistema por agotamiento de recursos	B	A				
	[A.11] Acceso no autorizado	MB		B	B		
	[A.23] Manipulación del *hardware*	MB	B		B		
	[A.25] Robo de equipos	MB	MA		A		

[hw_servidor sun fire] Servidor *sunfire*	[N.1] Fuego	MB	A				
	[N.2] Daños por agua	MB	A				
	[N.*] Desastres naturales	MB	MA				
	[I.5] Avería de origen físico o lógico	B	A				
	[I.6] Corte del suministro eléctrico	M	B				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M	A				
	[E.4] Errores de configuración	B		M			
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	B	B				
	[E.24] Caída del sistema por agotamiento de recursos	B	A				
	[A.11] Acceso no autorizado	MB		B	B		
	[A.23] Manipulación del *hardware*	MB	B		B		
	[A.25] Robo de equipos	MB	MA		A		
[hw_switch] *Switch*	[N.1] Fuego	MB	A				
	[N.2] Daños por agua	MB	A				
	[N.*] Desastres naturales	MB	MA				
	[I.5] Avería de origen físico o lógico	B	A				
	[I.6] Corte del suministro eléctrico	M	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M	A				
	[E.4] Errores de configuración	B		M			
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	B	A				
	[E.24] Caída del sistema por agotamiento de recursos	B	MA				
	[A.11] Acceso no autorizado	MB		A	A		
	[A.23] Manipulación del *hardware*	MB	A		A		
	[A.25] Robo de equipos	MB	MA		A		
[hw_router] *Router*	[N.1] Fuego	MB	A				
	[N.2] Daños por agua	MB	A				
	[N.*] Desastres naturales	MB	MA				
	[I.5] Avería de origen físico o lógico	B	A				
	[I.6] Corte del suministro eléctrico	M	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M	A				
	[E.4] Errores de configuración	B		A			
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	B	A				
	[E.24] Caída del sistema por agotamiento de recursos	B	MA				
	[A.11] Acceso no autorizado	MB		A	A		
	[A.23] Manipulación del *hardware*	MB	A		A		

	[A.25] Robo de equipos	MB	MA		A		
[hw_almacenamiento] Almacenamiento emc	[N.1] Fuego	MB	A				
	[N.2] Daños por agua	MB	A				
	[N.*] Desastres naturales	MB	MA				
	[I.5] Avería de origen físico o lógico	B	A				
	[I.6] Corte del suministro eléctrico	M	M				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M	M				
	[I.10] Degradación de los soportes de almacenamiento de la información	B	M				
	[E.1] Errores de los usuarios	B	A	MA	MA		
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	B	B				
	[E.24] Caída del sistema por agotamiento de recursos	MB	M	A			
	[A.11] Acceso no autorizado	MB		MA	MA		
	[A.23] Manipulación del *hardware*	MB	B		A		
	[A.25] Robo de equipos	MB	MA		A		
[com_internet] Internet	[I.8] Fallo de servicios de comunicaciones	B	A				
	[E.2] Errores del administrador del sistema / de la seguridad	B	A	A	A		
	[E.24] Caída del sistema por agotamiento de recursos	B	M				
	[A.11] Acceso no autorizado	MB			A		
	[A.24] Denegación de servicio	MB	MA				
[com_lan] Red local	[I.8] Fallo de servicios de comunicaciones	B	B				
	[E.2] Errores del administrador del sistema / de la seguridad	B	A	A	A		
	[E.9] Errores de re encaminamiento	B			M		
	[E.19] Fugas de información	MB			MA		
	[E.24] Caída del sistema por agotamiento de recursos	B	B				
	[A.11] Acceso no autorizado	MB			A		
	[A.14] Interceptación de información (escucha)	MB			A		
	[A.24] Denegación de servicio	MB	MA				
[aux_aire] Aire acondicionado	[N.1] Fuego	MB	A				
	[N.2] Daños por agua	MB	A				
	[N.*] Desastres naturales	MB	MA				
	[I.6] Corte del suministro eléctrico	M	A				
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	B	M				
	[A.23] Manipulación del *hardware*	B	B		M		
[aux_generador] Generador eléctrico	[N.1] Fuego	MB	A				
	[N.2] Daños por agua	MB	M				

	[N.*] Desastres naturales	MB	A				
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	B	M				
	[A.23] Manipulación del *hardware*	B	B		M		
	[A.25] Robo de equipos	MB	MA		A		
[aux_ups] sistemas de Respaldo de energía	[N.1] Fuego	MB	A				
	[N.2] Daños por agua	MB	A				
	[N.*] Desastres naturales	MB	A				
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	B	B				
	[A.23] Manipulación del *hardware*	B	B		B		
	[A.25] Robo de equipos	MB	MA		A		
[l_datacenter] Cuarto de datos	[N.1] Fuego	MB	A				
	[N.2] Daños por agua	MB	A				
	[N.*] Desastres naturales	MB	MA				
	[A.6] Abuso de privilegios de acceso	B	A	A	A		
[p_administrador_red] Administrador de red	[E.19] Fugas de información	MB			M		
	[E.28] Indisponibilidad del personal	B	MB				
	[A.19] Revelación de información	MB			A		
	[A.30] Ingeniería social (picaresca)	MB	MB	A	B		
[p_adm_plataformas] Administrador de plataformas	[E.19] Fugas de información	MB		B	M		
	[E.28] Indisponibilidad del personal	B	MB				
	[A.19] Revelación de información	MB			A		
	[A.30] Ingeniería social (picaresca)	MB	MB	A	B		
[p_desarrollador] Desarrollador	[E.19] Fugas de información	MB		B	M		
	[E.28] Indisponibilidad del personal	B	MB				
	[A.19] Revelación de información	MB			A		
	[A.30] Ingeniería social (picaresca)	MB	MB	A	B		
[p_prov] Proveedor	[E.4] Errores de configuración	MB		A			
	[E.18] Destrucción de la información	B	A				
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	B	B				
	[E.28] Indisponibilidad del personal	B	B				
	[E.29] Extorción	MB	B	M	M		

Fuente: elaboración propia

Definir salvaguardas que permita proponer los mecanismos de protección del activo ante la amenaza detectada, para lo que con el responsable de cada uno de los activos, se realza una constatación física y lógica, en el que se consideran aspectos como: los fallos anteriores que tuvieron, el mantenimiento recibido y el lugar físico en el cual se encuentra instalado, éste último basado en la ficha levantada de cada activo; con lo cual, se establecen salvaguardas para cada amenaza identificada, las que se detallan en el siguiente cuadro.

Cuadro 19.- Determinación de salvaguardas ante amenazas

Activo	Amenaza	Salvaguarda
[hw_servidor_dl380g6] Servidor hp dl380g6	[N.1] Fuego	Disponer de extintores adecuados. Implementar sensores de monitoreo de temperatura de HW. Contar con sensores de humo dentro del *DataCenter.*
	[N.2] Daños por agua	Dar mantenimiento a tuberías que pudiese generar fuga de agua.
	[N.*] Desastres naturales	Mantener réplicas del servidor en un sitio alterno.
	[I.5] Avería de origen físico o lógico	Disponer de sensores de monitoreo del estado del *hardware.*
	[I.6] Corte del suministro eléctrico	Mantener conectado el equipo a sistemas de alimentación ininterrumpida. Disponer de un generador eléctrico.
	[I.7] Condiciones inadecuadas de temperatura o humedad	Disponer de sensores de monitoreo de temperatura y humedad.
	[E.4] Errores de configuración	Definir procesos de configuración de equipos. Disponer de equipos alternos para realizar pruebas de concepto.
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	Contar con personal calificado para el mantenimiento. Realizar pruebas previas a la aplicación de actualizaciones en producción. Establecer procedimientos de mantenimiento o actualización.
	[E.24] Caída del sistema por agotamiento de recursos	Mantener un inventario de los recursos del equipo. Llevar un control del tiempo de vida de cada recurso. Disponer de elementos redundantes.
	[A.11] Acceso no autorizado	Aplicar políticas de acceso al equipo. No mantener las configuraciones por defecto.
	[A.23] Manipulación del *hardware*	Identificar al personal responsable del equipo. Aplicar políticas de control de acceso al *DataCenter.*
	[A.25] Robo de equipos	Disponer de cámaras de seguridad dentro del *DataCenter.* Aplicar políticas de control de acceso al *DataCenter.*
[hw_maq_virtuales] Máquinas virtuales	[I.5] Avería de origen físico o lógico	Disponer de sensores de monitoreo del estado del *hardware.*
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	Contar con personal calificado para el mantenimiento. Realizar pruebas previas a la aplicación de actualizaciones en producción.

		Establecer procedimientos de mantenimiento o actualización.
	[E.24] Caída del sistema por agotamiento de recursos	Mantener un inventario de los recursos del equipo. Llevar un control del tiempo de vida de cada recurso. Disponer de elementos redundantes.
	[A.11] Acceso no autorizado	Aplicar políticas de acceso al equipo. No mantener las configuraciones por defecto.
	[A.23] Manipulación del *hardware*	Identificar al personal responsable del equipo. Aplicar políticas de control de acceso al *DataCenter.*
[hw_maq_virtuales] Vpc_aws	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	Solicitar respaldos de los equipos previos a la actualización programada. Mantener respaldos periódicos de los equipos virtuales.
	[A.11] Acceso no autorizado	Aplicar políticas de acceso a personal autorizado. Aplicar políticas de seguridad al equipo.
[hw_servidor hp smf5600] Servidor hp smf5600	[N.1] Fuego	Contar con extintores adecuados. Implementar sensores de monitoreo de temperatura de HW. Contar con sensores de humo dentro del *DataCenter.*
	[N.2] Daños por agua	Dar mantenimiento a tuberías que pudieses generar fuga de agua.
	[N.*] Desastres naturales	Mantener réplicas del servidor en un sitio alterno.
	[I.5] Avería de origen físico o lógico	Disponer de sensores de monitoreo del estado del *hardware.*
	[I.6] Corte del suministro eléctrico	Mantener conectado el equipo a sistemas de alimentación ininterrumpida. Disponer de un generador eléctrico.
	[I.7] Condiciones inadecuadas de temperatura o humedad	Disponer de sensores de monitoreo de temperatura y humedad.
	[E.4] Errores de configuración	Definir procesos de configuración de equipos. Disponer de equipos alternos para realizar pruebas de concepto.
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	Contar con personal calificado para el mantenimiento. Realizar pruebas previas a la aplicación de actualizaciones en producción. Establecer procedimientos de mantenimiento o actualización.
	[E.24] Caída del sistema por agotamiento de recursos	Mantener un inventario de los recursos del equipo.

		Llevar un control del tiempo de vida de cada recurso.
		Disponer de elementos redundantes.
	[A.11] Acceso no autorizado	Aplicar políticas de control de acceso al equipo. No mantener las configuraciones por defecto.
	[A.23] Manipulación del *hardware*	Identificar al personal responsable del equipo. Aplicar políticas de control de acceso al *DataCenter.*
	[A.25] Robo de equipos	Disponer de cámaras de seguridad dentro del *DataCenter.* Aplicar políticas de control de acceso al *DataCenter.*
[hw_servidor sun fire] Servidor *sunfire*	[N.1] Fuego	Contar con extintores adecuados. Implementar sensores de monitoreo de temperatura de HW. Contar con sensores de humo dentro del *DataCenter.*
	[N.2] Daños por agua	Dar mantenimiento a tuberías que pudieses generar fuga de agua.
	[N.*] Desastres naturales	Mantener réplicas del servidor en un sitio alterno.
	[I.5] Avería de origen físico o lógico	Disponer de sensores de monitoreo del estado del *hardware.*
	[I.6] Corte del suministro eléctrico	Mantener conectado el equipo a sistemas de alimentación ininterrumpida. Disponer de un generador eléctrico.
	[I.7] Condiciones inadecuadas de temperatura o humedad	Disponer de sensores de monitoreo de temperatura y humedad.
	[E.4] Errores de configuración	Definir procesos de configuración de equipos. Disponer de equipos alternos para realizar pruebas de concepto.
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	Contar con personal calificado para el mantenimiento. Realizar pruebas previas a la aplicación de actualizaciones en producción. Establecer procedimientos de mantenimiento o actualización.
	[E.24] Caída del sistema por agotamiento de recursos	Mantener un inventario de los recursos del equipo. Llevar un control del tiempo de vida de cada recurso. Disponer de elementos redundantes.
	[A.11] Acceso no autorizado	Aplicar políticas de control de acceso al equipo. No mantener las configuraciones por defecto.
	[A.23] Manipulación del *hardware*	Identificar al personal responsable del equipo.

		Aplicar políticas de control de acceso al *DataCenter*.
	[A.25] Robo de equipos	Disponer de cámaras de seguridad dentro del *DataCenter.*
		Aplicar políticas de control de acceso al *DataCenter*.
[hw_switch] *Switch*	[N.1] Fuego	Contar con extintores adecuados. Implementar sensores de monitoreo de temperatura de HW. Contar con sensores de humo dentro del *DataCenter.*
	[N.2] Daños por agua	Dar mantenimiento a tuberías que pudieses generar fuga de agua.
	[N.*] Desastres naturales	Mantener réplicas del servidor en un sitio alterno.
	[I.5] Avería de origen físico o lógico	Disponer de sensores de monitoreo del estado del *hardware.*
	[I.6] Corte del suministro eléctrico	Mantener conectado el equipo a sistemas de alimentación ininterrumpida. Disponer de un generador eléctrico.
	[I.7] Condiciones inadecuadas de temperatura o humedad	Disponer de sensores de monitoreo de temperatura y humedad.
	[E.4] Errores de configuración	Definir procesos de configuración de equipos. Disponer de equipos alternos para realizar pruebas de concepto.
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	Contar con personal calificado para el mantenimiento. Realizar pruebas previas a la aplicación de actualizaciones en producción. Establecer procedimientos de mantenimiento o actualización.
	[E.24] Caída del sistema por agotamiento de recursos	Mantener un inventario de los recursos del equipo. Llevar un control del tiempo de vida de cada recurso. En lo posible disponer de elementos redundantes.
	[A.11] Acceso no autorizado	Aplicar políticas de control de acceso al equipo. No mantener las configuraciones por defecto.
	[A.23] Manipulación del *hardware*	Identificar al personal responsable del equipo. Mantener un control de acceso al *DataCenter.*
	[A.25] Robo de equipos	Disponer de cámaras de seguridad dentro del *DataCenter.* Mantener un control de acceso al *DataCenter.*
[hw_router] *Router*	[N.1] Fuego	Contar con extintores adecuados. Implementar sensores de monitoreo de temperatura de HW.

		Contar con sensores de humo dentro del *DataCenter.*
	[N.2] Daños por agua	Dar mantenimiento a tuberías que pudieses generar fuga de agua.
	[N.*] Desastres naturales	Mantener réplicas del servidor en un sitio alterno.
	[I.5] Avería de origen físico o lógico	Disponer de sensores de monitoreo del estado del *hardware.*
	[I.6] Corte del suministro eléctrico	Mantener conectado el equipo a sistemas de alimentación ininterrumpida. Disponer de un generador eléctrico.
	[I.7] Condiciones inadecuadas de temperatura o humedad	Disponer de sensores de monitoreo de temperatura y humedad.
	[E.4] Errores de configuración	Definir procesos de configuración de equipos. Disponer de equipos alternos para realizar pruebas de concepto.
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	Contar con personal calificado para el mantenimiento. Realizar pruebas previas a la aplicación de actualizaciones en producción. Establecer procedimientos de mantenimiento o actualización.
	[E.24] Caída del sistema por agotamiento de recursos	Mantener un inventario de los recursos del equipo. Llevar un control del tiempo de vida de cada recurso. Disponer de elementos redundantes.
	[A.11] Acceso no autorizado	Aplicar políticas de control de acceso al equipo. No mantener las configuraciones por defecto.
	[A.23] Manipulación del *hardware*	Identificar al personal responsable del equipo. Aplicar políticas de control de acceso al *DataCenter.*
	[A.25] Robo de equipos	Disponer de cámaras de seguridad dentro del *DataCenter.* Mantener un control de acceso al *DataCenter.*
[hw_almacenamiento] Almacenamiento emc	[N.1] Fuego	Contar con extintores adecuados. Implementar sensores de monitoreo de temperatura de HW. Contar con sensores de humo dentro del *DataCenter.*
	[N.2] Daños por agua	Dar mantenimiento a tuberías que pudieses generar fuga de agua.
	[N.*] Desastres naturales	Mantener réplicas del servidor en un sitio alterno.
	[I.5] Avería de origen físico o lógico	Disponer de sensores de monitoreo del estado del *hardware.*
	[I.6] Corte del suministro eléctrico	Mantener conectado el equipo a sistemas de alimentación ininterrumpida.

		Disponer de un generador eléctrico.
	[I.7] Condiciones inadecuadas de temperatura o humedad	Disponer de sensores de monitoreo de temperatura y humedad.
	[I.10] Degradación de los soportes de almacenamiento de la información	Mantener un inventario de los recursos del equipo.
		Llevar un control del tiempo de vida de cada recurso.
		Disponer de elementos redundantes.
	[E.1] Errores de los usuarios	Disponer de manuales técnicos de administración del equipo.
		Disponer de personal capacitado para la administración.
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	Contar con personal calificado para el mantenimiento.
		Realizar pruebas previas a la aplicación de actualizaciones en producción.
		Establecer procedimientos de mantenimiento o actualización.
	[E.24] Caída del sistema por agotamiento de recursos	Mantener un inventario de los recursos del equipo.
		Llevar un control del tiempo de vida de cada recurso.
		Disponer de elementos redundantes.
	[A.11] Acceso no autorizado	Establecer controles de acceso al equipo.
		No mantener las configuraciones por defecto.
	[A.23] Manipulación del *hardware*	Identificar al personal responsable del equipo.
		Aplicar políticas de control de acceso al *DataCenter.*
	[A.25] Robo de equipos	Disponer de cámaras de seguridad dentro del *DataCenter.*
		Mantener un control de acceso al *DataCenter.*
[com_internet] Internet	[I.8] Fallo de servicios de comunicaciones	Disponer de comunicaciones redundantes.
	[E.2] Errores del administrador del sistema / de la seguridad	Establecer procesos para la administración del sistema.
	[E.24] Caída del sistema por agotamiento de recursos	Mantener un inventario de los recursos del equipo.
		Llevar un control del tiempo de vida de cada recurso.
		Disponer de elementos redundantes.
	[A.11] Acceso no autorizado	Aplicar políticas de control de acceso al equipo.
		No mantener las configuraciones por defecto.
	[A.24] Denegación de servicio	Configurar correctamente el *firewall.*
		Configurar umbrales de conexiones permitidas para evitar *floods.*

		Implementar sistemas IDS/IPS.
[com_lan] Red local	[I.8] Fallo de servicios de comunicaciones	Disponer de comunicaciones redundantes.
	[E.2] Errores del administrador del sistema / de la seguridad	Establecer procesos para la administración del sistema.
	[E.9] Errores de [re-]encaminamiento	Configurar correctamente los *switches.* Disponer de personal experto para la administración de los equipos. Establecer procesos en cambios de re-encaminamientos.
	[E.19] Fugas de información	Implementar sistemas de Prevención de Fuga de Información (DLP).
	[E.24] Caída del sistema por agotamiento de recursos	Mantener un inventario de los recursos del equipo. Llevar un control del tiempo de vida de cada recurso. Disponer de elementos redundantes.
	[A.11] Acceso no autorizado	Aplicar políticas de control de acceso al equipo. No mantener las configuraciones por defecto.
	[A.14] Interceptación de información (escucha)	Aplicar políticas de seguridad a la red. Establecer cifrado de datos.
	[A.24] Denegación de servicio	Configurar correctamente el *firewall.* Configurar umbrales de conexiones permitidas para evitar *floods.* Implementar sistemas IDS/IPS.
[aux_aire] Aire acondicionado	[N.1] Fuego	Contar con extintores adecuados. Implementar sensores de monitoreo de temperatura de HW. Contar con sensores de humo dentro del *DataCenter.*
	[N.2] Daños por agua	Dar mantenimiento a tuberías que pudieses generar fuga de agua.
	[N.*] Desastres naturales	Mantener réplicas del servidor en un sitio alterno.
	[I.6] Corte del suministro eléctrico	Disponer de un generador eléctrico.
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	Contar con personal calificado para el mantenimiento. Realizar pruebas previas a la aplicación de actualizaciones en producción. Establecer procedimientos de mantenimiento o actualización.
	[A.23] Manipulación del *hardware*	Identificar al personal responsable del equipo. Mantener un control de acceso al *DataCenter.*

[aux_generador] Generador eléctrico	[N.1] Fuego	Contar con extintores adecuados. Implementar sensores de monitoreo de temperatura de HW. Contar con sensores de humo dentro del *DataCenter.*
	[N.2] Daños por agua	Dar mantenimiento a tuberías que pudieses generar fuga de agua.
	[N.*] Desastres naturales	Mantener réplicas del servidor en un sitio alterno.
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	Contar con personal calificado para el mantenimiento. Realizar pruebas previas a la aplicación de actualizaciones en producción. Establecer procedimientos de mantenimiento o actualización.
	[A.23] Manipulación del *hardware*	Identificar al personal responsable del equipo. Aplicar políticas de control de acceso al *DataCenter.*
	[A.25] Robo de equipos	Disponer de cámaras de seguridad dentro del *DataCenter.* Aplicar políticas de control de acceso al *DataCenter*.
[aux_ups] Sistemas de respaldo de energía	[N.1] Fuego	Contar con extintores adecuados. Implementar sensores de monitoreo de temperatura de HW. Contar con sensores de humo dentro del *DataCenter.*
	[N.2] Daños por agua	Dar mantenimiento a tuberías que pudieses generar fuga de agua.
	[N.*] Desastres naturales	Mantener réplicas del servidor en un sitio alterno.
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	Contar con personal calificado para el mantenimiento. Realizar pruebas previas a la aplicación de actualizaciones en producción. Establecer procedimientos de mantenimiento o actualización.
	[A.23] Manipulación del *hardware*	Identificar al personal responsable del equipo. Aplicar políticas de control de acceso al *DataCenter.*
	[A.25] Robo de equipos	Disponer de cámaras de seguridad dentro del *DataCenter.* Aplicar políticas de control de acceso al *DataCenter*.
[l_datacenter] Cuarto de datos	[N.1] Fuego	Contar con extintores de CO2. Implementar sensores de monitoreo de temperatura de HW.
		Contar con sensores de humo dentro del *DataCenter.*
	[N.2] Daños por agua	Dar mantenimiento a tuberías que pudieses generar fuga de agua.
	[N.*] Desastres naturales	Mantener réplicas del servidor en un sitio alterno.

	[A.6] Abuso de privilegios de acceso	Mantener la trazabilidad de acceso al cuarto de datos. Aplicar políticas de acceso al *DataCenter.*
[p_administrador_red] Administrador de red	[E.19] Fugas de información	Implementar sistemas de Prevención de Fuga de Información (DLP).
	[E.28] Indisponibilidad del personal	Capacitar a personal que pueda suplir la ausencia del responsable.
	[A.19] Revelación de información	Establecer políticas de confidencialidad de información.
	[A.30] Ingeniería social (picaresca)	Formación y concienciación del personal.
[p_adm_plataformas] Administrador de plataformas	[E.19] Fugas de información	Implementar sistemas de Prevención de Fuga de Información (DLP).
	[E.28] Indisponibilidad del personal	Capacitar a personal que pueda suplir la ausencia del principal.
	[A.19] Revelación de información	Establecer políticas de confidencialidad de información.
	[A.30] Ingeniería social (picaresca)	Formación y concienciación del personal.
[p_desarrollador] Desarrollador	[E.19] Fugas de información	Implementar sistemas de Prevención de Fuga de Información (DLP).
	[E.28] Indisponibilidad del personal	Capacitar a personal que pueda suplir la ausencia del principal.
	[A.19] Revelación de información	Establecer políticas de confidencialidad de información.
	[A.30] Ingeniería social (picaresca)	Formación y concienciación del personal.
[p_prov] Proveedor	[E.4] Errores de configuración	Definir procesos de configuración de equipos. Disponer de equipos alternos para realizar pruebas de concepto.
	[E.18] Destrucción de la información	Establecer acuerdos con el proveedor para la destrucción de información. Mantener respaldos de la información que se encuentre en el proveedor.
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	Contar con personal calificado para el mantenimiento. Realizar pruebas previas a la aplicación de actualizaciones en producción. Establecer procedimientos de mantenimiento o actualización.
	[E.28] Indisponibilidad del personal	Acordar con el proveedor el cumplimiento de SLA's.
	[E.29] Extorción	Mantener contratos legalmente aprobados entre las partes.

Fuente: elaboración propia

Se debe aclarar que, las salvaguardas propuestas no son ejecutadas, ya que el objetivo principal del estudio se enfoca en las vulnerabilidades de los servicios *web* de la PUCE Ambato, por lo que, queda a decisión de la institución el acogerlas, ejecutarlas y realizar el análisis de madurez de las mismas.

Determinar Impacto.- Determinar el alcance del daño que tendría la materialización de una amenaza sobre los activos de la institución, en cada una de las dimensiones.

En la tabla siguiente se presenta los rangos de medición para calificar la probabilidad de las amenazas.

Tabla 5.- Escala de probabilidad

Impacto	Nivel	Peso
MB	Puede ocurrir solo en circunstancias excepcionales	1
B	Es muy raro que ocurra	2
M	Puede ocurrir en cualquier momento	3
A	Probablemente ocurra en la mayoría de circunstancias	4
MA	Se espera que ocurra en la mayoría de circunstancias	5

Fuente: adoptado de Consejo Superior de Administración Electrónica de España (2012)

Estimar la valoración del impacto de la amenaza sobre el activo en la respectiva dimensión, ésta se realiza conjuntamente con el responsable del activo, en la tabla siguiente, se muestran las escalas de impacto utilizadas.

Tabla 6.- Escala de impacto

Impacto	Nivel	Peso
MB	No genera perjuicios a la institución	1
B	Pocos daños que se controlan inmediatamente	2
M	Pueden generar daños asociados a otros servicios	3
A	Generan daños importantes, asociados a otros servicios	4
MA	Perjuicios que generan daños catastróficos	5

Fuente: tomado de Consejo Superior de Administración Electrónica de España (2012)

En base al análisis que se realice, se debe llenar el formulario que se indica en el siguiente cuadro, y se debe respetar las valoraciones por amenaza y dimensión.

Cuadro 20.- Formulario para determinar el impacto

Activo	**Amenaza**	**Probabilidad**	**Impacto**				
			[D]	**[I]**	**[C]**	**[A]**	**[T]**
Activo 01	Amenaza 01	MB	MA		A		
	Amenaza 02	MB	MA				
	Amenaza 03	MB	MA		A		
	Amenaza 04	B	A		B		

Fuente: elaboración propia

Los resultados se pueden observar en el cuadro siguiente.

Cuadro 21.- Valoración de impactos

Activo	Amenaza	Probabilidad	Impacto				
			[D]	**[I]**	**[C]**	**[A]**	**[T]**
[hw_servidor_dl380g6] Servidor hp dl380g6	[N.1] Fuego	MB	MA				
	[N.2] Daños por agua	MB	MA				
	[N.*] Desastres naturales	MB	MA				
	[I.5] Avería de origen físico o lógico	B	A				
	[I.6] Corte del suministro eléctrico	A	M				
	[I.7] Condiciones inadecuadas de temperatura o humedad	B	A				
	[E.4] Errores de configuración	M		M			
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	B	A				
	[E.24] Caída del sistema por agotamiento de recursos	B	MA				
	[A.11] Acceso no autorizado	B		A	A		
	[A.23] Manipulación del *hardware*	B	B		A		
	[A.25] Robo de equipos	MB	MA		A		
[hw_maq_virtuales] Máquinas virtuales	[I.5] Avería de origen físico o lógico	MB	A				
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	B	A				
	[E.24] Caída del sistema por agotamiento de recursos	B	A				
	[A.11] Acceso no autorizado	MB		A	A		
	[A.23] Manipulación del *hardware*	MB	A		A		
[hw_maq_virtuales] Vpc_aws	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	MB	B				
	[A.11] Acceso no autorizado	MB		M	B		
[hw_servidor hp smf5600] Servidor hp smf5600	[N.1] Fuego	MB	MA				
	[N.2] Daños por agua	MB	MA				
	[N.*] Desastres naturales	MB	MA				
	[I.5] Avería de origen físico o lógico	M	A				
	[I.6] Corte del suministro eléctrico	B	M				
	[I.7] Condiciones inadecuadas de temperatura o humedad	B	A				
	[E.4] Errores de configuración	B		B			
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	B	A				
	[E.24] Caída del sistema por agotamiento de recursos	B	MA				
	[A.11] Acceso no autorizado	B		A	A		
	[A.23] Manipulación del *hardware*	B	A		A		
	[A.25] Robo de equipos	MB	MA		A		

[hw_servidor sun fire] Servidor *sunfire*	[N.1] Fuego	MB	MA				
	[N.2] Daños por agua	MB	MA				
	[N.*] Desastres naturales	MB	MA				
	[I.5] Avería de origen físico o lógico	MA	A				
	[I.6] Corte del suministro eléctrico	B	M				
	[I.7] Condiciones inadecuadas de temperatura o humedad	B	A				
	[E.4] Errores de configuración	B		M			
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	B	A	B			
	[E.24] Caída del sistema por agotamiento de recursos	MA	A	A			
	[A.11] Acceso no autorizado	B		A	A		
	[A.23] Manipulación del *hardware*	B	A		A		
	[A.25] Robo de equipos	MB	MA		A		
[hw_switch] *Switch*	[N.1] Fuego	MB	MA				
	[N.2] Daños por agua	MB	MA				
	[N.*] Desastres naturales	MB	MA				
	[I.5] Avería de origen físico o lógico	A	MA				
	[I.6] Corte del suministro eléctrico	A	M				
	[I.7] Condiciones inadecuadas de temperatura o humedad	B	A				
	[E.4] Errores de configuración	M		A			
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	B	MA				
	[E.24] Caída del sistema por agotamiento de recursos	A	MA				
	[A.11] Acceso no autorizado	B		MA	A		
	[A.23] Manipulación del *hardware*	B	MA		A		
	[A.25] Robo de equipos	MB	MA				
[hw_router] *Router*	[N.1] Fuego	MB	MA				
	[N.2] Daños por agua	MB	MA				
	[N.*] Desastres naturales	MB	MA				
	[I.5] Avería de origen físico o lógico	A	MA				
	[I.6] Corte del suministro eléctrico	A	M				
	[I.7] Condiciones inadecuadas de temperatura o humedad	B	A				
	[E.4] Errores de configuración	M		MA			
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	B	MA				
	[E.24] Caída del sistema por agotamiento de recursos	A	MA				
	[A.11] Acceso no autorizado	B		A	A		
	[A.23] Manipulación del *hardware*	B	A		A		

	[A.25] Robo de equipos	MB	MA		A		
[hw_almacenamiento] Almacenamiento emc	[N.1] Fuego	MB	MA				
	[N.2] Daños por agua	MB	MA				
	[N.*] Desastres naturales	MB	MA				
	[I.5] Avería de origen físico o lógico	M	MA				
	[I.6] Corte del suministro eléctrico	A	M				
	[I.7] Condiciones inadecuadas de temperatura o humedad	B	A				
	[I.10] Degradación de los soportes de almacenamiento de la información	M	A				
	[E.1] Errores de los usuarios	B	A	MA	MA		
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	B	MA				
	[E.24] Caída del sistema por agotamiento de recursos	M	MA	MA			
	[A.11] Acceso no autorizado	B		MA	MA	A	A
	[A.23] Manipulación del *hardware*	B	A		A		
	[A.25] Robo de equipos	MB	MA		A		
[com_internet] Internet	[I.8] Fallo de servicios de comunicaciones	M	MA				
	[E.2] Errores del administrador del sistema / de la seguridad	B	MA	A	A		
	[E.24] Caída del sistema por agotamiento de recursos	B	MA				
	[A.11] Acceso no autorizado	MB			A		
	[A.24] Denegación de servicio	MB	MA				
[com_lan] Red local	[I.8] Fallo de servicios de comunicaciones	B	MA				
	[E.2] Errores del administrador del sistema / de la seguridad	B	MA	A	A		
	[E.9] Errores de [re-]encaminamiento	B			A		
	[E.19] Fugas de información	MB			MA		
	[E.24] Caída del sistema por agotamiento de recursos	M	MA				
	[A.11] Acceso no autorizado	MB			A		
	[A.14] Interceptación de información (escucha)	MB			A		
	[A.24] Denegación de servicio	MB	B				
[aux_aire] Aire acondicionado	[N.1] Fuego	MB	A				
	[N.2] Daños por agua	MB	A				
	[N.*] Desastres naturales	MB	A				
	[I.6] Corte del suministro eléctrico	A	A				
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	B	M				
	[A.23] Manipulación del *hardware*	B	A		B		
[aux_generador] Generador eléctrico	[N.1] Fuego	MB	A				
	[N.2] Daños por agua	MB	A				

	[N.*] Desastres naturales	MB	A				
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	B	A				
	[A.23] Manipulación del *hardware*	A	A		B		
	[A.25] Robo de equipos	MB	MA		A		
[aux_ups] Sistemas de respaldo de energía	[N.1] Fuego	MB	MA				
	[N.2] Daños por agua	MB	MA				
	[N.*] Desastres naturales	MB	MA				
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	B	A				
	[A.23] Manipulación del *hardware*	MB	A		B		
	[A.25] Robo de equipos	MB	MA		A		
[l_datacenter] Cuarto de datos	[N.1] Fuego	MB	MA				
	[N.2] Daños por agua	MB	MA				
	[N.*] Desastres naturales	MB	MA				
	[A.6] Abuso de privilegios de acceso	MB	A	A	A		
[p_administrador_red] Administrador de red	[E.19] Fugas de información	MB			A		
	[E.28] Indisponibilidad del personal	B	M				
	[A.19] Revelación de información	MB			A		
	[A.30] Ingeniería social (picaresca)	MB	A	B	A		
[p_adm_plataformas] Administrador de plataformas	[E.19] Fugas de información	MB		A	A		
	[E.28] Indisponibilidad del personal	B	M				
	[A.19] Revelación de información	MB			A		
	[A.30] Ingeniería social (picaresca)	MB	A	A	A		
[p_desarrollador] Desarrollador	[E.19] Fugas de información	MB		A	MA		
	[E.28] Indisponibilidad del personal	B	M				
	[A.19] Revelación de información	MB			MA		
	[A.30] Ingeniería social (picaresca)	MB	A	A	MA		
[p_prov] Proveedor	[E.4] Errores de configuración	MB		A			
	[E.18] Destrucción de la información	MB	MA				
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	B	A				
	[E.28] Indisponibilidad del personal	MB	MA				
	[E.29] Extorción	MB	MA	MA	MA		

Fuente: elaboración propia.

Del análisis anterior, las amenazas de origen natural causan mayor daño, a pesar de tener una probabilidad de ocurrencia muy baja. Esto se debe a la ubicación física del cuarto de datos, se encuentra en el cuarto piso, en un lugar improvisado para alojar equipos de cómputo; es decir, no fue construido con las normas que exige la construcción de un cuarto de datos.

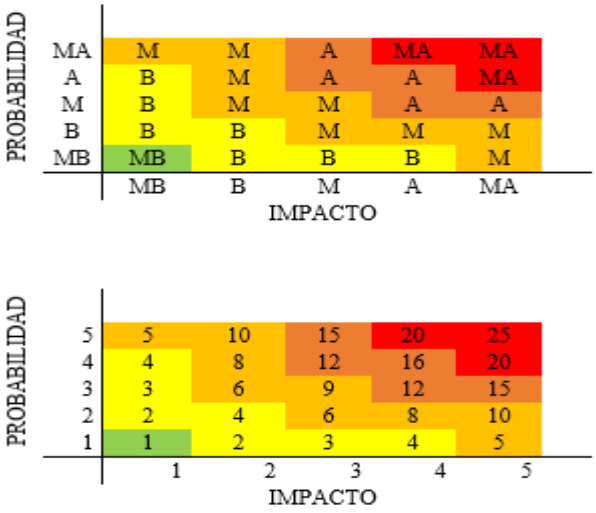
Las amenazas por errores y fallos no intencionados, poseen una probabilidad entre baja y media, pero su impacto es muy alto, esto se debe a que la institución no cuenta con equipos redundantes para que actúen como respaldo si el principal llega sufrir un daño.

Determinar Riesgos.- Calcular el riesgo en base al impacto de cada dimensión y la frecuencia de ocurrencia de la amenaza, para lo cual se genera una matriz de 5x5, en el eje de las X se coloca el impacto y en el eje de las Y la probabilidad; finalmente, el riesgo se obtiene producto del impacto y la probabilidad.

Riesgo = impacto * probabilidad

Todos los resultados de riesgo obtenido, deben ser validados en la matriz de riesgo que se indica en la figura siguiente.

Figura 9.- Matriz de riesgo



Fuente: adoptado de Consejo Superior de Administración Electrónica de España (2012)

En base al resultado obtenido en el paso anterior, se puede establecer el riesgo de una determinada zona, como se describe en la tabla a continuación detallada.

Tabla 7.- Equivalentes de escalas y pesos del riesgo

Rango	Zona	Descripción
20 – 25	MA	Riesgos que requieren mitigación inmediata
12 – 16	A	Riesgos que requieren planes de mitigación a corto plazo
5 – 10	M	Riesgos que requieren planes de mitigación a largo plazo
2 – 4	B	Riesgos que requieren seguimiento
1	MB	Riesgos que no requieren seguimiento

Fuente: elaboración propia

Los resultados de la determinación de riesgos se detallan en el siguiente capítulo.

Identificar vulnerabilidades.- Para determinar las vulnerabilidades o debilidades existentes en los servicios *web* de la PUCE Ambato, se despliega la herramienta informática con la cual se lleva a cabo el análisis de vulnerabilidades de los servicios *web*; para lo que, se configura la herramienta *Vega Subgraph*, es de libre acceso y utilización, además no requiere licencia alguna para su uso, ésta herramienta se instala previamente en un servidor con sistema operativo Linux, basado en la distribución *KaliLinux V2017.3*

La distribución *KaliLinux*, es una herramienta para auditoria informática, ya que cuenta con varios módulos que permiten analizar la seguridad informática desde varios puntos de vista. El despliegue de la herramienta *Vega Subgraph* se indican en el Apéndice B.

Por recomendación de las herramientas informáticas, se debe disponer de entornos de prueba para el análisis de vulnerabilidades, esto con el fin de evitar degradación del servicio a ser analizado. Por lo que, como condición dada por el Jefe del Departamento de Informática, se establece que todas las pruebas sean efectuadas en servidores de desarrollo, con la finalidad de no interferir en la disponibilidad de los servicios de producción, por lo que se procede con el despliegue de equipos de pruebas en los que, con la ayuda de los responsables de los servicios se levantan los últimos respaldos.

Para identificar los servicios a analizar, se debe disponer de las direcciones *web* que permiten el ingreso a cada uno de éstos. En el cuadro siguiente se detalla los servicios *web* de la PUCE Ambato a ser analizados, estas direcciones son las direcciones de producción, internamente se manejan las direcciones de pruebas para los análisis.

Cuadro 22.- Servicios *web* PUCE Ambato

Servicio	**Dirección**	**Estado**
Academics	http://app.pucesa.edu.ec:9000/academics/	Activo
Moodle	http://moodle.pucesa.edu.ec	Activo
Tablero de Control	http://app.pucesa.edu.ec:9009/tablero/	Activo
Impresión *web*	http://app.pucesa.edu.ec:9191/app	Activo
Catalogo en Línea	http://app.pucesa.edu.ec:9040/opac/	Activo
Repositorio Digital	http://repositorio.pucesa.edu.ec/	Activo
Mesa de Ayuda	http://app.pucesa.edu.ec:9675/pro_users/	Activo
Reserva Laboratorios	http://app.pucesa.edu.ec:9011/mrbs	Activo

Fuente: elaboración propia

Paso 4.- Iniciar el proceso de análisis del servicio *web*, los pasos se indican en el Apéndice C

Paso 5.- Llenar el formulario de detección de vulnerabilidades por servicio, para el seguimiento de éstos, el mismo se indica en el cuadro siguiente.

Cuadro 23.- Formulario para registrar las vulnerabilidades por servicio

Servicio	Nombre servicio a analizar		
Dirección	Dirección *web* del servicio		
Grado	**Número**	**Vulnerabilidad**	**Detalle**
Grado de afectación	Número de detecciones	Nombre de la vulnerabilidad detectada	Causa por la cual se detectó la vulnerabilidad

Fuente: elaboración propia

Los resultados del análisis, se detallan en el capítulo siguiente.

Determinar Salvaguardas.- Para determinar las protecciones a las debilidades detectadas en el análisis de los servicios *web*, se obtiene un listado de todas las vulnerabilidades en común, indiferentemente del servicio analizado o grado de afectación, analizar la vulnerabilidad con las consecuencias que éste genera, luego proponer todas las posibles soluciones para solventarla. Esto se debe registrar en el formulario que se indica a continuación.

Cuadro 24.- Formulario para registro de salvaguardas a vulnerabilidades

Vulnerabilidad	**Salvaguardia**
Vulnerabilidad 01	Salvaguardia 11 Salvaguardia 12 Salvaguardia 13
Vulnerabilidad 02	Salvaguardia 21 Salvaguardia 22 Salvaguardia 23

Fuente: elaboración propia

Una vez obtenidas las vulnerabilidades, son analizadas las remediaciones que podrían aplicarse, para lo que se propone lo mostrado en el cuadro siguiente, con la finalidad de que sea aplicado y validado en los servicios escaneados.

Cuadro 25.- Salvaguardas para vulnerabilidades detectadas

Vulnerabilidad	Salvaguarda
ASP/ASPX Error Detected / PHP Error Detected	1. El desarrollador deberá desactivar los mensajes de error para usuarios remotos. 2. Se deberá configurar errores personalizados para evitar mostrar los errores del sistema ya que contienen información del sistema.
Possible Source Code Disclosure	1. El desarrollador deberá validar que todos los complementos que use en el desarrollo, no desplieguen información de código fuente, en caso de detectar problemas deberá remover el complemento o verificar los permisos de acceso.
Bash ShellShock Injection	1. En equipos basados en Linux, se deberá mantener actualizado el *bash* a su última versión. 2. Se deberá mantener las mejores prácticas de seguridad para sistemas basados en Linux.
Cleartext Password over HTTP	1. Aplicar políticas de contraseñas, para que éstas cumplan con criterios de complejidad. 2. Se debe aplicar un certificado de seguridad que permita cifrar la información, así se evita que la información sea transmitida en texto plano.
Directory Listing Detected	1. Para servidores *web* Apache, en el archivo *htaccess* se deberá agregar la línea *Options – Indexes.* 2. En el archivo de configuración de apache, dentro de la sección <*Directory* /var/www/> remover la opción Indexes, lo que debe quedar únicamente *options FollowSymLinks.*
Email Addres Found	1. El desarrollador del sistema deberá verificar que no existe direcciones de correo incrustadas en ingresos proporcionados por el usuario. 2. No es recomendable mostrar las librerías de *javascript*, ya que el servidor puede mostrar automáticamente direcciones de correo electrónicas.
Form Password Field with Autocomplete Enabled	1. El desarrollador del sistema deberá deshabilitar el parámetro autocomplete del campo, esto es al atributo autocomplete del formulario asignarle el valor de *off*.
HTTP trace Support Detected	1. En servidores Apache, en la configuración del navegador *web*, se deberá colocar al parámetro *TraceEnable* el valor de *off*.

	2. Para servidores basados en IIS, se dispone del parámetro *EnableTraceMethod.*
Integer Overflow	1. El desarrollador deberá evitar un desbordamiento de enteros eligiendo un tipo entero que pueda contener todos los valores posibles de un cálculo. 2. El desarrollador deberá verificar todos los resultados de las operaciones matemáticas, con la finalidad de determinar condiciones de desbordamientos.
Internal Addresses Found	1. El desarrollador del sistema deberá aplicar las mejores prácticas de seguridad para evitar que direcciones internas del sistema sean expuestos a los usuarios remotos.
Local Filesystem Paths Found	1. El desarrollador debe personalizar la salida de errores, ya que las salidas por defecto contienen información confidencial, como rutas del sistema. 2. Los errores de éste tipo deben enviarse a un registro de eventos para ser analizados por el desarrollador.
Page Fingerprint Differential Detected-Possible Local File Include	1. El desarrollador del sistema debe predeterminar la ruta de los recursos del sistema de archivos y realizar comprobaciones de permiso de acceso. 2. En aplicaciones desarrolladas en ASP.NET se debe utilizar la función *GetFullPath(),* en PHP la función *realpath()*, y en *java* la función *getCanonicalPath(),* éstas funciones retornan la ruta predeterminada del recurso, lo que mitiga la vulnerabilidad.
Page Fingerprint Differential Detected-Possible Xpath Injection	1. El desarrollador del sistema deberá validar todas las entradas de usuario, al descartar todos los caracteres que sean peligrosos para la aplicación. 2. El desarrollador debe utilizar páginas de error personalizadas, ya que los errores por defecto del sistema pueden mostrar información sensible.
Session Cookie Without HttpOnly Flag	1. En desarrollos con PHP se deberá asignar al parámetro *session.cookie_httponly* el valor de True, dentro del archivo php.ini. 2. Para desarrollos de ASP.NET, dentro del archivo *web*.config, en el elemento *system.web/httpCookies* se deberá agregar la opción *httpCookies httpOnlyCookies="true*".
Session Cookie Without Secure Flag	1. En servidores *web* Apache, debe verificar si en al archivo httpd.conf posee activado el modulo

	mod_headers.so, y activar la opción *Header edit Set-Cookie* ^(.*)$ $1;*HttpOnly;Secure o Header set Set-Cookie HttpOnly;Secure* en Apache inferiores a la versión 2.2.4.
Shell Injection	1. El desarrollador del sistema deberá evitar la ejecución de comandos desde el intérprete de comandos. 2. Si es necesario la ejecución de comandos, el desarrollador deberá validar antes de ser ejecutados.
SQL Injection	1. El desarrollador del sistema deberá hacer uso de procedimientos almacenados para las transacciones con la base de datos. 2. En las variables tipo cadena, se deberá validar las entradas del usuario y descartar cualquier ingreso indebido. 3. Deberá hacer uso de consultas con parámetros. 4. Configurar controles de acceso a la base de datos, limita la explotación de la vulnerabilidad.
URL Injection	1. El desarrollador del sistema deberá aplicar las mejores prácticas de seguridad para la utilización de URL remotas.

Fuente: elaboración propia

Se analiza la factibilidad de aplicar las remediaciones necesarias para asegurar los servicios que son basadas en *software* libre, no poseen soporte, lo que dificulta el poder aplicar mitigación alguna, los servicios que son adquiridos poseen el licenciamiento pero no el código fuente, lo que dificulta la remediación, ya que se posee únicamente los binarios del aplicativo y en el servicio que es desarrollado por la institución no se encuentra inconveniente para la aplicación de las salvaguardas necesarias hasta reducir las mismas.

Para aplicar las salvaguardas que se indica, se prioriza las de grado Alto, es decir, se mitiga las vulnerabilidades con alto grado de riesgo a que sean atacadas, es así que, al aplicar las remediaciones y analizar nuevamente la vulnerabilidad se observó que el número de vulnerabilidades aumentó, al revisar se identificó que éste hecho se produce al aplicar los certificados de seguridad.

El problema con los certificados se dio en que, se generaron con una longitud de 1024 bits, lo que actualmente es vulnerable, al revisar documentación sobre la generación de certificados digitales se

recomienda que la longitud de un certificado digital debe de ser al menos 2048 bits, lo que les hace más seguros.

Luego de aplicar los nuevos certificados se realizan nuevamente los análisis respectivos, a lo que los resultados son favorables, se mitiga por completo la vulnerabilidad con respecto a los certificados digitales.

Capítulo 5

Resultados

5.1 Producto final del proyecto de titulación

El análisis de vulnerabilidades en los servicios *web* de la PUCE Ambato, se realiza a los servicios desplegados localmente como los de nube, por lo que, se analizan los activos que intervienen exclusivamente en la disponibilidad.

Las salvaguardas propuestas para minimizar las amenazas de los activos, no son ejecutadas, lo que queda a criterio de la organización el aplicarlas y realizar su seguimiento.

Para el análisis, se selecciona una herramienta gratuita que permite realizar un escáner de seguridad de las aplicaciones *web* y que ofrece un reporte de detecciones bastante amplio.

Una vez realizado los análisis previos, se determina los dos puntos esenciales en la presente investigación, los que son: Determinar Riesgos e Identificar Vulnerabilidades.

Determinar Riesgos.- En base a la probabilidad de ocurrencia y al impacto, se procede a determinar los riesgos, los que se indican en el cuadro siguiente:

Cuadro 26.- Riesgos identificados

Activo	Amenaza	Probabilidad	Riesgo				
			[D]	[I]	[C]	[A]	[T]
[hw_servidor_dl380g6] Servidor hp dl380g6	[N.1] Fuego	MB	M	-	-	-	-
	[N.2] Daños por agua	MB	M	-	-	-	-
	[N.*] Desastres naturales	MB	M	-	-	-	-
	[I.5] Avería de origen físico o lógico	B	M	-	-	-	-
	[I.6] Corte del suministro eléctrico	A	A	-	-	-	-
	[I.7] Condiciones inadecuadas de temperatura o humedad	B	M	-	-	-	-
	[E.4] Errores de configuración	M	-	M	-	-	-
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	B	M	-	-	-	-
	[E.24] Caída del sistema por agotamiento de recursos	B	M	-	-	-	-
	[A.11] Acceso no autorizado	B	-	M	M	-	-
	[A.23] Manipulación del *hardware*	B	B	-	M	-	-
	[A.25] Robo de equipos	MB	M	-	B	-	-
[hw_maq_virtuales] Máquinas virtuales	[I.5] Avería de origen físico o lógico	MB	B	-	-	-	-
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	B	M	-	-	-	-
	[E.24] Caída del sistema por agotamiento de recursos	B	M	-	-	-	-
	[A.11] Acceso no autorizado	MB	-	B	B	-	-
	[A.23] Manipulación del *hardware*	MB	B	-	B	-	-
[hw_maq_virtuales] Vpc_aws	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	MB	B	-	-	-	-
	[A.11] Acceso no autorizado	MB	-	B	B	-	-
[hw_servidor hp smf5600] Servidor hp smf5600	[N.1] Fuego	MB	M	-	-	-	-
	[N.2] Daños por agua	MB	M	-	-	-	-
	[N.*] Desastres naturales	MB	M	-	-	-	-
	[I.5] Avería de origen físico o lógico	M	A	-	-	-	-
	[I.6] Corte del suministro eléctrico	B	M	-	-	-	-
	[I.7] Condiciones inadecuadas de temperatura o humedad	B	M	-	-	-	-
	[E.4] Errores de configuración	B	-	B	-	-	-
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	B	M	-	-	-	-
	[E.24] Caída del sistema por agotamiento de recursos	B	M	-	-	-	-
	[A.11] Acceso no autorizado	B	-	M	M	-	-
	[A.23] Manipulación del *hardware*	B	M	-	M	-	-
	[A.25] Robo de equipos	MB	M	-	B	-	-

[hw_servidor sun fire] Servidor *sunfire*	[N.1] Fuego	MB	M	-	-	-	-
	[N.2] Daños por agua	MB	M	-	-	-	-
	[N.*] Desastres naturales	MB	M	-	-	-	-
	[I.5] Avería de origen físico o lógico	MA	MA	-	-	-	-
	[I.6] Corte del suministro eléctrico	B	M	-	-	-	-
	[I.7] Condiciones inadecuadas de temperatura o humedad	B	M	-	-	-	-
	[E.4] Errores de configuración	B	-	M	-	-	-
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	B	M	B	-	-	-
	[E.24] Caída del sistema por agotamiento de recursos	MA	MA	MA	-	-	-
	[A.11] Acceso no autorizado	B	-	M	M	-	-
	[A.23] Manipulación del *hardware*	B	M	-	M	-	-
	[A.25] Robo de equipos	MB	M	-	B	-	-
[hw_switch] *Switch*	[N.1] Fuego	MB	M	-	-	-	-
	[N.2] Daños por agua	MB	M	-	-	-	-
	[N.*] Desastres naturales	MB	M	-	-	-	-
	[I.5] Avería de origen físico o lógico	A	MA	-	-	-	-
	[I.6] Corte del suministro eléctrico	A	A	-	-	-	-
	[I.7] Condiciones inadecuadas de temperatura o humedad	B	M	-	-	-	-
	[E.4] Errores de configuración	M	-	A	-	-	-
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	B	M	-	-	-	-
	[E.24] Caída del sistema por agotamiento de recursos	A	MA	-	-	-	-
	[A.11] Acceso no autorizado	B	-	M	M	-	-
	[A.23] Manipulación del *hardware*	B	M	-	M	-	-
	[A.25] Robo de equipos	MB	M	-	-	-	-
[hw_router] *Router*	[N.1] Fuego	MB	M	-	-	-	-
	[N.2] Daños por agua	MB	M	-	-	-	-
	[N.*] Desastres naturales	MB	M	-	-	-	-
	[I.5] Avería de origen físico o lógico	A	MA	-	-	-	-
	[I.6] Corte del suministro eléctrico	A	A	-	-	-	-
	[I.7] Condiciones inadecuadas de temperatura o humedad	B	M	-	-	-	-
	[E.4] Errores de configuración	M	-	A	-	-	-
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	B	M	-	-	-	-
	[E.24] Caída del sistema por agotamiento de recursos	A	MA	-	-	-	-
	[A.11] Acceso no autorizado	B	-	M	M	-	-
	[A.23] Manipulación del *hardware*	B	M	-	M	-	-

	[A.25] Robo de equipos	MB	M	-	B	-	-
[hw_almacenamiento] Almacenamiento emc	[N.1] Fuego	MB	M	-	-	-	-
	[N.2] Daños por agua	MB	M	-	-	-	-
	[N.*] Desastres naturales	MB	M	-	-	-	-
	[I.5] Avería de origen físico o lógico	M	A	-	-	-	-
	[I.6] Corte del suministro eléctrico	A	A	-	-	-	-
	[I.7] Condiciones inadecuadas de temperatura o humedad	B	M	-	-	-	-
	[I.10] Degradación de los soportes de almacenamiento de la información	M	A	-	-	-	-
	[E.1] Errores de los usuarios	B	M	M	M	-	-
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	B	M	-	-	-	-
	[E.24] Caída del sistema por agotamiento de recursos	M	A	A	-	-	-
	[A.11] Acceso no autorizado	B	-	M	M	M	M
	[A.23] Manipulación del *hardware*	B	M	-	M	-	-
	[A.25] Robo de equipos	MB	M	-	B	-	-
[com_internet] Internet	[I.8] Fallo de servicios de comunicaciones	M	A	-	-	-	-
	[E.2] Errores del administrador del sistema / de la seguridad	B	M	M	M	-	-
	[E.24] Caída del sistema por agotamiento de recursos	B	M	-	-	-	-
	[A.11] Acceso no autorizado	MB	-	-	B	-	-
	[A.24] Denegación de servicio	MB	M	-	-	-	-
[com_lan] Red local	[I.8] Fallo de servicios de comunicaciones	B	M	-	-	-	-
	[E.2] Errores del administrador del sistema / de la seguridad	B	M	M	M	-	-
	[E.9] Errores de [re-]encaminamiento	B	-	-	M	-	-
	[E.19] Fugas de información	MB	-	-	M	-	-
	[E.24] Caída del sistema por agotamiento de recursos	M	A	-	-	-	-
	[A.11] Acceso no autorizado	MB	-	-	B	-	-
	[A.14] Interceptación de información (escucha)	MB	-	-	B	-	-
	[A.24] Denegación de servicio	MB	B	-	-	-	-
[aux_aire] Aire acondicionado	[N.1] Fuego	MB	B	-	-	-	-
	[N.2] Daños por agua	MB	B	-	-	-	-
	[N.*] Desastres naturales	MB	B	-	-	-	-
	[I.6] Corte del suministro eléctrico	A	A	-	-	-	-
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	B	M	-	-	-	-
	[A.23] Manipulación del *hardware*	B	M	-	B	-	-
[aux_generador] Generador eléctrico	[N.1] Fuego	MB	B	-	-	-	-
	[N.2] Daños por agua	MB	B	-	-	-	-

	[N.*] Desastres naturales	MB	B	-	-	-	-
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	B	M	-	-	-	-
	[A.23] Manipulación del *hardware*	A	A	-	M	-	-
	[A.25] Robo de equipos	MB	M	-	B	-	-
[aux_ups] Sistemas de respaldo de energía	[N.1] Fuego	MB	M	-	-	-	-
	[N.2] Daños por agua	MB	M	-	-	-	-
	[N.*] Desastres naturales	MB	M	-	-	-	-
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	B	M	-	-	-	-
	[A.23] Manipulación del *hardware*	MB	B	-	B	-	-
	[A.25] Robo de equipos	MB	M	-	B	-	-
[l_datacenter] Cuarto de datos	[N.1] Fuego	MB	M	-	-	-	-
	[N.2] Daños por agua	MB	M	-	-	-	-
	[N.*] Desastres naturales	MB	M	-	-	-	-
	[A.6] Abuso de privilegios de acceso	MB	B	B	B	-	-
[p_Administrador_red] administrador de red	[E.19] Fugas de información	MB	-	-	B	-	-
	[E.28] Indisponibilidad del personal	B	M	-	-	-	-
	[A.19] Revelación de información	MB	-	-	B	-	-
	[A.30] Ingeniería social (picaresca)	MB	B	B	B	-	-
[p_adm_plataformas] Administrador de plataformas	[E.19] Fugas de información	MB	-	B	B	-	-
	[E.28] Indisponibilidad del personal	B	M	-	-	-	-
	[A.19] Revelación de información	MB	-	-	B	-	-
	[A.30] Ingeniería social (picaresca)	MB	B	B	B	-	-
[p_desarrollador] Desarrollador	[E.19] Fugas de información	MB	-	B	M	-	-
	[E.28] Indisponibilidad del personal	B	M	-	-	-	-
	[A.19] Revelación de información	MB	-	-	M	-	-
	[A.30] Ingeniería social (picaresca)	MB	B	B	M	-	-
[p_prov] Proveedor	[E.4] Errores de configuración	MB	-	B	-	-	-
	[E.18] Destrucción de la información	MB	M	-	-	-	-
	[E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	B	M	-	-	-	-
	[E.28] Indisponibilidad del personal	MB	M	-	-	-	-
	[E.29] Extorción	MB	M	M	M	-	-

Fuente: elaboración propia

Como indica el modelo, se trata inicialmente la zona MA, las que son determinadas como muy críticas, dentro de ésta se encuentra:

El servidor *SunFire*, el que debido a los años con los que cuenta, adquirido en 2009, tiene probabilidades muy altas de sufrir daños en sus componentes o algún tipo de avería física o lógica, por lo que debe ser dado de baja.

El *Switch* de comunicaciones, tiene un riesgo muy alto de sufrir daños, por avería o agotamiento de recursos, por lo que se ve necesario el contar con un *switch* de respaldo o en su defecto implementar un sistema de alta disponibilidad, y evitar paralizaciones del servicio si sufriera daño alguno.

El *Router*, posee un riesgo muy alto de presentar averías de origen físico o lógico, como también puede presentar agotamiento en alguno de sus componentes y dejar de prestar servicio, por lo que se debe contar con un equipo de reemplazo.

En la zona Alta, los activos que más resaltan son el generador eléctrico y el aire acondicionado.

Identificar Vulnerabilidades.- En la tabla que se muestra a continuación, se detalla el resultado del servicio *Academics*.

Servicio *web*: *Academics*
Dirección: http://app.pucesa.edu.ec:9000/academics/

Tabla 8.- Vulnerabilidades servicio *Academics*

Grado	Número	Vulnerabilidad	Detalle
Alto	1	*Cleartext Password over HTTP*	Se detectó un formulario que puede enviar la clave en texto plano para su validación en el servidor, mediante un canal no seguro, lo que puede ser capturado fácilmente por terceras personas.
Alto	1	*Page Fingerprint Differential Detected-Possible Local File Include*	Se detectó una firma de respuesta diferente en relación a un archivo local, esto puede indicar que un archivo local incluye la vulnerabilidad, lo que puede permitir a los atacantes obtener acceso no autorizado a los archivos, también pueden indicar la presencia de una vulnerabilidad de enumeración de archivos, que en lugar de permitir al atacante obtener acceso a los archivos, les permita determinar si existen archivos en el sistema.

Bajo	1	*Form Password Field with Autocomplete Enabled*	La información ingresada en un formulario, puede ser almacenada por el navegador del equipo local, lo que puede ser descifrada por terceros.
Bajo	2	*Email Addres Found*	En el contenido escaneado, se han detectado patrones de direcciones de correo electrónico, las que pueden ser las direcciones de usuarios del sistema o direcciones de terceros integradas en los componentes de programación.
Bajo	3	*ASP/ASPX Error Detected*	La vulnerabilidad detectada puede revelar información detallada sobre errores que se produzcan en el aplicativo, la que puede ser aprovechada para generar ataques más complejos.

Fuente: elaboración propia

En la siguiente tabla, se resume las vulnerabilidades del servicio *Academics*

Tabla 9.- Resumen vulnerabilidades *Academics*

Grado	Número Vulnerabilidades
Alto	2
Medio	0
Bajo	6
Total	8

Fuente: elaboración propia

En la tabla que se muestra a continuación, se detalla los resultados obtenidos del servicio *Moodle*.

Servicio *web*: *Moodle*
Dirección: http://moodle.pucesa.edu.ec

Tabla 10.- Vulnerabilidades servicio *Moodle*

Grado	Número	Vulnerabilidad	Detalle
Alto	1	*Cleartext Password over HTTP*	Se detectó un formulario que puede enviar la clave en texto plano para su validación en el servidor, mediante un canal no seguro, lo que puede ser capturado fácilmente por terceras personas.
Medio	1	*HTTP trace Support Detected*	Esta vulnerabilidad permite que terceras personas pueden realizar trazas de sitios cruzados al utilizar scripts de *cross-site* para recupera el valor de la *cookie HttpOnly.*

Medio	40	*Local Filesystem Paths Found*	Se detecta la existencia de rutas absolutas del sistema de archivos, las que pueden revelar información sobre el diseño del sistema de archivos a terceras personas.
Medio	3	*PHP Error detected*	La vulnerabilidad detectada puede revelar información detallada sobre errores que se produzcan en el aplicativo, la que puede ser aprovechada para generar ataques más complejos.
Medio	1	*Possible Source Code Disclosure*	La vulnerabilidad permite que se pueda acceder a fragmentos de la aplicación, lo que podría usarse para extraer el código fuente de la aplicación y archivos de configuración.
bajo	46	*Directory Listing Detected*	El servidor envía el contenido de los directorios. Esto podría exponer archivos no destinados a la recuperación de usuario. El listado del directorio puede proporcionar información sobre el diseño y las características del sistema, como la codificación utilizada por los desarrolladores y administradores. Esta información puede aumentar la probabilidad de ataques por fuerza bruta.
Bajo	1	*Form Password Field with Autocomplete Enabled*	La información ingresada en un formulario, puede ser almacenada por el navegador del equipo local, lo que puede ser descifrada por terceros.

Fuente: elaboración propia

En la tabla siguiente, se resume las vulnerabilidades del servicio *Moodle*

Tabla 11.- Resumen vulnerabilidades *Moodle*

Grado	**Número Vulnerabilidades**
Alto	1
Medio	45
Bajo	47
Total	93

Fuente: elaboración propia

En la tabla siguiente, se detalla los resultados obtenidos del servicio Tablero de Control.

Servicio *web*: Tablero de Control
Dirección: http://app.pucesa.edu.ec:9009/tablero

Tabla 12.- Detalle servicio Tablero de Control

Grado	Número	Vulnerabilidad	Detalle
Alto	1	*Session Cookie Without Source Flag*	Si una *cookie* de sesión se configuró sin el indicador de seguridad, puede ser aprovechado por terceras personas para tener acceso a información no autorizada
Alto	1	*Session Cookie Without HttpOnly Flag*	Se ha detectado que la cookie se configuró sin el indicador *HttpOnly*. Cuando este indicador no está presente, es posible acceder a la cookie a través del código de *script* del lado del cliente.
Alto	3	*SQL Injection*	Estas vulnerabilidades están presentes cuando la información ingresada se usa para construir una consulta SQL. Si no se toman precauciones, la entrada suministrada puede modificar la cadena de consulta de manera que realice acciones sin intención. Estas acciones incluyen obtener acceso no autorizado de lectura o escritura a los datos almacenados en la base de datos, así como modificar la lógica de la aplicación.
Alto	3	*Shell Injection*	Es un ataque que busca la ejecución de comandos en el servidor, con el objetivo de acceder a la información, los comandos del sistema operativo suministrados por el atacante generalmente se ejecutan con los privilegios de la aplicación vulnerable.
Medio	1	*HTTP trace Support Detected*	Esta vulnerabilidad permite que terceras personas pueden realizar trazas de sitios cruzados al utilizar scripts de *cross-site* para recupera el valor de la cookie *HttpOnly*
Bajo	6	*Directory Listing Detected*	El servidor envía el contenido de los directorios. Esto podría exponer archivos no destinados a la recuperación de usuario. El listado del directorio puede proporcionar información sobre el diseño y las características del sistema, como la codificación utilizada por los desarrolladores y administradores. Esta información puede aumentar la probabilidad de ataques por fuerza bruta.

Fuente: elaboración propia

En la tabla indicada, se resume las vulnerabilidades del servicio Tablero de Control.

Tabla 13.- Resumen vulnerabilidades Servicio Tablero de Control

Grado	Número Vulnerabilidad
Alto	8
Medio	1
Bajo	6
Total	15

Fuente: elaboración propia

En la tabla siguiente, se detalla los resultados obtenidos del servicio Impresión *web*.

Servicio *web*: Impresión *web*
Dirección: http://app.pucesa.edu.ec:9191/app

Tabla 14.- Detalle vulnerabilidades servicio Impresión *web*

Grado	Número	Vulnerabilidad	Detalle
Alto	1	*Cleartext Password over HTTP*	Se detectó un formulario que puede enviar la clave en texto plano para su validación en el servidor, mediante un canal no seguro, lo que puede ser capturado fácilmente por terceras personas.
Alto	4	*Integer Overflow*	Se detectó que los valores enteros almacenados en variables, exceden el valor máximo permitido o que las operaciones aritméticas retornan valores que sobrepasan la capacidad de la variable declarada.
Alto	3	*Page Fingerprint Differential Detected-Possible Local File Include*	Se detectó una firma de respuesta diferente en relación a un archivo local, esto puede indicar que un archivo local incluye la vulnerabilidad, lo que puede permitir a los atacantes obtener acceso no autorizado a los archivos, también pueden indicar la presencia de una vulnerabilidad de enumeración de archivos, que en lugar de permitir al atacante obtener acceso a los archivos, les permita determinar si existen archivos en el sistema.
Medio	1	*HTTP Trace Support Detected*	Esta vulnerabilidad permite que terceras personas pueden realizar trazas de sitios cruzados al utilizar scripts de *cross-site* para recupera el valor de la cookie *HttpOnly.*
Medio	2	*Local Filesystem Paths Found*	Se detecta la existencia de rutas absolutas del sistema de archivos, las que pueden revelar información sobre el diseño del sistema de archivos a terceras personas.

Bajo	1	*Form Password Field with Autocomplete Enabled*	La información ingresada en un formulario, puede ser almacenada por el navegador del equipo local, lo que puede ser descifrada por terceros.
Bajo	2	*Internal Addresses Found*	Se ha detectado la existencia de referencias a otro equipo o redes en información que es de acceso público. Las que pueden revelar información sobre la estructura de la red a terceras personas.

Fuente: elaboración propia

En la tabla indicada, se resume las vulnerabilidades del servicio Impresión *web*.

Tabla 15.- Resumen vulnerabilidades servicio Impresión *web*

Grado	**Número Vulnerabilidad**
Alto	8
Medio	3
Bajo	3
Total	14

Fuente: elaboración propia

En la tabla indicada, se detalla los resultados obtenidos del servicio Catalogo en Línea.

Servicio *web*: Catalogo en Línea
Dirección: http://app.pucesa.edu.ec:9040/opac/

Tabla 16.- Detalle vulnerabilidades servicio Catalogo en Línea

Grado	**Número**	**Vulnerabilidad**	**Detalle**
Alto	1	*Cleartext Password over HTTP*	Se detectó un formulario que puede enviar la clave en texto plano para su validación en el servidor, mediante un canal no seguro, lo que puede ser capturado fácilmente por terceras personas.

Fuente: elaboración propia

En la tabla que se muestra a continuación, se resume las vulnerabilidades del servicio Catalogo

en Línea.

Tabla 17.- Resumen vulnerabilidades servicio Catalogo en Línea

Grado	**Número Vulnerabilidad**
Alto	1
Total	1

Fuente: elaboración propia

En la tabla siguiente, se detalla los resultados obtenidos del servicio Repositorio Digital.

Servicio *web*: Repositorio Digital
Dirección: http://repositorio.pucesa.edu.ec/

Tabla 18.- Detalle vulnerabilidades servicio Repositorio Digital

Grado	Número	Vulnerabilidad	Detalle
Alto	1	*Session Cookie Without Secure Flag*	Si una *cookie* de sesión se configuró sin el indicador de seguridad, puede ser aprovechado por terceras personas para tener acceso a información no autorizada.
Alto	28	*Page Fingerprint Differential Detected - Possible Xpath Injection*	Se detectó una firma de respuesta diferente en relación a una solicitud de inyección *XPath*, que puede indicar la existencia de una vulnerabilidad de inyección *XPath*, lo que puede permitir a los atacantes elevar los privilegios para acceder a la información.
Alto	29	*SQL Injection*	Estas vulnerabilidades están presentes cuando la información ingresada se usa para construir una consulta SQL. Si no se toman precauciones, la entrada suministrada puede modificar la cadena de consulta de manera que realice acciones sin intención. Estas acciones incluyen obtener acceso no autorizado de lectura o escritura a los datos almacenados en la base de datos, así como modificar la lógica de la aplicación.
Alto	33	*Shell Injection*	Es un ataque que busca la ejecución de comandos en el servidor, con el objetivo de acceder a la información, los comandos del sistema operativo suministrados por el atacante generalmente se ejecutan con los privilegios de la aplicación vulnerable.
Alto	42	*Integer Overflow*	Se detectó que los valores enteros almacenados en variables, exceden el valor máximo permitido o que las operaciones aritméticas retornan valores que sobrepasan la capacidad de la variable declarada.
Alto	4	*Bash ShellShock Injection*	Es una vulnerabilidad que permite la ejecución de código remoto por línea de comando en el servidor, mediante acceso no autorizado

Alto	28	*Page Fingerprint Differential Detected - Possible Local File Include*	Se detectó una firma de respuesta diferente en relación a un archivo local, esto puede indicar que un archivo local incluye la vulnerabilidad, lo que puede permitir a los atacantes obtener acceso no autorizado a los archivos, también pueden indicar la presencia de una vulnerabilidad de enumeración de archivos, que en lugar de permitir al atacante obtener acceso a los archivos, les permita determinar si existen archivos en el sistema.
Medio	4	*URL Injection*	Se ha determinado que una etiqueta HTML en la página de destino tiene un atributo (como src, href o *value*) que es un URI suministrado por el escáner. Existe una variedad de implicaciones de seguridad, dependiendo de la etiqueta. Las consecuencias más graves incluyen ataques de *phishing* o posibles riesgos entre dominios que pueden ocurrir si el navegador del usuario objetivo obtiene contenido malicioso automáticamente desde estos enlaces.

Fuente: elaboración propia

En la tabla detallada, se resumen los resultados obtenidos del servicio Repositorio Digital.

Tabla 19.- Resumen vulnerabilidades servicio Repositorio Digital

Grado	**Número Vulnerabilidad**
Alto	165
Medio	4
Total	169

Fuente: elaboración propia

En la tabla siguiente, se detalla los resultados obtenidos del servicio Mesa de Ayuda.

Servicio *web*: Mesa de Ayuda
Dirección: http://app.pucesa.edu.ec:9675/pro_users/

Tabla 20.- Detalle vulnerabilidades servicio Mesa de Ayuda

Grado	Número	Vulnerabilidad	Detalle
Alto	1	*Session Cookie Without Secure Flag*	Si una *cookie* de sesión se configuró sin el indicador de seguridad, puede ser aprovechado por terceras personas para tener acceso a información no autorizada.
Alto	2	*Creartext Password over HTTP*	Se detectó una firma de respuesta diferente en relación a un archivo local, esto puede indicar que un archivo local incluye la vulnerabilidad, lo que puede permitir a los atacantes obtener acceso no autorizado a los archivos, también pueden indicar la presencia de una vulnerabilidad de enumeración de archivos, que en lugar de permitir al atacante obtener acceso a los archivos, les permita determinar si existen archivos en el sistema.
Alto	1	*Page Fingerprint Differential Detected-Possible Local File Include*	Se detectó una firma de respuesta diferente en relación a un archivo local, esto puede indicar que un archivo local incluye la vulnerabilidad, lo que puede permitir a los atacantes obtener acceso no autorizado a los archivos, también pueden indicar la presencia de una vulnerabilidad de enumeración de archivos, que en lugar de permitir al atacante obtener acceso a los archivos, les permita determinar si existen archivos en el sistema.
Bajo	2	*Form Password Field with Autocomplete Enabled*	La información ingresada en un formulario, puede ser almacenada por el navegador del equipo local, lo que puede ser descifrada por terceros.

Fuente: elaboración propia

A continuación, se resume los resultados obtenidos del servicio Mesa de Ayuda.

Tabla 21.- Resumen vulnerabilidades del servicio Mesa de Ayuda

Grado	Número Vulnerabilidad
Alto	4
Bajo	2
Total	6

Fuente: elaboración propia

En la tabla siguiente, se detalla los resultados obtenidos del servicio Reserva Laboratorios.

Servicio *web*: Reserva Laboratorios
Dirección: http://app.pucesa.edu.ec:9011/mrbs

Tabla 22.- Detalle vulnerabilidades servicio Reserva Laboratorios

Grado	Número	Vulnerabilidad	Detalle
Alto	24	*Integer Overflow*	Se detectó que los valores enteros almacenados en variables, exceden el valor máximo permitido o que las operaciones aritméticas retornan valores que sobrepasan la capacidad de la variable declarada.
Alto	8	*Shell Injection*	Es un ataque que busca la ejecución de comandos en el servidor, con el objetivo de acceder a la información, los comandos del sistema operativo suministrados por el atacante generalmente se ejecutan con los privilegios de la aplicación vulnerable.
Alto	7	*SQL Injection*	Estas vulnerabilidades están presentes cuando la información ingresada se usa para construir una consulta SQL. Si no se toman precauciones, la entrada suministrada puede modificar la cadena de consulta de manera que realice acciones sin intención. Estas acciones incluyen obtener acceso no autorizado de lectura o escritura a los datos almacenados en la base de datos, así como modificar la lógica de la aplicación.
Medio	1	*HTTP Trace Support Detected*	Esta vulnerabilidad permite que terceras personas pueden realizar trazas de sitios cruzados al utilizar scripts de *cross-site* para recupera el valor de la cookie *HttpOnly*

Fuente: elaboración propia

En la tabla se detalla el resumen de los resultados obtenidos del servicio Reserva Laboratorios.

Tabla 23.- Resumen vulnerabilidades servicio Reserva Laboratorios

Grado	Número Vulnerabilidad
Alto	39
Medio	1
Total	40

Fuente: elaboración propia

Verificar

Se verifica las salvaguardas establecidas, para comprobar que fueron efectivas para mitigar las vulnerabilidades detectadas.

Monitorear Resultados.- Con la finalidad de verificar las salvaguardas, se realiza nuevamente un análisis de vulnerabilidades, a lo que se adjunta un comparativo de los resultados iniciales y finales, a continuación se detalla los resultados obtenidos.

Academics

En la tabla siguiente, se detalla los resultados obtenidos del servicio *Academics* luego de haber aplicado las salvaguardas.

Servicio *web*: *Academics*
Dirección: http://app.pucesa.edu.ec:9000/academics/

Tabla 24.- Vulnerabilidades servicio *Academics* luego de salvaguardas

Grado	Número	Vulnerabilidad
Alto	0	Cleartext Password over HTTP
Alto	0	Page Fingerprint Differential Detected-Possible Local File Include
Bajo	0	Form Password Field with Autocomplete Enabled
Bajo	2	Email Addres Found
Bajo	3	ASP/ASPX Error Detected

Fuente: elaboración propia

En la tabla, se resume el número de vulnerabilidades obtenidas antes y después de aplicar las salvaguardas, también se indica las vulnerabilidades por mitigar

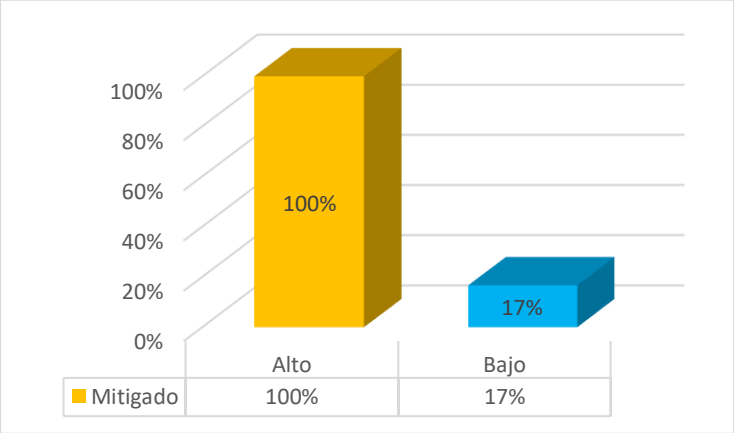
Tabla 25.- Comparativo de resultados servicio *Academics*

Grado	Antes	Después	Mitigado
Alto	2	0	2
Medio	0	0	0
Bajo	6	5	1
Total	8	5	3

Fuente: elaboración propia

En el siguiente gráfico se muestra en porcentajes las vulnerabilidades mitigadas.

Gráfico 4.- Porcentaje reducción vulnerabilidades *Academics*



Fuente: elaboración propia

El servicio *Academics* es un desarrollo propio de la Universidad, cuenta con el soporte del desarrollador para aplicar las recomendaciones de seguridad, al atacar a las de mayor grado; por tal motivo, se logra mitigar el 100% de las vulnerabilidades Altas, que es el objetivo.

Moodle

En la tabla, se detalla los resultados obtenidos del servicio *Moodle* luego de haber aplicado las salvaguardas.

Servicio *web*: *Moodle*
Dirección: http://moodle.pucesa.edu.ec

Tabla 26.- Vulnerabilidades servicio *Moodle* luego de salvaguardas

Grado	Número	Vulnerabilidad
Alto	0	*Cleartext Password over HTTP*
Medio	0	*HTTP trace Support Detected*
Medio	40	*Local Filesystem Paths Found*
Medio	3	*PHP Error detected*
Medio	1	*Possible Source Code Disclosure*
Bajo	0	*Directory Listing Detected*
Bajo	0	*Form Password Field with Autocomplete Enabled*

Fuente: elaboración propia

En la tabla siguiente, se resume el número de vulnerabilidades obtenidas antes y después de aplicar las salvaguardas.

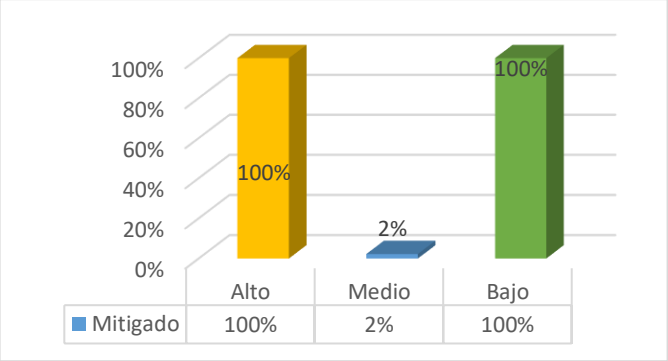
Tabla 27.- Comparativo de resultados servicio *Moodle*

Grado	Antes	Después	Mitigado
Alto	1	0	1
Medio	45	44	1
Bajo	47	0	47
Total	93	44	49

Fuente: elaboración propia

En el gráfico, se muestra en porcentajes las vulnerabilidades mitigadas

Gráfico 5.- Porcentaje reducción vulnerabilidades *Moodle*



Fuente: elaboración propia

El servicio *Moodle* es una plataforma de acceso libre, desarrollada por terceros, por lo que no se posee soporte para poder aplicar las recomendaciones de seguridad en el desarrollo, las vulnerabilidades son corregidas en nuevas versiones o actualizaciones que emite la empresa desarrolladora, por lo que se ve limitado el poder aplicar las recomendaciones a nivel de programación, en lo que si se logra mitigar vulnerabilidades es a nivel de servidor; por tal motivo, se logra mitigar el 100% de las vulnerabilidades altas y el 100% de vulnerabilidades bajas, las vulnerabilidades media hacen referencia a desarrollo como tal.

Tablero de Control

En la tabla indicada, se detalla los resultados obtenidos del servicio Tablero de Control, luego de haber aplicado las salvaguardas.

Servicio *web*: Tablero de Control
Dirección: http://app.pucesa.edu.ec:9009/tablero

Tabla 28.- Vulnerabilidades servicio Tablero de Control luego de salvaguardas

Grado	Número	Vulnerabilidad
Alto	0	*Session Cookie Without Source Flag*
Alto	0	*Session Cookie Without HttpOnly Flag*
Alto	3	*SQL Injection*
Alto	3	*Shell Injection*
Medio	0	*HTTP trace Support Detected*
Bajo	6	*Directory Listing Detected*

Fuente: elaboración propia

En la tabla siguiente, se resume el número de vulnerabilidades obtenidas antes y después de aplicar las salvaguardas.

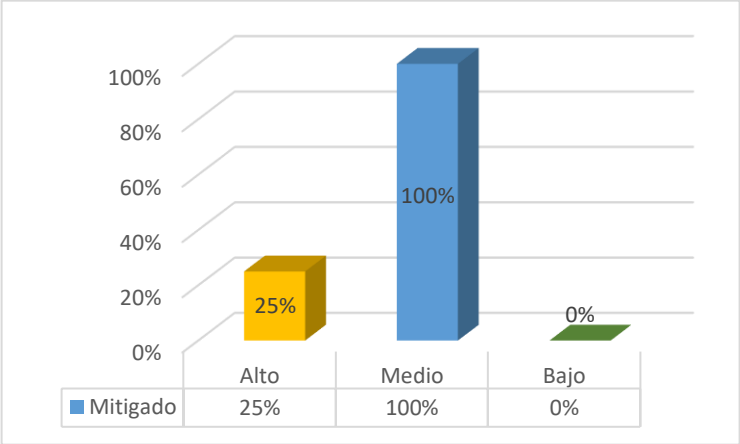
Tabla 29.- Comparativo de resultados servicio Tablero de Control

Grado	Antes	Después	Mitigado
Alto	8	6	2
Medio	1	0	1
Bajo	6	6	0
Total	15	12	3

Fuente: elaboración propia

En el gráfico se muestra en porcentajes las vulnerabilidades mitigadas.

Gráfico 6.- Porcentaje reducción vulnerabilidades tablero de Control



Fuente: elaboración propia

El servicio Tablero de Control es un servicio desarrollado por terceros, por lo que no posee el soporte necesario para aplicar las recomendaciones de seguridad a nivel de desarrollo, se mitiga

las vulnerabilidades a nivel de servidor, por tal motivo se mitiga únicamente el 25% de las vulnerabilidades Altas.

Impresión web

En la tabla siguiente, se detalla los resultados obtenidos del servicio Impresión *web*, luego de haber aplicado las salvaguardas.

Servicio *web*: Impresión *web*
Dirección: http://app.pucesa.edu.ec:9191/app

Tabla 30.- Vulnerabilidades servicio Impresión *web* luego de salvaguardas

Grado	Número	Vulnerabilidad
Alto	0	*Cleartext Password over HTTP*
Alto	4	*Integer Overflow*
Alto	3	*Page Fingerprint Differential Detected-Possible Local File Include*
Medio	0	*HTTP Trace Support Detected*
Medio	2	*Local Filesystem Paths Found*
Bajo	1	*Form Password Field with Autocomplete Enabled*
Bajo	2	*Internal Addresses Found*

Fuente: elaboración propia

En la tabla siguiente se resume el número de vulnerabilidades obtenidas antes y después de aplicar las salvaguardas, indicándose las vulnerabilidades por mitigar.

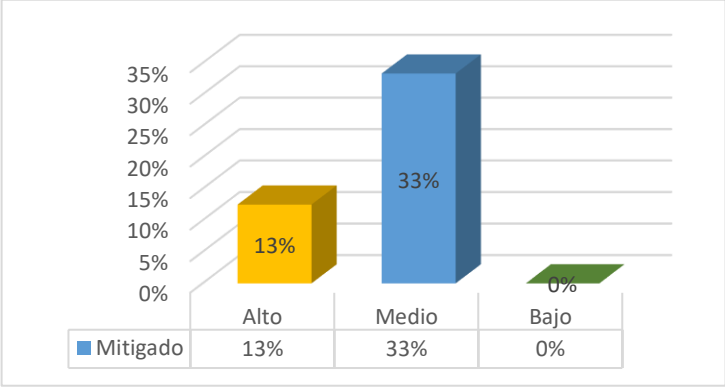
Tabla 31.- Comparativo de resultados servicio Impresión *web*

Grado	Antes	Después	Mitigado
Alto	8	7	1
Medio	3	2	1
Bajo	3	3	0
Total	14	12	2

Fuente: elaboración propia

En el gráfico siguiente, se muestra en porcentajes las vulnerabilidades mitigadas.

Gráfico 7.- Porcentaje reducción vulnerabilidades Impresión *web*



Fuente: elaboración propia

El servicio Impresión *web* es un servicio desarrollado por terceros, posee un licenciamiento para la version13, lanzada en 2013, pero al momento existe la versión 16 en la que se corrigen varias de las vulnerabilidades detectadas tanto a nivel de desarrollo como a nivel de servidor *web*, a pesar de ello se logra mitigar únicamente el 13% de las vulnerabilidades Altas.

Catálogo en Línea

En la tabla siguiente, se detalla los resultados obtenidos del servicio Catalogo en Línea, luego de haber aplicado las salvaguardas.

Servicio *web*: Catalogo en Línea
Dirección: http://app.pucesa.edu.ec:9040/opac/

Tabla 32.- Vulnerabilidades servicio Catalogo en Línea luego de salvaguardas

Grado	Número	Vulnerabilidad
alto	0	*Cleartext Password over HTTP*

Fuente: elaboración propia

En la tabla siguiente, se resume el número de vulnerabilidades obtenidas antes y después de aplicar las salvaguardas, también se indica las vulnerabilidades a mitigar.

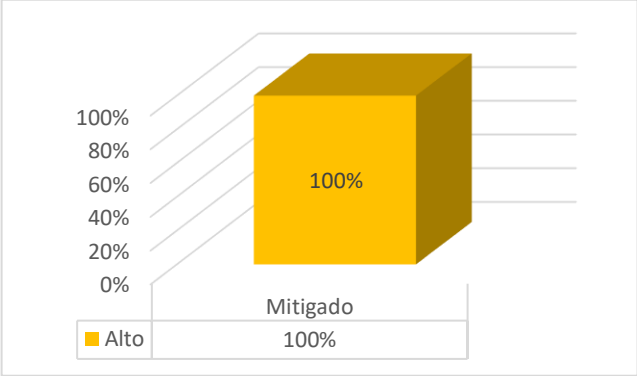
Tabla 33.- Comparativo de resultados servicio Catalogo en Línea

Grado	Antes	Después	Mitigado
Alto	1	0	1
Total	1	0	1

Fuente: elaboración propia

En el gráfico se detalla el porcentaje de las vulnerabilidades mitigadas

Gráfico 8.- Porcentajes reducción vulnerabilidades Catalogo en Línea



Fuente: elaboración propia

El servicio Catálogo en Línea es un servicio desarrollado por terceros, posee un licenciamiento para la versión 9, lanzada en 2015, se cuenta con el soporte necesario en caso de requerir cambios en el desarrollo, pero como se observa en el análisis, posee excelentes seguridades a nivel de su desarrollo ya que la vulnerabilidad detectada es únicamente por el certificado de seguridad que debe aplicarse a nivel de servidor *web*, por lo que se logra mitigar el 100% de las vulnerabilidades.

Repositorio Digital

En la tabla siguiente, se detalla los resultados obtenidos del servicio Repositorio Digital, luego de haber aplicado las salvaguardas.

Servicio *web*: Repositorio Digital
Dirección: http://repositorio.pucesa.edu.ec/

Tabla 34.- Vulnerabilidades servicio Repositorio Digital luego de salvaguardas

Grado	Número	Vulnerabilidad
Alto	0	*Session Cookie Without Secure Flag*
Alto	28	*Page Fingerprint Differential Detected - Possible Xpath Injection*
Alto	29	*SQL Injection*
Alto	33	*Shell Injection*
Alto	42	*Integer Overflow*
Alto	4	*Bash ShellShock Injection*
Alto	28	*Page Fingerprint Differential Detected - Possible Local File Include*
Medio	4	*URL Injection*

Fuente: elaboración propia

En la tabla, se resume el número de vulnerabilidades obtenidas antes y después de aplicar las salvaguardas, también se indica las vulnerabilidades por mitigar.

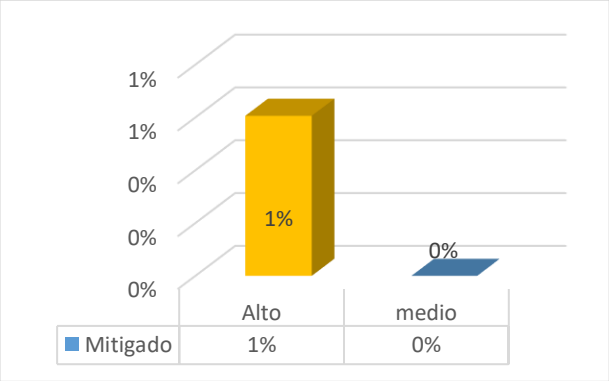
Tabla 35.- Comparativo de resultados servicio Repositorio Digital

Grado	Antes	Después	Mitigado
Alto	165	164	1
Medio	4	4	0
Total	169	168	1

Fuente: elaboración propia

En el siguiente gráfico, se muestra en porcentajes las vulnerabilidades mitigadas.

Gráfico 9.- Porcentajes reducción vulnerabilidades Repositorio Digital



Fuente: elaboración propia

El servicio Repositorio Digital es un desarrollado de terceros, es de libre uso, no posee licenciamiento de soporte, es decir que las vulnerabilidades críticas que se detecten son mitigadas en nuevas versiones, actualmente se cuenta con la versión 5.0 lanzada en 2016, al momento existe la versión 6 en la que se corrigen varias de las vulnerabilidades altas detectadas, es así que, se hace difícil el poder mitigar las vulnerabilidades a nivel de desarrollo como a nivel de servidor *web*, por lo que se logra mitigar únicamente el 1% de las vulnerabilidades Altas.

Mesa de Ayuda

En la tabla siguiente, se detalla los resultados obtenidos del servicio Mesa de Ayuda, luego de haber aplicado las salvaguardas.

Servicio *web*: Mesa de Ayuda
Dirección: http://app.pucesa.edu.ec:9675/pro_users/

Tabla 36.- Vulnerabilidades servicio Mesa de Ayuda luego de salvaguardas

Grado	Número	Vulnerabilidad
Alto	0	*Session Cookie Without Secure Flag*
Alto	0	*Creartext Password over HTTP*
Alto	0	*Page Fingerprint Differential Detected- Possible Local File Include*
Bajo	0	*Form Password Field with Autocomplete Enabled*

Fuente: elaboración propia

En la tabla siguiente, se resume el número de vulnerabilidades obtenidas antes y después de aplicar las salvaguardas, también se indica las vulnerabilidades por mitigar.

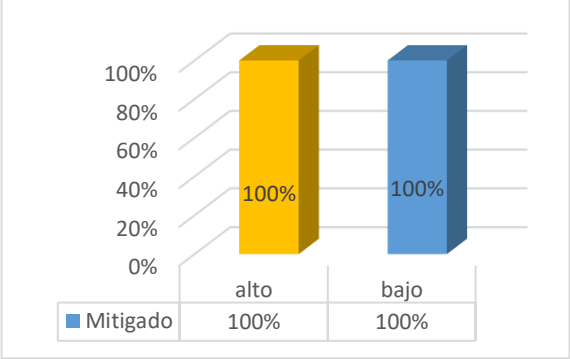
Tabla 37.- Comparativo de resultados servicio Mesa de Ayuda

Grado	Antes	Después	Mitigado
Alto	4	0	4
Bajo	2	0	2
Total	6	0	6

Fuente: elaboración propia

En el gráfico se muestra en porcentajes las vulnerabilidades mitigadas.

Gráfico 10.- Porcentaje reducción vulnerabilidades Mesa de Ayuda



Fuente: elaboración propia

El servicio Mesa de Ayuda es un desarrollado de terceros, es de libre uso, no posee licenciamiento de soporte, es decir que se hace difícil el poder mitigar las vulnerabilidades a nivel de desarrollo pues se cuenta únicamente con los binarios, pero del análisis realizado es bastante satisfactorio, ya que las vulnerabilidades son a nivel de despliegue de servidor, lo que se logra mitigar el 100% de vulnerabilidades con la aplicación de las recomendaciones.

Reserva Laboratorios

En la tabla siguiente, se detalla los resultados obtenidos del servicio Reserva Laboratorios, luego de haber aplicado las salvaguardas.

Servicio *web*: Reserva Laboratorios
Dirección: http://app.pucesa.edu.ec:9011/mrbs

Tabla 38.- Vulnerabilidades servicio Reserva Laboratorios luego de salvaguardas

Grado	Número	Vulnerabilidad
Alto	24	*Integer Overflow*
Alto	8	*Shell Injection*
Alto	7	*SQL Injection*
Medio	0	*HTTP Trace Support Detected*

Fuente: elaboración propia

En la tabla se resume el número de vulnerabilidades obtenidas antes y después de aplicar las salvaguardas, también se indica las vulnerabilidades por mitigar.

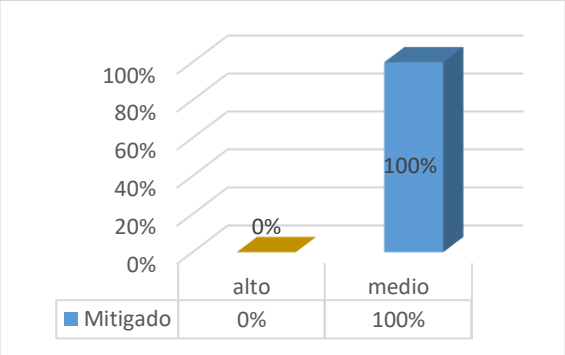
Tabla 39.- Comparativo de resultados servicio Reserva Laboratorios

Grado	Antes	Después	Mitigado
Alto	39	39	0
Medio	1	0	1
Total	40	39	1

Fuente: elaboración propia

En la figura se muestra en porcentajes las vulnerabilidades mitigadas.

Gráfico 11.- Porcentaje reducción vulnerabilidades Reserva Laboratorios



Fuente: elaboración propia

El servicio Reserva Laboratorios es desarrollado por terceros, es de libre uso, no posee licenciamiento de soporte, es decir que se hace difícil el poder mitigar las vulnerabilidades a nivel de desarrollo, ya que se posee únicamente los binarios, se logra mitigar únicamente vulnerabilidades a nivel de servidor, el que representa un 100% de grado Bajo, pero las altas hacen referencia a problemas de desarrollo.

Actuar

Se establece el periodo en el cual se debe llevar a cabo una nueva verificación de los servicios, para determinar que las salvaguardas estén bien definidas

Retroalimentación.- Se debe indicar que las vulnerabilidades residuales deben ser analizadas y mitigadas hasta que sean reducidas en el mayor número posible, esto debe contemplarse como un marco de mejora continua, también se debe mantener una bitácora de las vulnerabilidades más comunes y cuál es su mitigación, en la tabla siguiente se resume el número de vulnerabilidades encontradas al inicio del análisis como también las que se obtuvo al final de una iteración de mitigaciones, la que es un punto de partida para llevar un control en la reducción de vulnerabilidades.

Tabla 40.- Resumen de vulnerabilidades mitigadas

Servicio	Antes			Después		
	Alto	medio	Bajo	Alto	medio	Bajo
Academics	2	0	6	0	0	5
Moodle	1	45	47	0	44	0
Tablero de Control	8	1	6	6	0	6
Impresión *Web*	8	3	3	7	2	3
Catalogo en Línea	1	0	0	0	0	0
Repositorio Digital	165	4	0	164	4	0
Mesa de ayuda	4	0	2	0	0	0
Reserva Laboratorios	39	1	0	39	0	0
SUMA	**228**	**54**	**64**	**216**	**50**	**14**

Fuente: Elaboración propia

5.2 Comprobación del modelo

Para comprobar que las vulnerabilidades de los servicios *web* de la PUCE Ambato son reducidas con la aplicación del modelo propuesto, se utiliza la estadística inferencial al aplicar la prueba de chi-cuadrado a los resultados obtenidos en los análisis realizados, con lo que se determina la siguiente hipótesis nula H0 y la hipótesis alternativa H1:

- Hipótesis nula (H0).- El modelo propuesto no mitiga las vulnerabilidades de los servicios *web* de la PUCE Ambato, ya que la reducción de vulnerabilidades no

depende de las salvaguardas, al establecer un grado de significancia del 5% para el cálculo de Chi-cuadrado.

- Hipótesis alternativa (H1).- El modelo propuesto si mitiga las vulnerabilidades de los servicios *web* de la PUCE Ambato, ya que la reducción de vulnerabilidades depende de las salvaguardas, al establecer un grado de significancia del 5% para el cálculo de Chi-cuadrado.

Al finalizar el análisis de vulnerabilidades altas, se obtuvo la siguiente tabla de valores observados.

Tabla 41.- Frecuencias de valores observados

	Valores Observados	
Análisis	**Antes**	**Después**
Vulnerabilidades altas	228	216
Vulnerabilidades altas mitigadas	0	12

Fuente: elaboración propia

Para el cálculo la prueba de chi-cuadrado se realiza los siguientes pasos:

1. Sumar las filas y columnas, para obtener la sumatoria de frecuencias observadas, como se observa la siguiente tabla.

Tabla 42.- Sumatoria de frecuencias de valores observados

	Valores Observados		
Análisis	**Antes**	**Después**	**Total**
Vulnerabilidades altas	228	216	444
Vulnerabilidades altas mitigadas	0	12	12
Total	228	228	**456**

Fuente: elaboración propia

2. Calcular las frecuencias de valores esperadas

$$fe = \frac{total\ columna * total\ fila}{\sum total\ fila}$$

$$fe(antes\ altas) = \frac{228 * 444}{456} = 222$$

$$fe(antes\ altas\ mitigadas) = \frac{228 * 12}{456} = 6$$

$$fe(despues\ altas) = \frac{228 * 444}{456} = 222$$

$$fe(despues\ altas\ mitigadas) = \frac{228 * 12}{456} = 6$$

Al finalizar los cálculos, se obtiene la siguiente tabla de frecuencias esperadas.

Tabla 43.- Frecuencias de valores esperadas

Análisis	**Antes**	**Después**
Vulnerabilidades altas	222	222
Vulnerabilidades altas mitigadas	6	6

Fuente: elaboración propia

3. Calcular X^2calc

$$X^2calc = \sum . \frac{(fo - fe)2}{fe}$$

$$fo = Frecuencia\ de\ valor\ observado$$

$$fe = Frecuencia\ de\ valor\ esperado$$

$$X^2calc = \frac{(228 - 222)2}{222} + \frac{(216 - 222)2}{222} + \frac{(0 - 6)2}{6} + \frac{(12 - 6)2}{6}$$

$$X^2calc = 12.3243$$

4. Calcular el grado de libertad

$$V = (Cantidad\ de\ filas - 1) * (Cantidad\ de\ columnas - 1)$$

$$V = (2 - 1) * (2 - 1)$$

$$V = 1$$

5. Calcular grado de significancia

G= 5%, de acuerdo al enunciado

6. Calcular el parámetro P

$$P = (1 - Grado\ de\ significancia)$$

$$P = (1 - 0.05) = 0.95$$

7. Encontrar en la tabla de criticidad, el valor critico correspondiente a 1 grado de libertad y p=0.95

$$X^2critico = 3.841$$

8. Comparar resultados

   Si el valor de chi-cuadrado calculado es menor o igual que chi-cuadrado crítico, entonces se acepta la hipótesis nula (H0), caso contrario se acepta la hipótesis alternativa (H1).

   $X^2calc \leq X^2critico \rightarrow H0$

   $X^2calc \geq X^2critico \rightarrow H1$

   $X^2calc = 12.3243$

   $X^2critico = 3.841$

   $12.3243 \geq 3.841 \rightarrow H1$

Análisis de resultados

Como se observa en el resultado obtenido, Chi Cuadrado calculado es mayor que Chi-Cuadrado crítico, por lo que se rechaza la hipótesis nula (H0) y se acepta la hipótesis alternativa (H1); es decir, se demuestra que la aplicabilidad del modelo propuesto reduce las vulnerabilidades de los servicios *web* de la PUCE Ambato con un nivel de significancia del 5% para el cálculo de Chi Cuadrado.

Capítulo 6

Conclusiones y Recomendaciones

6.1 Conclusiones

En el marco teórico se analiza las metodologías *coras, magerit y octave* para la gestión de riesgos informáticos, se revisa los definiciones que engloban la seguridad informática; igualmente, los problemas de seguridad informática detectados en otras instituciones, los que son de gran aporte a la presente investigación y permite fortalecer la propuesta.

En el análisis realizado, el servicio *Academics* es un desarrollo propio, los servicios Impresión *web*, Catalogo en Línea y Tablero de Control son adquiridos y el servicio de *Moodle*, Repositorio Digital, Reserva Laboratorios y Mesa de Ayuda son basados en *software* libre; se determina que, los de mayor dificultad para aplicar las salvaguardas son los adquiridos, ya que se posee únicamente los ejecutables.

De los servicios analizados, el Repositorio Digital posee el mayor número de vulnerabilidades, con 165 de grado alto y 4 de grado medio, además el servicio con menor número de vulnerabilidades es el Catálogo en Línea, con una sola detección de grado alto, con la aplicación de las salvaguardas a las vulnerabilidades, el servicio de *Academics*, *Moodle*, Catálogo en línea y Mesa de Ayuda, poseen una reducción del 100% de las detecciones de grado alto, mientras que el Repositorio Digital tiene una reducción del 1% de las de grado alto, esto se debe a que el 99% de las detecciones son relacionadas a problemas de programación.

6.2 Recomendaciones

Tener presente el modelo propuesto, para cualquier servicio web que se ponga en producción, con la intención de ser un soporte para el análisis de vulnerabilidades que conduzca hacia un funcionamiento sin riesgos del servicio implementado.

Para servicios que no sean desarrollados, se realicen análisis de vulnerabilidades conjuntamente con el proveedor para que; en caso de existir, se realice las correcciones necesarias por el propio proveedor hasta que éstos sean mitigados y no representen riesgo de la información institucional.

Analizar las vulnerabilidades en los servicios web luego de una actualización de seguridad, despliegue de un nuevo módulo y si el servicio no presenta modificaciones se recomienda el análisis cada 3 meses para asegurar que las salvaguardas implementadas cumplan su función.

Apéndice A

Modelo de entrevista para medir el nivel de seguridad de los activos informáticos de la PUCE Ambato.

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

AMBATO

MAESTRÍA EN GERENCIA INFORMÁTICA

TEMA: Modelo para la mitigación de vulnerabilidades informáticas en los servicios web de la Pontificia Universidad Católica del Ecuador Ambato

Elaborado por: Eduardo Remache.

Objetivo: El objetivo de la presente investigación es evidenciar el nivel de seguridad que poseen los servicios web de la PUCE Ambato.

Temario de preguntas:

¿Cuáles son los servicios web que se ofrecen?

¿Los servicios web son adquiridos o desarrollados?

¿Existe un proceso para analizar las vulnerabilidades web en los servicios adquiridos o desarrollados?

¿Quiénes son los clientes?

¿Alguna vez, sus clientes han intentado ingresar de manera fraudulenta a los servicios?

¿Son seguros los servicios web brindados?

¿Posee la Universidad equipos de seguridad perimetral?

¿Existe un profesional que controle de forma específica la seguridad en la empresa?

¿Se realiza un analiza de vulnerabilidades a los servicios web de forma regular?

¿Los aplicativos web se encuentran alojados localmente o en la nube?

¿Los activos informáticos se encuentran en sitios seguros?

¿Existe control de acceso a los activos?

¿Cuáles son los principales riesgos a los que están expuestos los activos?

¿La infraestructura tecnológica está protegida por un UPS?

¿En caso de sufrir cortes de energía eléctrica, la Universidad posee un generador?

¿La transferencia de energía del generador es automática o manual?

¿Ha presentado daños en equipos por fallos eléctricos?

¿Existe alguna plataforma de respaldo de información?

¿Los respaldos de información son locales o remotos?

¿En los servicios en la nube, se ha presentado indisponibilidad del servicio?

¿La seguridad que le da su proveedor de servicios en la nube, es el adecuado?

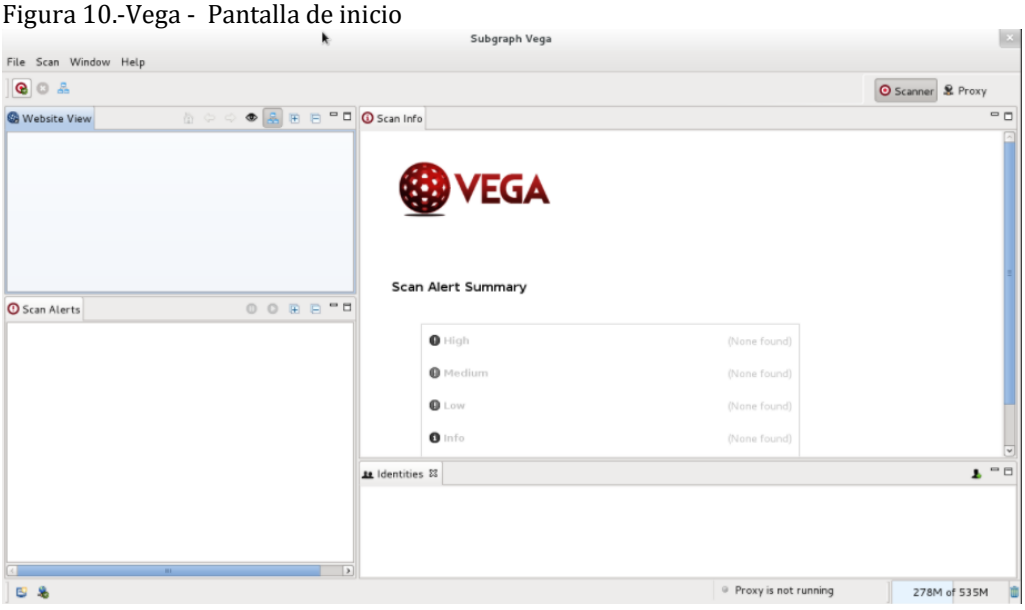
Apéndice B

Instalación de Vega *Subgraph*

A continuación, se muestra el procedimiento que se utilizó para instalar el programa de análisis de vulnerabilidades Vega *Subgraph* en *KaliLinux* 2017.3

1. En la consola de comandos, instalar el paquete lib*web*kitgtk como prerrequisito. *sudo apt-get install libwebkitgtk-1.0.*
2. Descargar el programa del sitio oficial de Vega *Subgraph*, https://subgraph.com/vega/download/index.en.html.
3. Desempaquetar el archivo descargado en el directorio /var/Vega.
4. Cambiarse al directorio /var/Vega e iniciar el aplicativo con el comendo./Vega.
5. El programa queda listo para iniciar el análisis de vulnerabilidades como se indica en la figura siguiente.

Figura 10.-Vega - Pantalla de inicio



Fuente: tomado de (Subgraph, 2017)

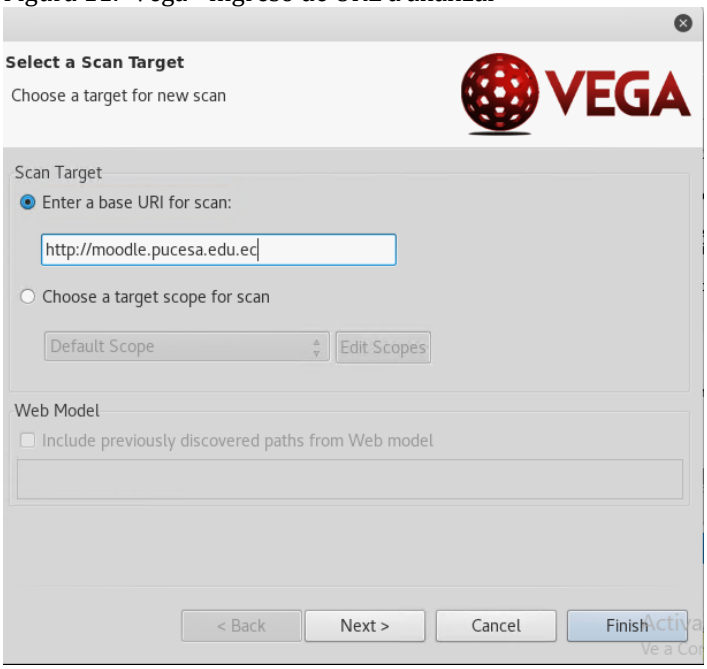
Apéndice C

Análisis de vulnerabilidades con Vega *Subgraph*

A continuación se describe el proceso para el análisis de vulnerabilidades en los servicios *web* de la PUCE Ambato.

1. En la ventana de inicio, seleccionar *Scan/Start New Scan* se muestra la ventana para ingresar la dirección *web* a analizar, como muestra la figura siguiente.

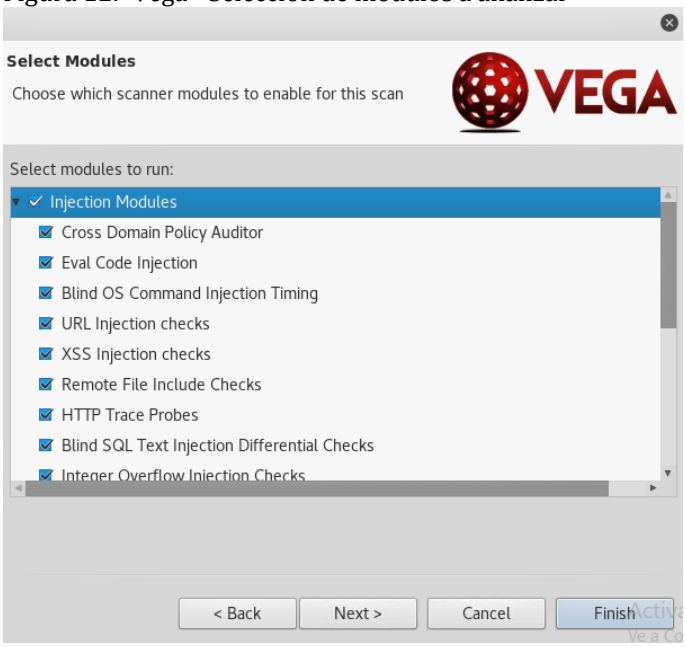
Figura 11.- Vega - Ingreso de URL a analizar



Fuente: tomado de (Subgraph, 2017)

2. En la siguiente ventana, permite seleccionar los módulos que se van a analizar para mejor resultado, como muestra la figura siguiente.

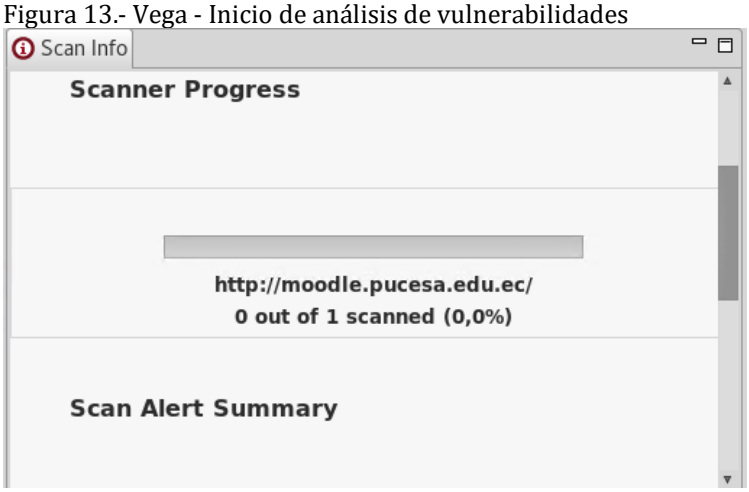
Figura 12.- Vega - Selección de módulos a analizar



Fuente: tomado de (Subgraph, 2017)

3. Al finalizar, Vega inicia el proceso de análisis de vulnerabilidades como se muestra en la figura siguiente.

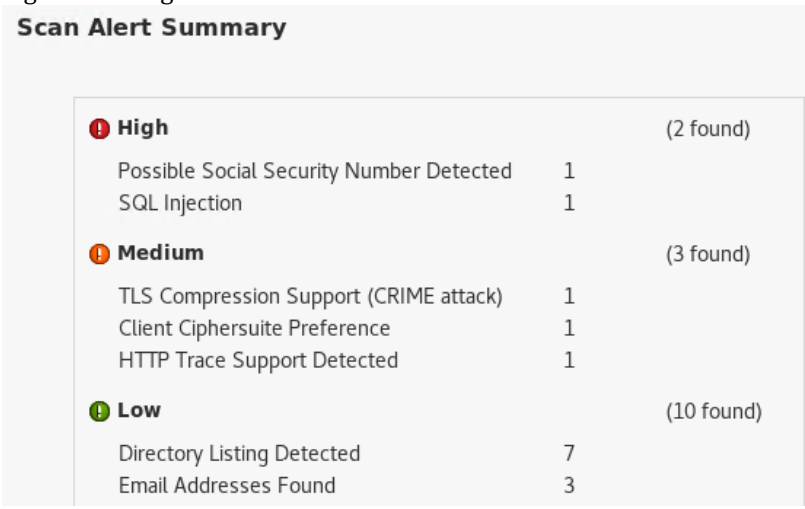
Figura 13.- Vega - Inicio de análisis de vulnerabilidades



Fuente: tomado de (Subgraph, 2017)

4. Una vez que se completó, se muestra los resultados del análisis, como se indica en la figura a continuación.

Figura 14.- Vega - Resultado de análisis de vulnerabilidades



Fuente: tomado de (Subgraph, 2017)

Referencias

Abril, A., Pulido, J., & Bohada, J. (2014). Análisis de Riesgos en Seguridad de la Información. *Ciencia, Innovación y Tecnología*, *1*(0), 39–53.

Acunetix. (2016). Web Application Vulnerability Report.

Alemán, H., & Rodríguez, C. (2015). Metodologías para el análisis de riesgos en los sgsi | Alemán y Rodriguez. Recuperado el 15 de agosto de 2017, de http://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1874

Alfsan. (2012). Arquitectura de n capas | Administracion de Base de Datos. Recuperado el 2 de agosto de 2017, de http://iutll-abdd.blogspot.com/2012/05/arquitectura-de-n-capas.html

Anderson, J. (1980). *Computer Security Threat Monitoring and Surveillance*. Recuperado de https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/ande80.pdf

Areitio, J. (2008). *Seguridad de la información. Redes, informática y sistemas de información*. Editorial Paraninfo.

Ávila, O. (2011). Computación en la nube. Recuperado de www.izt.uam.mx/newpage/contactos/anterior/n80ne/nube.pdf

Banco Interamericano de Desarrollo. (2016). Solo seis países en América Latina y el Caribe tienen estrategias contra los ciberataques. Recuperado el 13 de octubre de 2016, de http://www.efe.com/efe/america/sociedad/solo-seis-paises-en-america-latina-y-el-caribe-tienen-estrategias-contra-los-ciberataques/20000013-2868086#

Carrión García, A. (2006). El Modelo EFQM, mas allá del ISO 9.000. *REVISTA DE INFORMACIÓN BÁSICA*, *1*(1), 12–16.

Consejo Superior de Administración Electrónica de España. (2012). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Version 3. Libro 1- Metodo, Libro II Catalogo, Libro III Guia de técnicas. Recuperado de

https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WoZHdKjibIU

Cortés, M., & Iglesias, M. (2004). *Generalidades sobre Metodología de la Investigación.* (Primera). Mexico. Recuperado de http://www.unacar.mx/contenido/gaceta/ediciones/metodologia_investigacion.pdf

de Bustos Pérez, J. A. (2002). Seguridad y Software Libre. Recuperado de http://www.segu-info.com.ar

definicionabc.com. (2018). Definición de Amenaza » Concepto en Definición ABC. Recuperado el 6 de febrero de 2018, de https://www.definicionabc.com/general/amenaza.php

Definicion.de. (2018). Concepto de seguridad - Definición, Significado y Qué es. Recuperado el 17 de febrero de 2018, de https://definicion.de/seguridad/

Duque, B. (2010). Metodologías de Gestión de Riesgos. Recuperado de https://auditoriauc20102mivi.wikispaces.com/file/view/Metodolog%C3%ACas+deGesti%C3%B2n+de+Riesgos.pdf

Economiadigital. (2017). Mayores Ciberataques 2016. Recuperado el 9 de agosto de 2017, de http://www.economiadigital.es/tecnologia-y-tendencias/los-diez-mayores-ataques-informaticos-de-2016_188964_102.html

Erb, M. (2009). 6. Amenazas y Vulnerabilidades. Recuperado el 23 de agosto de 2017, de https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/

Forigua, S., & Ballesteros, O. (2006). RISK MANAGEMENT CAPABILITY. Recuperado el 15 de agosto de 2017, de http://scholar.googleusercontent.com/scholar?q=cache:hC6RcveCnvkJ:scholar.google.com/+metodologia+de+riesgo+coras&hl=es&lr=lang_es&as_sdt=0,5&as_vis=1

grupocontrol. (2010). Evolución de la Seguridad Informática. Recuperado el 17 de febrero de 2018, de https://www.grupocontrol.com/evolucion-de-la-seguridad-informatica

Haystax Technology. (2017). Insider Attacks Industry Survey. Recuperado el 23 de junio de 2017, de https://haystax.com/blog/ebook/insider-attacks-industry-survey/

Huerta, A. (2012). Introducción al análisis de riesgos – Metodologías (II). Recuperado el 15 de agosto de 2017, de https://www.securityartwork.es/2012/04/02/introduccion-al-analisis-de-riesgos-%e2%80%93-metodologias-ii/

Iteracy. (2017, enero 2). Browser statistics - Iteracy. Recuperado el 11 de julio de 2017, de https://www.iteracy.com/blog/post/browser-statistics

Kamlofsky, J., Colombo, H., Sliafertas, M., & Pedernera, J. (2015). Un Enfoque para Disminuir los Efectos de los Ciber-ataques a las Infraestructuras Críticas. *CONAIISI 2015: MEMORIAS DEL III CONGRESO NACIONAL DE INGENIERIA INFORMATICA / SISTEMAS DE INFORMACION. ISSN: 2346-9927*.

Lujan, S. (2002). Programación de aplicaciones web de Sergio Luján Mora - Editorial Club Universitario. Recuperado el 1 de agosto de 2017, de http://www.editorial-club-universitario.es/libro.asp?ref=367

Márquez Alcañiz, L., Rosado, D. G., Mellado, D., & Fernández-Medina Patón, E. (2014). *Hacia un proceso de migración de la seguridad de sistemas heredados al Cloud*. Universidad de Alicante. Recuperado de http://rua.ua.es/dspace/handle/10045/40427

Medina, J. (2014). Evaluación de Vulnerabilidades TIC. Laderas del Campillo (Murcia). Recuperado de https://ia802606.us.archive.org/28/items/pdfy-qulPxZjcFnnP61Nx/SG6-Javier-Medina-Evaluacion-de-Vulnerabilidades-TIC.pdf

Mieres, J. (2009). Buenas prácticas en seguridad informática. Recuperado el 8 de mayo de 2017, de https://www.welivesecurity.com/wp-content/uploads/2014/01/buenas_practicas_seguridad_informatica.pdf

Molina-Miranda, M. F. (2017). Análisis de riesgos de centro de datos basado en la herramienta pilar de Magerit. *Espirales revista multidisciplinaria de investigación*, *1*(11). Recuperado de http://www.revistaespirales.com/index.php/es/article/view/125

Oliveros, A., Danyans, F., & Mastropietro, M. (2014). Prácticas de Ingeniería de Requerimientos en el desarrollo de aplicaciones Web.

OWASP Fundación. (2013). *los 10 riesgos mas criticos en aplicaciones web*.

Pérez, L. (2014). Los 7 principales riesgos de TI para las organizaciones, de acuerdo con Zurich. Recuperado el 3 de mayo de 2017, de http://searchdatacenter.techtarget.com/es/cronica/Los-7-principales-riesgos-de-TI-para-las-organizaciones-de-acuerdo-con-Zurich

pmg-ssi.com. (2015). ISO 27001: Ciclo de Deming. Recuperado el 18 de febrero de 2018, de http://www.pmg-ssi.com/2015/06/iso-27001-ciclo-de-deming/

Prandini, P., & Pallero, M. (2013). Vulnerabilidades, amenazas y riesgo en "texto claro" | Magazcitum. Recuperado el 4 de mayo de 2017, de http://www.magazcitum.com.mx/?p=2193#.WQqZRMa23IV

Pressman, R. (2010). *Ingeniería del software, un enfoque practico* (Septima). University of Connecticut: The McGraw-Hill. Recuperado de http://artemisa.unicauca.edu.co/~cardila/Libro_Pressman_7.pdf

RED CEDIA. (2014). *RED CEDIA* (No. 1) (p. 12). Recuperado de http://csirt.cedia.org.ec/wp-content/uploads/2014/05/Informe-de-Resultados-2014.pdf

Salazar Carpió, K. E. (2013). Ethical Hacking for Web Application. *Revista de Información, Tecnología y Sociedad*, 57.

Sotelo, M., Torres, J., & Rivera, J. (2012). Un Proceso Práctico de Análisis de Riesgos de Activos de Información. Presentado en IV Congreso Internacional de Computación y Telecomunicaciones, Perú. Recuperado de http://www.comtel.pe/comtel2012/callforpaper2012/P26C.pdf

Subgraph. (2017). Vega Vulnerability Scanner. Recuperado el 22 de febrero de 2017, de https://subgraph.com/vega/index.fr.html

Sullivan, P. (2016). Gestión de riesgos de seguridad de la información: Comprensión de los componentes. Recuperado el 17 de agosto de 2017, de http://searchdatacenter.techtarget.com/es/consejo/Gestion-de-riesgos-de-seguridad-de-la-informacion-Comprension-de-los-componentes

Urrutia, J. A. (2014). Metodologias de Evaluacion de Riesgos Informaticos - UNAD 2014. Recuperado el 15 de agosto de 2017, de http://metodologia-y-evaluacion-de-riesgos.blogspot.com/

Vanegas, G. A., & Pardo, C. J. (2014). Hacia un modelo para la gestión de riesgos de TI en MiPyMEs:MOGRIT, *12*, 35–48.

Verizon Business RISK Team. (2008). 2008 Data Breach Investigations Report. Recuperado de http://www.verizonenterprise.com/resources/security/databreachreport.pdf

W3Techs. (2017, julio 15). Usage Statistics and Market Share of Web Servers for Websites, July 2017. Recuperado el 15 de julio de 2017, de https://w3techs.com/technologies/overview/web_server/all

www.efqm.es. (2018). EFQM.es: Modelo de excelencia y calidad EFQM. Recuperado el 14 de julio de 2017, de http://www.efqm.es/