ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

PROPUESTA DE IMPLEMENTACIÓN DE UN MODELO PARA LA REDUCCIÓN DE RIESGOS DE SEGURIDAD INFORMÁTICA EN SERVICIOS WEB DE LA ESPOCH

AUTORA: JESSICA NATALY CASTILLO FIALLOS

Proyecto de investigación, presentado ante el Instituto de Posgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado de MAGISTER EN SEGURIDAD TELEMÁTICA

RIOBAMBA-ECUADOR

2016

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

CERTIFICACIÓN:

El tribunal del PROYECTO DE INVESTIGACIÓN CERTIFICA QUE:

El proyecto de investigación titulado "PROPUESTA DE IMPLEMENTACIÓN DE UN MODELO PARA LA REDUCCIÓN DE RIESGOS DE SEGURIDAD INFORMÁTICA EN SERVICIOS WEB DE LA ESPOCH", de responsabilidad de la Ing. Jessica Nataly Castillo Fiallos ha sido prolijamente y se autoriza su presentación.

Tribunal:

Ing. Oscar Omar Espíndola Lara, M.Sc. **PRESIDENTE**	**FIRMA**
Ing. Andrés Santiago Cisneros Barahona, M.Sc. **DIRECTOR**	**FIRMA**
Ing. Edwin Vinicio Altamirano Santillán, M.Sc. **MIEMBRO DEL TRIBUNAL**	**FIRMA**
Ing. Alberto Leopoldo Arellano Aucancela, M.Sc. **MIEMBRO DEL TRIBUNAL**	**FIRMA**
DOCUMENTALISTA SISBIB ESPOCH	**FIRMA**

Riobamba, 2016

DERECHOS INTELECTUALES

Yo, Jessica Nataly Castillo Fiallos, con cédula de identidad 060459021-6 soy responsable de las ideas, doctrinas, resultados y propuestas expuestas en la presente investigación y los derechos de autoría pertenecen a la Escuela Superior Politécnica de Chimborazo.

0604590216

DECLARACIÓN DE AUTENTICIDAD

Yo, Jessica Nataly Castillo Fiallos, declaro que el presente Proyecto de Investigación, es de mi autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otra Fuente están debidamente citados y referenciados.

Como autor/a, asumo la responsabilidad legal y académica de los contenidos de este proyecto de investigación de maestría.

Riobamba, 2016

_____

Jessica Nataly Castillo Fiallos

060459021-6

DEDICATORIA

Dedico este trabajo a Dios, a mis padres Carmita Fiallos, César Castillo, por brindarme su apoyo y amor incondicional en cada uno de los desafíos que se han presentado en el trascurso de mi vida, a mis hermanas por estar siempre presentes cuando necesito unas palabras de aliento. Paulina, Erika y mi hermoso sobrino Rafhael.

Jessica

AGRADECIMIENTO

Agradezco a la Escuela Superior Politécnica de Chimborazo, Instituto de Posgrado, al Director de mi tesis Ing. Santiago Cisneros, por brindarme apoyo y compartir su profesionalismo, que me ha permitido alcanzar esta nueva meta.

Reconocimiento y gratitud al personal que labora en la DTIC, por brindarme su apoyo incondicional en el desarrollo del trabajo investigativo.

Jessica

ÍNDICE DE CONTENIDOS

INDICE DE TABLAS

INDICE DE GRÁFICOS

ÍNDICE DE ANEXOS

RESUMEN

Se implementó un Modelo para la Reducción de Riesgos de Seguridad Informática en Servicios Web de la Escuela Superior Politécnica de Chimborazo (ESPOCH). Para el desarrollo del Modelo se analizó la problemática y falencia interna, la vulnerabilidad que presentan actualmente, debido a defectos del software, al recurso humano de la Dirección de Tecnologías de Información y Comunicación (DTIC). Se compararon los valores del indicador número de vulnerabilidades y se aplicó la estadística inferencial para demostrar la hipótesis. La herramienta que se utilizó fue VEGA, la cual permitió escanear las vulnerabilidades web. Para lo que se identificaron los activos relevantes, amenazas, salvaguardas, se escanearon las Uniform Resource Locator (URLs) de los Servicios Web de la ESPOCH, impactos y se midió el nivel de riesgo. Se compararon los resultados obtenidos en base al número de vulnerabilidades, determinando que la implementación del modelo para la reducción de riesgos ayudo a reducir las vulnerabilidades encontradas, mitigando las mismas que se encontraron en el análisis preliminar de la investigación, las vulnerabilidades fueron: altas 416, medias 175 y bajas 1475, tres de las vulnerabilidades más frecuentes fueron: Structured Query Language (SQL) Injection, Hypertext Preprocessor (PHP) Error Detected y Directory Listing Detected. Resultado de la aplicación del modelo bajo la Plataforma VEGA fue de un 84% de reducción de vulnerabilidades. Se recomienda aplicar el Modelo propuesto cada trimestral en los diferentes Servicios Web.

Palabras clave: <RIESGOS DE SEGURIDAD INFORMÁTICA>, <SERVICIOS WEB>, <ESCANER DE VULNERABILIDADES> [Vega], <ATAQUE INFORMÁTICO SQL>, <ERROR DE SERVICOS WEB>, <ERROR DE DIRECTORIOS>

SUMMARY

The research Proposal Implementation of a Model for reduction of Computer Security Risks in Web Services ESPOCH held in Riobamba city. It helps to reduce security risks in Web Services of Escuela Superior Politécnica de Chimborazo. The scientific method was used because it uses steps to obtain knowledge and valid and reliable results. It was considered a problem and internal flaw the vulnerability that currently present due to software defects, human resource DTIC (Department of Information Technology and Communication). It did not meet the appropriate processes when modifying web services. Due to it did not keep constant and consistent training with the roles these factors have. The indicator values were compared number of vulnerabilities and inferential statistics was applied to test the hypothesis. The tool used was VEGA, which allowed scan web vulnerabilities For what the relevant assets, threats, safeguards were identified. URLs (Uniform Resource Locator) of the Web Services ESPOCH, impacts were scanned and the level of risk was measured. The results based on the number of vulnerabilities were compared, determining that the implementation of the model for risk reduction helped reduce vulnerabilities found. Also, it mitigated the same as found in the preliminary analysis of the research. The vulnerabilities were high 416, medium 175 and low 1475, three of the most common vulnerabilities were: SQL (Structured Query Language) Injection, PHP (Hypertext Preprocessor) Error Detected and Directory Listing Detected. It is recommended to apply Improvement Plan proposed to minimize the Risks.

Keywords: <COMPUTER SECURITY RISKS> <RIOBAMBA [City]> <WEB SERVICES>, <VEGA>, <SQL INJECTION [Computer Attack SOL]>, <PHP ERROR DETECTED [Error Web]>, <DIRECTORY LISTING DETECTED>[Error Directory]>

CAPÍTULO I

INTRODUCCIÓN

En la actualidad las tecnologías de la información son elementos fundamentales para la superación y desarrollo de un país, la información que en ellas se maneja es considerada un activo cada vez más valioso el cual puede hacer que una organización triunfe o quiebre, es por eso que debemos mejorar la seguridad de las mismas.

La mayoría de las empresas desconocen la magnitud del problema con el que se enfrentan considerando la seguridad como algo secundario y generalmente no se invierte el capital humano ni económico necesario para prevenir principalmente el daño y/o pérdida de la información que hoy en día con el uso de nueva tecnología para almacenarla, transmitirla y recobrarla está expuesta.

Las amenazas que afectan las características principales de la seguridad como son la confidencialidad, integridad y disponibilidad de la información pueden ser internas o externas, originadas accidentalmente o con un fin perverso dejando a la organización con problemas como por ejemplo la paralización de sus actividades que deja como resultado una perdida cuantiosa de tiempo de producción y dinero factores importantes para el desarrollo de una organización.

En vista que en la actualidad son muchos los riesgos que afectan la seguridad de las instituciones y por lo general el capital con el que se cuenta para protegerlas no es el suficiente debemos tener identificadas y controladas esas vulnerabilidades y esto se logra con un adecuado plan de seguridad elaborado en base a un análisis de riesgo previo.

Persiguiendo este objetivo que es la seguridad de la información, es que se presenta la Propuesta de implementación de un modelo para la reducción de riesgos de seguridad informática en servicios web de la ESPOCH que se desarrollará en los siguientes capítulos de este trabajo.

1.1. Problema de la investigación

1.2. Planteamiento del Problema

La gestión de seguridad referente a los riesgos en los sistemas web puede ser compleja debido al desconocimiento o falta de cultura con respecto a este tema.

Por lo que el principal problema es la falta de un estándar específico de seguridad informática para la gestión del riesgo que establezca reglas, normas, controles, políticas y procedimientos para los mismos, con el objetivo de analizar, prevenir, proteger o mitigar las posibles vulnerabilidades y su impacto en los servicios web, lo que representa una debilidad latente en su seguridad, integridad, disponibilidad de la información sensible que estos sistemas manejan, la cual podría ser utilizada por terceras personas sin la autorización de la Institución.

Un servicio web es una tecnología que utiliza un conjunto de protocolos y estándares que sirven para intercambiar datos entre aplicaciones, desarrollados en lenguajes de programación diferentes, y ejecutadas sobre cualquier plataforma. La interoperabilidad se consigue mediante la adopción de estándares abiertos. (**BRITO**, 2009, pág. 56).

El riesgo se refiere a la incertidumbre o probabilidad de que una amenaza se materialice utilizando la vulnerabilidad existente de un activo o grupo de activos, generando daños. (**ROYAL**, 2009, pág. 45).

La Gestión de Riesgo es un método para determinar, analizar, valorar y clasificar el riesgo, para posteriormente implementar mecanismos que permitan controlarlo. **(ROCHA, FONSECA, & REDONDO,** 2014, pág. 105).

En su forma general contiene cuatro fases:

- **Análisis:** Determina los componentes de un sistema que requiere protección, sus vulnerabilidades que lo debilitan y las amenazas que lo ponen en peligro, con el resultado de revelar su grado de riesgo.

- **Clasificación:** Determina si los riesgos encontrados y los riesgos restantes son aceptables.
- **Reducción:** Define e implementa las medidas de protección. Además sensibiliza y capacita los usuarios conforme a las medidas.
- **Control:** Analiza el funcionamiento, la efectividad y el cumplimiento de las medidas, para determinar y ajustar las medidas deficientes y sanciona el incumplimiento.

Actualmente se han realizado varias investigaciones previas acerca del tema en cuestión, entre ellos:

- La investigación "Information Security Risk Management in a World of Services" (**LALANNE, MUNIER, & GABILLON**, 2013, pág 23), trata acerca de las arquitecturas abstractas orientadas a Servicios (SOA), ya que ofrecen nuevas oportunidades para la interconexión de sistemas, sin embargo no es insignificante en términos de seguridad, ya que las nuevas tecnologías han introducido nuevas vulnerabilidades y por lo tanto nuevos riesgos informáticos.

- La investigación A Risk Management Methodology for Project Risk Dependencies, se fundamenta en que los riesgos no siempre son independientes ya que no existe una administración adecuada entre ellos.

- La investigación "Reflections on Web-Oriented Architectures for Risk Management" (**FUGINI, MAGGIOLINI, RAIBULET, & UBEZIO**, 2009, pág 15), menciona como se desarrollan los avances tecnológicos para la administración de riesgos en ambientes de trabajo.

Por lo que el enfoque original de la presente investigación que se diferencia de investigaciones anteriores es que se orienta a proponer un modelo adaptado a los servicios web, el cual permitirá reducir los riesgos existentes con la finalidad de mejorar la seguridad e integridad de la información.

1.2.1. Formulación del Problema

¿Cuál será el nivel de mejora al implementar un modelo de reducción de riesgos en la seguridad informática en los servicios web?

1.2.2. Sistematización del Problema

- ¿Qué metodologías de manejo de riesgos existen?
- ¿Cuáles son las ventajas y desventajas de las metodologías de manejo de riesgos existen?
- ¿Cuáles son los riesgos de seguridad existentes en los servicios web?
- ¿Cuáles son los servidores web con mayor riesgo?
- ¿Cómo reducir los riesgos informáticos en los servicios web?

1.3. Justificación de la Investigación

1.3.1. Justificación Teórica

Dado a que el riesgo es un problema potencial que puede ocurrir en un procesador segmentado aparecen los modelos de seguridad de riegos estos nos ayudan a disminuirlos para lo cual se analizara las ventajas de los modelos de seguridad informática existentes que permita controlar de mejor manera los riesgos mejorando su seguridad y vulnerabilidad.

La gestión de riesgos es un enfoque que nos permite manejar la probabilidad de que un riesgo sea una amenaza, utilizando diferentes políticas, normas, actividades que incluyan la evaluación de riesgo, estrategias para poder manejarlo y mitigarlo utilizando los recursos disponibles.

La metodología MAGERIT divide los activos de la organización en varios grupos, lo que permite identificar una mayor cantidad de riesgos y poder tomar medidas para evitar posibles inconvenientes. Esta metodología se relaciona directamente con el uso de las tecnologías de la información (Metodologías para el análisis de riesgos en Seguridad Informática (**DESONGLES**, 2009, pág. 57).

Los objetivos de la metodología de Magerit son:

Directos

- Concienciar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de atajarlos a tiempo.
- Ofrecer un método sistemático para analizar tales riesgos.
- Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.

Indirectos

- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

Los servicios web son una tecnología que utiliza protocolos y estándares para intercambiar información entre distintas aplicaciones desarrolladas en diferentes lenguajes de programación y ejecutadas en varias plataformas, estos servicios web permiten el apoyo al aprendizaje educativo en las instituciones.

El método original OCTAVE utiliza un enfoque de tres fases para examinar las cuestiones de organización y tecnología, el montaje de una visión global de las necesidades de seguridad de la información de la organización. Consiste en una serie de talleres, ya sea facilitado o llevado a cabo por un equipo de análisis interdisciplinario de tres a cinco de personal propio de la organización. El método aprovecha el conocimiento de múltiples niveles de la organización, centrándose en:

- Construcción de los Perfiles de Amenazas Basados en Activos
- Identificación de la Infraestructura de Vulnerabilidades
- Desarrollo de Planes y Estrategias de Seguridad

1.3.2. Justificación Metodológica

La principal ventaja en el manejo de riesgos es trabajar de manera oportuna para evitar que las vulnerabilidades en los servicios web se concreten.

Actualmente las metodologías más utilizadas para la gestión de riesgos de la seguridad informática son:

- **Metodología MAGERIT:** es un método formal que permite investigar e identificar los riesgos que soportan los sistemas informáticos, con la finalidad de contrarrestar y recomendar las medidas apropiadas que se deben adoptar para controlar los riesgos latentes.
- **Metodología OCTAVE:** Se fundamenta en el estudio del riesgo organizacional tomando en consideración tres aspectos importantes riesgo operativo, prácticas de seguridad y la tecnología permitiendo así conocer el manejo de los recursos, la identificación y evaluación de riesgos que afecten la seguridad del sistema informático de una organización.

1.3.3. Justificación Práctica

Luego de establecer el modelo de seguridad informática, las pruebas se realizaran en los servidores web con mayor riesgo de la Escuela Superior Politécnica de Chimborazo en dos escenarios, en el primero comprobando las vulnerabilidades existentes y en el segundo aplicando el modelo y comprobando ambos escenarios para determinar el nivel de riesgos.

1.4. Objetivos

1.4.1. General

- Elaborar un modelo para la reducción de riesgos de seguridad informática en los Servicios web de la Espoch.

1.4.2. Específicos

- Analizar las metodologías de gestión de riesgos de seguridad informática existentes para la selección de uno de ellos como base.
- Determinar los servicios web de mayor vulnerabilidad.
- Verificar el nivel de mejora al implementar el modelo de gestión de riesgos de seguridad informática seleccionado, en los servicios web.

1.5. Hipótesis

- La propuesta de un modelo de reducción de riesgos informáticos mejorará el nivel de seguridad en los servicios web de la Espoch.

1.6. Operacionalización Conceptual

Tabla 1-1 Operacionalización Conceptual

VARIABLE	TIPO	CONCEPTO
Modelo Propuesto de riesgos de la seguridad informática en servicios web	Independiente	Conjunto de normas de seguridad del modelo propuesto adaptado en base a normas existentes.
Nivel de Seguridad	Dependiente	Nivel de protección de la información contra riesgos en los servicios web.

Elaborado por: Castillo Jessica, 2016

1.7. Operacionalización Metodológica

Tabla 2-1 Operacionalización Metodológica

VARIABLE	INDICADOR	TÉCNICA	INSTRUMENTO
Modelo Propuesto de riesgos de la seguridad informática en servicios web	• Complejidad • Facilidad de Implementación • Tiempo de Implementación. • Recursos necesarios	Búsqueda de información. Pruebas Observación	Matrices de control de riesgos, Encuestas
Nivel de Seguridad	• Número de vulnerabilidades	Pruebas Observación Análisis	Matrices de control de riesgos Encuestas

Fuente: Escuela Superior Politécnica de Chimborazo
Elaborado por: Castillo Jessica, 2016

CAPITULO II

MARCO DE REFERENCIA

2.1. Elementos del riesgo

A la hora de dotar de seguridad a un sistema de información, hay que tener en cuenta todos los elementos que lo componen, analizar las amenazas que existen, el nivel de vulnerabilidad ante determinadas amenazas y valorar el impacto que un ataque causaría sobre todo el sistema. (**AGUILERA**, 2010, pág. 9)

En la figura siguiente se observa la aproximación metódica para determinar el riesgo y los elementos que actúan:

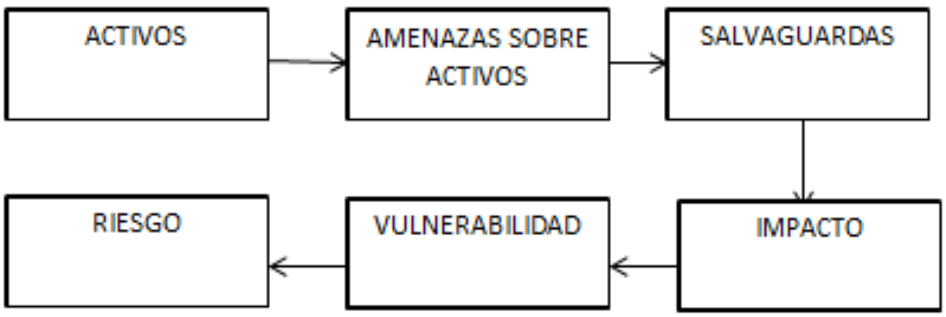


Gráfico 1-2 Aproximación metódica para determinar el riesgo

Fuente: Magerit
Elaborado por: Castillo Jessica, 2016

2.2. Activos

Son los recursos que pertenecen al propio sistema de información o que están relacionados con este. La presencia de los activos facilita el funcionamiento de la empresa u organización y la consecuencia de los objetivos. Al hacer un estudio de los activos existentes hay q tener en cuenta la relación que guardan entre ellos y la influencia que se ejerce, como afectaría en uno de ellos un daño ocurrido a otro. (**AGUILERA**, 2010, pág. 56).

Podemos clasifícalos en los siguientes tipos:

- Datos
- Software
- Hardware
- Redes
- Soportes
- Instalaciones
- Personal
- Servicio

2.3. Amenazas

Para empezar con la base de este capítulo se menciona el factor más importante que involucra el argumento "Reducción de riesgos informáticos", conceptualizando e incluyendo el contenido que conlleva al término amenaza.

Se inicia diciendo que una amenaza es considerada como una posibilidad de ocurrencia de cualquier tipo de evento que puede producir un daño sobre los elementos de un sistema. e información, las amenazas y por consecuentes daños que puede causar un evento de este tipo. Desde el punto de vista de la entidad que maneja los datos, existen amenazas de origen externo como por ejemplo las agresiones técnicas, naturales o humanos, sino también amenazas de origen interno, como la negligencia del propio personal o las condiciones técnicas, procesos operativos internos. Generalmente se distinguen y dividen en tres grupos: (**ERB**, 2014, www.protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/).

- **Criminalidad:** son todas las acciones, causado por la intervención humana, que violan la ley y que están penadas por esta. Con criminalidad política se entiende todas las acciones dirigido desde el gobierno hacia la sociedad civil.
- **Sucesos de origen físico:** son todos los eventos naturales y técnicos, sino también eventos indirectamente causados por la intervención humana.

Negligencia y decisiones institucionales: son todas las acciones, decisiones u omisiones por parte de las personas que tienen poder e influencia sobre el sistema. Al mismo tiempo son las amenazas menos predecibles porque están directamente

relacionado con el comportamiento humano. (**ERB**, 2014, www.protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/).

2.3.1. Origen común de las amenazas

Debido a que el uso de Internet se encuentra en aumento, cada vez más compañías permiten a sus socios y proveedores acceder a sus sistemas de información. Por lo tanto, es fundamental saber cuál podría ser el origen de las amenazas y qué recursos de la compañía necesitan protección para así controlar el acceso al sistema y los derechos de los usuarios del sistema de información. Los mismos procedimientos se aplican cuando se permite el acceso a la compañía a través de Internet. (CCMBenchmarck, 2015)

En la tabla siguiente se cita varios ejemplos del origen de las amenazas más comunes con los que podemos encontrarnos.

Tabla 3-2 Origen común de las amenazas

NOMBRE	ORIGEN DE LAS AMENAZAS	EJEMPLO
Herramientas de seguridad	Cualquier herramienta de seguridad representa un arma de doble filo: de la misma forma que un administrador las utiliza para detectar y solucionar fallos en sus sistemas o en la subred completa, un potencial intruso las puede utilizar para detectar esos mismos fallos y aprovecharlos para atacar los equipos.	• Nessus • Saint • Satan • Etc.
Puertas traseras	Durante el desarrollo de aplicaciones grandes o de sistemas operativos es habitual entre los programadores insertar "atajos" en los sistemas habituales de autenticación del programa o del núcleo que se está diseñando. A estos atajos se los denomina puertas traseras, y con ellos se consigue mayor velocidad a la hora de detectar y depurar fallos.	• Back Orifice • NetBus,-Computer Online Forensic Evidence Extractor (COFEE). • Etc.

Bombas lógicas	Las bombas lógicas son partes de código de ciertos programas que permanecen sin realizar ninguna función hasta que son activadas; en ese punto, la función que realizan no es la original del programa, sino que generalmente se trata de una acción perjudicial.	• Algunos ejemplos de acciones que puede realizar una bomba lógica • Borrar información del disco duro • Mostrar un mensaje • Reproducir una canción • Enviar un correo electrónico • Apagar el monitor • Abre tu Porta CD • Etc.
Virus	Es una secuencia de códigos que se inserta en un fichero ejecutable (denominado huésped), de forma que cuando el archivo se ejecuta, el virus también lo hace, insertándose a sí mismo en otros programas. Aunque los virus existentes para entornos Unix son más una curiosidad que una amenaza real, en sistemas sobre plataformas IBM-PC o compatibles (Linux, FreeBSD, NetBSD, Minix, Solaris.) ciertos virus, especialmente los de boot, pueden tener efectos nocivos, como dañar el sector de arranque.	• Fizzer, Zeus, etc.
Canales cubiertos	Los canales cubiertos (o canales ocultos) son canales de comunicación que permiten a un proceso transferir información de forma que viole la política de seguridad del sistema. No constituyen una amenaza demasiado habitual en redes de I+D, sin embargo, es posible su existencia, y en este caso su detección suele ser difícil.	• Multiplicación en tiempo. • Etc.
Gusano	Un gusano es un programa capaz de ejecutarse	Archivos que pueden ser

	y propagarse por sí mismo a través de redes, en ocasiones portando virus o aprovechando bugs de los sistemas a los que conecta para dañarlos.	de tipo: • exe, com, bat, pif, vbs, scr, doc, xls, msi, eml, etc.
Programas conejo o Bacterias	Son los programas que no hacen nada útil, sino que simplemente se dedican a reproducirse hasta que el número de copias acaba con los recursos del sistema produciendo una negación de servicio.	• memoria • procesador • disco, etc.),
Caballos de Troya	Los troyanos o caballos de Troya son instrucciones escondidas en un programa de forma que éste parezca realizar las tareas que un usuario espera de él, pero que realmente ejecute funciones ocultas, es decir que ocultan su función real bajo la apariencia de un programa inofensivo que a primera vista funciona correctamente.	• Backdoors • Keyloggers • Etc.
Técnicas salami	Por técnica salami se conoce al robo automatizado de pequeñas cantidades de bienes de una gran cantidad origen. El hecho de que la cantidad inicial sea grande y la robada pequeña hacen extremadamente difícil su detección.	• Dinero • Etc.
Catástrofes	Las catástrofes (naturales o artificiales) son la amenaza menos probable contra los entornos habituales.	• Terremotos • Inundaciones • Incendios , Etc.
Spyware	Son programas espías: Código malicioso cuyo objetivo principal es recoger información sobre las actividades de un usuario de un computador (tendencias de navegación), para permitir el despliegue sin autorización en ventanas emergentes de propaganda de mercado, o para robar información personal.	• Aureate/Radiate • BargainBuddy • ClickTillUWin • Conducent • Etc.

Spam	Recibo de mensajes no solicitados, principalmente por correo electrónico, cuyo propósito es difundir grandes cantidades de mensajes comerciales o propagandísticos. Se han presentado casos en los que los envíos se hacen a sistemas de telefonía celular.	• Mensajes comerciales • Mensajes de cadena • Etc.
Phishing	Es un ataque del tipo ingeniería social, cuyo objetivo principal es obtener de manera fraudulenta datos confidenciales de un usuario, aprovechando la confianza que este tiene en los servicios tecnológicos, el desconocimiento de la forma en que operan y la oferta de servicios en algunos casos con pobres medidas de seguridad.	• Excusas utilizadas para engañar al usuario • Mensajes privados • Etc.

Fuente: (**RUIZ**, 2012, dialnet.unirioja.es/descarga/articulo/3311853.pdf), (Amenazas Lógicas, 2013).
Elaborado por: Castillo Jessica, 2016

2.4. Salvaguardas

Una salvaguarda es un mecanismo de protección frente a las amenazas, reducen la frecuencia de las amenazas y limitan el daño causado por estas. Hay diferentes aspectos en los cuales puede actuar una salvaguarda para alcanzar sus objetivos de limitación del impacto y/o mitigación del riesgo.

Se requieren procedimientos tanto para la operación de las salvaguardas preventivas como para la gestión de incidencias y la recuperación tras las mismas, como la política de personal, que es necesaria cuando se consideran sistemas atendidos por personal. La política de personal debe cubrir desde las fases de especificación del puesto de trabajo y selección, hasta la formación continua. Soluciones técnicas, frecuentes en el entorno de las tecnologías de la información, que pueden ser (**REYES**, 2015, pág. 78):

- Aplicaciones (software)
- Dispositivos físicos
- Protección de las comunicaciones

- Seguridad física, de los locales y áreas de trabajo

2.5. Impacto

Es el daño sobre el activo causado por la amenaza, conociendo el valor de los activos sería muy sencillo calcular el valor del impacto. El Impacto en un Activo es la consecuencia sobre éste de la materialización de una Amenaza en agresión, consecuencia que puede desbordar ampliamente el Dominio y requerir la medida del daño producido a la organización. Es la diferencia en las estimaciones del estado de seguridad del Activo obtenidas antes y después del evento de agresión. (**REYES**, 2015, pág. 34)

2.6. Vulnerabilidades

La Vulnerabilidad es la capacidad, las condiciones y características del sistema mismo (incluyendo la entidad que lo maneja), que lo hace susceptible a amenazas, con el resultado de sufrir algún daño. En otras palabras, es la capacitad y posibilidad de un sistema de responder o reaccionar a una amenaza o de recuperarse de algún daño.

Las vulnerabilidades están directamente interrelacionadas con las amenazas porque si no existe una amenaza, tampoco existe la vulnerabilidad o no tiene importancia, porque no se puede ocasionar un daño. Dependiendo del contexto de la institución, se puede agrupar las vulnerabilidades en grupos característicos: Ambiental, Física, Económica, Social, Educativo, Institucional y Política. (**GESTIÓN DE RIESGO EN LA SEGURIDAD INFORMÁTICA**, 2014, https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/)

2.7. Riesgo

Se denomina riesgo a la posibilidad de que se materialice o no una amenaza aprovechando una vulnerabilidad. No constituye riesgo una amenaza cuando no hay vulnerabilidad ni una vulnerabilidad cuando no existe amenaza para la misma. (**AGUILERA**, Informática y comunicaciones, 2010, pág. 45)

Ante un determinado riesgo una organización puede optar por tres alternativas distintas:

- Asumirlo sin hacer nada. Esto solamente resulta lógico cuando el perjuicio esperado no tiene valor alguno o cuando el coste de aplicación de medidas superaría de la recuperación del daño.
- Aplicar medidas para disminuirlos o anularlos.
- Transferirlo (por ejemplo, contratando un seguro).

2.8. Metodologías de Reducción de Riesgos

A continuación se Identifica dos de las más importantes metodologías en cuanto al análisis de riesgos y vulnerabilidades en una Organización, como lo son Octave y Magert.

Estas son las dos más utilizadas a Nivel mundial, una porque es en español ya que fue desarrollada por el Consejo Superior de Administración Electrónica que hace parte del Ministerio de Administraciones Publicas de España y la otra porque es muy resumida en cuanto a la identificación de los activos de la Organización y no los clasifica demasiado, estamos hablando de Magerit y Octave respectivamente. (**MENDOZA**, 2011, https://seguridadenlasredes.wordpress.com/2010/08/12/metodologias-de-analisis-de-riesgos-magerit-y-octave/)

2.8.1. Características de las Metodologías

Se entiende como la descripción, el análisis y la valoración de los métodos de investigación. También se puede decir que guía, orienta la investigación así como también fija las normas de los métodos de la investigación y sus características principales son:

- **Práctica**: Se realizan ejercicios prácticos (individuales y en equipos) que conectan la teoría con aquello que será útil y aplicable.
- **Participativa:** Se utilizan técnicas para propiciar que el equipo construya su propio aprendizaje de forma activa.
- **Adaptada**: Se flexibilizan y ajustan los contenidos y metodología a las características, inquietudes, y necesidades reales del grupo.

- **Motivadora**: Se integra la experiencia del grupo participante. Se trabajan los objetivos de cada taller de forma lúdica y didáctica.
- **Integral**: Se potencian las competencias integrando el "saber" (conceptos, información, teoría), "querer" (motivación, actitudes y aspectos emocionales) y "poder" (habilidades y recursos personales).
- **Vivencial**: Se dirige al grupo y a la persona en todas sus dimensiones, interrelacionando cuerpo, emoción, razón, acción y contexto. Se aprende desde experiencias. (**SAENZ**, 2009, http://neurorganizaciones.blogspot.com/2009/01/caractersticas-principales-prctica-se.html)

2.9. MAGERIT

En la actualidad se está implementando las TIC's que son Tecnologías de la Información y la Comunicación. Las TIC´s introducen nuevas tecnologías y mucha seguridad en los procesos, pero la aplicación de las tecnologías supone que aparte de todos estos beneficios surjan aspectos no deseados que han de ser regulados y este es el fin de MAGERIT (**TELEFONICA**, 2008, pág. 180).

Magerit se esfuerza por enfatizarse en dividir los activos de la organización en variados grupos, para identificar más riesgos y poder tomar contramedidas para evitar así cualquier inconveniente.

La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de las tecnologías de la información, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza (**MOLINER**, 2005, pág. 80).

2.9.1. Definición

"Es un método formal para investigar los riesgos que soportan los Sistemas de Información, y para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos". (**DESONGLES**, 2005, pág. 195)

Magerit es un método para reducir riesgos que fue Elaborado por un equipo interdisciplinar del Comité Técnico de Seguridad de los Sistemas de Información y tratamiento Automatizado de Datos Personales, SSITAD. Magerit toma como referencia:

- Los criterios de ITSEC (Information Technologies Security Evaluation Criteria).
- Los criterios Comunes de Evaluación de la Seguridad de los Productos Y sistemas de Información.

2.9.2. Objetivos de MAGERIT

"Estudiar los riesgos que soportan un sistema de información y el entorno asociado a él". (**DESONGLES**, 2005, pág. 195)

Magerit propone la realización de un análisis de los riesgos que implica la evaluación del impacto que una violación de la seguridad tiene en la organización:

- Señala los riesgos existentes, identificando las amenazas que asechan al sistema de información.
- Determina la vulnerabilidad del sistema de prevención de dichas amenazas, generando resultados.

"Los resultados del análisis de riesgos permiten a la gestión de riesgos recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo se potencial o sus posibles perjuicios." (**DESONGLES**, 2005, pág. 195).

MAGERIT ofrece un método sistemático para analizar tales riesgos, también ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control, preparando a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

La aplicación de MAGERIT permite:

- Aportar racionalmente en el conocimiento del estado de seguridad de los Sistemas de Información y en la introducción de medidas de seguridad.
- Ayudar a garantizar una adecuada cobertura en extensión, de forma que no haya elementos del Sistema de información que queden fuera del análisis, y en intensidad, de forma que se alcance la profundidad necesaria en el análisis del sistema.
- Asegurar el desarrollo de cualquier tipo de sistemas, reformados o nuevos, en todas las fases desde la planificación hasta la implementación y mantenimiento.

2.10. OCTAVE

Una evaluación efectiva de riesgos en la seguridad de la información considera tanto los temas organizacionales como los técnicos, examina cómo la gente emplea la infraestructura en forma diaria. La evaluación es de vital importancia para cualquier iniciativa de mejora en seguridad, porque genera una visión a lo ancho de la organización de los riesgos de seguridad de la información, proveyéndonos de una base para mejorar a partir de allí. Para que una empresa comprenda cuáles son las necesidades de seguridad de la información, OCTAVE es una técnica de planificación y consulto ría estratégica en seguridad basada en el riesgo. (**DUQUE**, 2010, pág. 5).

2.10.1. Definición

OCTAVE es un modelo para la creación de metodologías de análisis de riesgos desarrolladas por la Universidad de Carnegie Mellon. El núcleo central de OCTAVE es un conjunto de criterios a partir de los cuales se pueden desarrollar diversas metodologías. (**CRAMMM**, 2011 , https://www.clubensayos.com/Tecnolog%C3%ADa/OCTAVE-VRS-CRAMM-APOYO-ISO-270001/11555.html)

Es una metodología que desde un punto de vista organizativo y técnico analiza los riesgos y propone un plan de mitigación. Cualquier metodología que aplique los criterios puede considerarse compatible con el modelo OCTAVE.

2.10.2. Objetivos de OCTAVE

OCATVE es un método auto-dirigida, flexible y evolucionado. Este método se puede adaptar al entorno de la organización única de riesgos, los objetivos de seguridad y resistencia, y el nivel de habilidad. OCTAVE mueve una organización hacia una visión basada en el riesgo operativo de seguridad y tecnología de direcciones en un contexto empresarial.

- Desarrollar criterios de medición de riesgo acordes con la misión de la organización, los objetivos de la meta, y los factores críticos de éxito.
- Crear un perfil de cada activo de información crítica que establece límites claros para el activo, identifica sus necesidades de seguridad, e identifica todos sus envases.
- Identificar las amenazas a cada activo de información en el contexto de sus contenedores.
- Identificar y analizar los riesgos para los activos de información y empezar a desarrollar enfoques de mitigación.

El método OCTAVE es un enfoque utilizado para evaluar las necesidades de seguridad de la información de una organización. (**PEREZ**, 2013, http://www.cert.org/resilience/products-services/octave/).

La aplicación de OCTAVE permite:

- Ayudar a garantizar una adecuada cobertura en extensión, de forma que no haya elementos del Sistema de información que queden fuera del análisis, y en intensidad, de forma que se alcance la profundidad necesaria en el análisis del sistema.

2.11. Servicios Web

"Los servicios web son aplicaciones que utilizan protocolos estándares de comunicación y registro para conectarse con otras de manera dinámica, utilizan un formato estándar como XML o una de sus variantes para presentar información y datos, un registro para

encontrar servicios ofrecidos por otras aplicaciones, negocian como recibir y enviar información (WSDL), y se adhieren a protocolos de comunicación (SOAP) para enviar la información por internet (HTTP)". (**GARCIA**, 2003, pág. 26)

Se dice que los servicios web son tecnologías que utilizan un conjunto de protocolos estándares que sirven para intercambiar la información entre las diferentes aplicaciones. Es decir que un servicio web es un componente de un software y es la considerada la manera más confiable para intercambiar información entre softwares.

2.11.1. Beneficios de los servicios Web

- **Promueven la interoperabilidad:** La interacción entre un proveedor y un solicitante de servicio está diseñada para que sea completamente independiente de la plataforma y el lenguaje. Esta interacción requiere un documento WSDL para definir la interfaz y describir el servicio, junto con un protocolo de red (generalmente HTTP).

- **Permiten la integración "justo-a-tiempo":** El proceso de descubrimiento se ejecuta dinámicamente, a medida que los solicitantes de servicio utilizan a los agentes para encontrar proveedores de servicio. Una vez el solicitante y el proveedor de servicio se han ubicado, se utiliza el documento WSDL del proveedor para enlazar al solicitante con el servicio. Esto significa que los solicitantes, los proveedores y los agentes actúan en conjunto para crear sistemas que son auto-configurables, adaptativos y robustos.

- **Reducen la complejidad por medio del encapsulamiento**: Los solicitantes y los proveedores del servicio se preocupan por las interfaces necesarias para interactuar. Como resultado, un solicitante de servicio no sabe cómo fue implementado el servicio por parte del proveedor, y éste a su vez, no sabe cómo utiliza el cliente el servicio. Estos detalles se encapsulan en los solicitantes y proveedores. El encapsulamiento es crucial para reducir la complejidad.

- **Dan una "nueva vida" a las aplicaciones de legado**: Es relativamente correcto tomar una aplicación, generar un wrapper SOAP, luego generar un documento WSDL para moldear la aplicación como un servicio web.
- **Abren la puerta a nuevas oportunidades de negocio**: Los servicios web facilitan la interacción con socios de negocios, al poder compartir servicios internos con un alto grado de integración.
- **Disminuyen el tiempo de desarrollo de las aplicaciones:** Pues gracias a la filosofía de orientación a objetos utilizada, el desarrollo se convierte más bien en una labor de composición. (**SERVICIOS WEB**, 2014, http://www.eumed.net/tesis-doctorales/2007/cavl/Beneficios%20de%20los%20servicios%20Web.htm)

2.12. Trabajos Relacionados

A continuación se resumen los trabajos realizados previamente sobre temas relacionados con análisis de riesgos:

- La investigación científica "Risk analysis in information systems: A fuzzification of the MAGERIT methodology" (**VICENTE & JIMENEZ**, 2014), trata acerca de que se han desarrollado varios métodos basados en la norma ISO 27000 norma internacional / IEC para lidiar con el análisis de riesgos en los sistemas de información (SI). Proponen una extensión de la metodología MAGERIT basado en modelos computacionales difusos clásicos. Una escala lingüística término se utiliza para representar los valores de activos, sus dependencias, frecuencia y la degradación de los activos asociados a las amenazas.

- La investigación científica "Aplicación de la metodología Magerit para el análisis y gestión de riesgos de la seguridad de la información aplicado a la empresa Pesquera e Industrial Bravito S.A. en la ciudad de Machala" (**VÁSQUEZ**, 2013, pág. 12), trata de la seguridad de la información en cada uno de los activos que componen la empresa "Pesquera e Industrial Bravito S.A." para ello contamos con la Magerit versión 3 Metodología y la herramienta PILAR 5.2.9 que ayudan a medir el riesgo de la situación actual de la empresa y como mitigación para alcanzar niveles aceptables de riesgo.

- La investigación científica "Comparison of Risk Analysis Methods: Mehari, Magerit, NIST800-30 and Microsoft's Security Management Guide" (**KUSHU**, **HORI**, **& SAKUIRA**, 2009, pág. 726), trata acerca de la comparación de cuatro métodos de análisis de riesgos: Mehari, Magerit, NIST800-30 y la Guía de Gestión de Seguridad de Microsoft. Mehari es un método para el análisis y gestión de riesgos. Magerit es un análisis de riesgos y metodología de gestión de sistemas de información. NIST 800-30 es una guía de gestión de riesgos para los sistemas de tecnología de la información. La seguridad es una guía de gestión de riesgos de seguridad desarrollado por Microsoft.

- La investigación científica "A Web-Service Architectural Perspective on Risk Manager in Work Environments" (**FUGINI, RAINULE, & UBEZIO,** 2010, pág. 327), trata acerca de los servicios web basados en una arquitectura SOA que permite identificar y resolver situaciones de riesgo que se presentan en ambientes de trabajo. La metodología y avances computacionales en el mundo IT, proveen un aporte significativo al manejo de riesgo e implícitamente la reducción de los accidentes en los ambientes de trabajo.

- La investigación "Desarrollo de una Metodología para la auditoría de riesgos informáticos (físicos y lógicos) y su aplicación al departamento de informática de la dirección provincial de ´pichincha del consejo de la judicatura". **(PAREDES & VEGA,** 2012, pág. 56**)** Define una metodología para la auditoría de riesgos informáticos con el objetivo de evaluar la eficacia y eficiencia que presenta el Departamento de Informática de la Dirección Provincial del Consejo de la Judicatura de la Provincia de Pichincha. Para la elaboración de la metodología, se realizó un análisis previo de las metodologías ITIL, COBIT, ISO 17799, CRMR y MARGERIT.
- La investigación científica "Reflections on Web-Oriented Architectures for Risk Management" (**FUGINI & MAGIONNILI,** 2009, pág. 361), trata acerca del avance tecnológico para la administración de riesgos en ambientes de trabajo. En el trabajo de investigación se analiza los diferentes tipos heterogéneos que deben ser considerados, por ejemplo en el ámbito tecnológico y social, en este contexto la idea principal es orientar las arquitecturas a la web para enfrentar las emergencias

y situaciones de riesgo en los lugares de trabajo. Se analiza un modelo basado en la arquitectura de tecnologías web que incluye servicios que mejoran la seguridad en los ambientes de trabajo y se discuten varios problemas tecnológicos, sociales y sus propuestas de solución.

- La investigación científica "A Risk Management Methodology for Project Risk Dependencies" (**LEUNG & HARETON,** 2011, pág. 324), trata acerca de los riesgos no siempre son independientes ya que no existe una administración clara entre ellos. Las dependencias pueden ser identificadas de forma explícita y analizadas, los administradores del proyecto deben ser capaces de planificar estrategias efectivas contra los riesgos con la finalidad de tomar decisiones. La presente investigación propone una metodología de gestión de riesgos para que los proyectos los administren.

CAPITULO III

DISEÑO DE INVESTIGACIÓN

La presente investigación se fundamentó con relación a los objetivos planteados fue orientada a través de un enfoque cualitativo para desarrollar la propuesta de implementación de un modelo para la reducción de riesgos de seguridad informática en servicios web de la Escuela Superior Politécnica de Chimborazo.

Para el desarrollo de este trabajo se utilizó la investigación documental y de campo.

3.1. Investigación Documental

"La investigación documental aplicada a la organización de empresas como una técnica de investigación en la que se deben seleccionar y analizar aquellos escritos que contienen datos de interés relacionados con el estudio" (**BARAY**, 2009, pág. 23) .

Se compiló la información del modelo elegido, que sirvió para la fundamentación científica del proyecto y la construcción de la propuesta.

3.1.1. Investigación de Campo

"Análisis sistemático de problemas en la realidad, con el propósito bien sea de describirlos, interpretarlos, entender su naturaleza y factores constituyentes, explicar sus causas y efectos, o predecir su ocurrencia, haciendo uso de métodos característicos de cualquiera de los paradigmas o enfoques de investigación conocidos o en desarrollo" (**BERNAL**, 2009, pág. 45).

Los datos de interés fueron recopilados y organizados, el procesamiento de la información, el análisis de los resultados y la obtención de conclusiones que confirman el diagnóstico de las necesidades sobre el problema de estudio.

3.2. Tipo de investigación

Descriptiva: Después de haber realizado la exploración e interpretación de la información recogida, de manera sintética se describió algunas irregularidades dentro de la investigación.

Explicativa: Luego de haber concluido con el trabajo sistematizado, se procedió a explicar las causas que están provocando estas irregularidades.

Después de haber realizado la investigación cualitativa se espera que con los datos copilados se obtenga una comprensión global del problema y sus causas.

3.3. Métodos de investigación

Este estudio se realizó a través de la aplicación del método deductivo, método inductivo y el método cuasi experimental

El método deductivo, pues se hizo necesario partir del conocimiento de las distintas teorías para obtener conclusiones particulares.

El método Inductivo, porque su análisis se hizo posible mediante un proceso que parte de un estudio particular a lo general específicamente de hechos singulares para llegar a principios generales.

El método cuasi experimental ya se tiene una ‘exposición’, una ‘respuesta’ y una hipótesis para contrastar, pero no hay aleatorización de los sujetos a los grupos de tratamiento y control.

3.4. Técnicas e instrumentos de recolección de datos.

La investigación requirió de técnicas como las documentales bibliográficas, entrevistas al administrador de DTIC, pruebas y análisis con la Plataforma VEGA.

VEGA es un escáner de código y pruebas de plataforma libre y abierta para probar la seguridad de las aplicaciones web. Vega puede ayudarle a encontrar y validar la inyección de SQL, Cross-Site Scripting (XSS), inadvertidamente revelado información sensible, y otras vulnerabilidades. Está escrito en Java, basado en GUI, y se ejecuta en Linux, OS X y Windows. (**VEGA**, 2015, https://subgraph.com/vega/)

La técnica de campo plasmadas en Entrevistas y la utilización de la plataforma VEGA de Linux que se sustentaron en guías de entrevistas previamente establecidos; las mismas que fueron aplicadas al administrador de DTIC y a los Servicios Web de la Plataforma de La Escuela Superior Politécnica de Chimborazo los cuales son:

- Escuela de Postgrado y Educación continúa
- Infraestructura de Datos Espaciales
- OASIS
- Evaluación Institucional
- Talento Humano
- Educación Virtual
- Biblioteca
- Médico
- Bienestar Politécnico
- Herbario
- Consulta del Estado de Matricula
- Bolsa de empleo
- Passport

3.4.1. Información primaria

Entrevista.- Esta técnica se realizó con el fin de conseguir información del entrevistado, por parte del investigador. Se entrevistó al administrador de DTIC de la Escuela Superior Politécnica de Chimborazo con el fin de determinar y priorizar las necesidades más urgentes.

Encuesta.- La encuesta es una técnica que permite obtener un mayor volumen de información que la entrevista.

De la misma forma se procedo a realizar la encuesta al administrador de DTIC para constatar las diversas amenazas que se presentan en los Servidores que prestan servicios Web.

Pruebas.- Las pruebas realizadas a los Servicios Web que presta la Escuela Superior Politécnica de Chimborazo fueron para medir el número de vulnerabilidades que se presentan en los diferentes servicios web con la utilización de la Plataforma VEGA de Linux.

En la investigación "Estudo e Analise de Vulnerabilidades Web "(**MONTEVERDE & CAMPIOLO**, 2014, pág. 45), se trata de que la seguridad web es importante para proporcionar protección a los clientes y a los servicios web. Múltiples vulnerabilidades web son explotados todos los días y los ataques tienen aumentado debido a las nuevas herramientas y aplicaciones web. En este trabajo se lleva a cabo un análisis de vulnerabilidades Web en diferentes tipos de aplicaciones con la herramienta de escáner VEGA. Un conjunto de Sitios Web heterogéneos y brasileños fueron seleccionados y analizados. En consecuencia, las principales formas de ataques utilizados en aplicaciones web se han investigado. Nuestros resultados muestran cómo las vulnerabilidades web pueden ser explotadas fácilmente. Así, se verifica que los sitios web deben mejorar su seguridad con urgencia.

3.5. Población y muestra

3.5.1. Población

La población considerada para esta investigación son los Servicios Web de la Espoch, la misma que no es extensa, entonces para el desarrollo del tema la muestra va a ser igual a la población.

N=13 Servicios Web

3.6. Gestión de riesgos

En la actualidad toda organización se encuentra expuesta a riesgos, cabe recalcar que no existe un ambiente 100% seguro y la aparición de riesgos es constante. Por tal motivo toda organización deberá estar alerta a cualquier cambio o situación extraña que considere que podría afectar a un activo o a toda la organización, utilizando una metodología de Reducción de riesgos para lo cual se tomado como referencia un análisis de las Empresas Ecuatorianos que utilizan Magerit como metodología para reducir los riesgos informáticos.

Tabla 4-3 Empresas que utilizan MAGERIT/OCTAVE

MAGERIT VS OCTAVE	
MAGERIT	**OCTAVE**
• Empresa Textil Fabril Fame SA., diseña, fabrica y comercializa vestuario, calzado y equipos de camping, opera en Sangolqui – Quito. • Escuela Politécnica del Ejército ubicada en Quito. • Empresa Eléctrica Regional Norte S.A. EMELNORTE, encargada de generar, distribuir y comercializar energía eléctrica, Prov. Imbabura. • Empresa Pezquera e Industrial Bravito S.A., la camaronera está opera en la Ciudad de Machala. • A&CGroup es una empresa de servicios de auditoría financiera que opera en Ecuador con oficinas en Guayaquil y Quito. • Banco de Guayaquil brinda servicios financieros la matriz se encuentra en Guayaquil. • Banco de Loja brinda servicios financieros la matriz se encuentra en la provincia de Loja. • Municipalidad de Guayaquil	• MANPOWER, brinda servicios de colocación de personal está ubicada en Quito. • Empresa Pirámide Digital CIA. Ltda., capacitación de personal, ubicada en provincia de pichincha.

Fuente: (**BURNEO**, 2013, pág. 23), (**FUENTES**, 2011, pág. 12), (**BARRAGAN**, 2013, pág. 2).
Elaborado por: Castillo Jessica, 2016

A continuación se selecciona la metodología que cumple con los parámetros previstos para el desarrollo de la investigación.

3.7. Selección de la Metodología

Para elegir la metodología que se va a usar en el presente trabajo se tomaron en cuenta los siguientes criterios: Idioma, cubre todas las etapas de un análisis de riesgo, utilización de la metodología a nivel mundial, documentación disponible, aplicación en Ecuador, se calificó de 1 a 5 siendo 1 el puntaje más bajo y 5 el más alto.

Tabla 5-3 Parámetros de Valoración

Metodología	Idioma	Cubre todas las etapas de un análisis de riesgo	Documentación Disponible	Aplicación en Ecuador
MAGERIT	4	5	5	4
OCTAVE	2	4	2	2

Fuente: Seguridad en equipos informáticos. IFCT0510, Autor José Francisco Giménez Albacete
Elaborado por: Castillo Jessica, 2016

3.8. Metodología Seleccionada

Como se observa en la tabla anterior se mide las dos metodologías por los criterios más relevantes, la metodología escogida para la presente investigación es MAGERIT ya que es la que obtuvo mayor puntaje cumpliendo con la mayoría de los parámetros medidos anteriormente.

MAGERIT es una metodología de análisis y gestión de riesgos de los Sistemas de Información fue Elaborado por el Consejo Superior de Administración Electrónica para tratar de reducir los riesgos de implantación y uso de las Tecnologías de Información enfocadas a las Administración Publica.

3.9. Proceso de MAGERIT

El cálculo de los riesgos de seguridad de información incluye el análisis y la evaluación del riesgo. Esta etapa se construye en el núcleo central de MAGERIT, y su correcta aplicación condiciona la validez y utilidad de todo el proyecto.

Objetivos del análisis de riesgos:

- Identificación de activos de información
- Identificación de amenazas
- Determinar si existen salvaguardas para los activos
- Identificación de vulnerabilidades
- Estimar el impacto si una amenaza llegara a materializarse.

Toda organización se halla expuesta a diferentes riesgos, puesto a que no existe un ambiente 100% seguro, ya que están expuestos a vulnerabilidades y los riesgos son constantes. Por este y otros motivos la organización deberá estar pendiente a cualquier cambio o situación extraña que se presente, pudiendo afectar negativamente un activo, un dominio o a toda su organización.

Para MAGERIT esta etapa es la más importante considerándose en el núcleo central de la investigación ya que su correcta aplicación condiciona la validez y utilidad de todo el proyecto.

El análisis de riesgos permite determinar las vulnerabilidades, riesgos, peligros, etc., que existen en nuestros activos evaluando de manera ordenada para llegar a conclusiones con fundamento.

3.9.1. Elementos de Análisis de Riesgos

- **Activos**: Son todos los elementos del Sistema de Información que generan valor para la organización.
- **Amenazas**: Son todos los eventos que pueden afectar a los activos de la organización causando daños o pérdidas materiales.

- **Salvaguardas**: Son los mecanismos de defensa que utilizamos para amenazas que pueden causarnos daño.

Con los elementos anteriormente mencionados se puede identificar:

- **El impacto**: Es todo lo que podría pasar en la organización.
- **El riesgo**: lo que probablemente pase.

En el siguiente gráfico se muestra los elementos que intervienen en el análisis del riesgo.

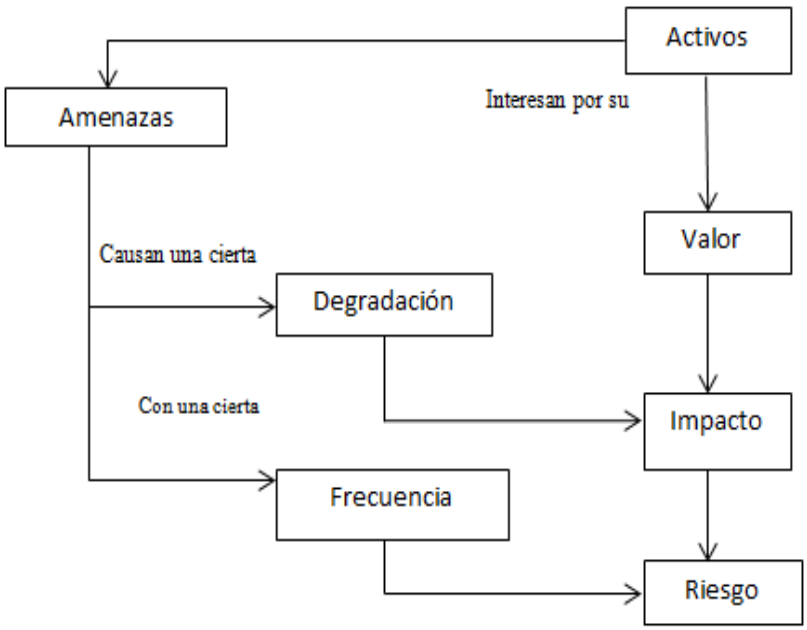


Gráfico 2-3 Análisis de riesgos

Fuente: MAGERIT
Elaborado por: Castillo Jessica, 2016

Para el desarrollo de esta etapa, la recolección de la información se desarrolló mediante encuestas y entrevistas a los técnicos de la Dirección de Tecnologías de la Información y Comunicación (DTIC) de la Escuela Superior Politécnica de Chimborazo, también se considera las inspecciones físicas realizadas a los servidores Web y su entorno físico.

3.10. Identificación de activos de información

La identidad de activos es importante ya que permite materializar con precisión el alcance de la investigación, permite valorar los activos con veracidad e identificar las amenazas a las que se encuentran expuestos dichos activos.

En la siguiente tabla se muestra los activos de la DTIC.

Tabla 6-3 Activos

Número de Activo	Activo
Activo 1	Servicios Web
Activo 2	Equipos Informáticos
Activo 3	Soportes de información
Activo 4	Instalaciones
Activo 5	Personal

Fuente: Alex Tacuri
Elaborado por: Castillo Jessica, 2016

3.10.1. Activo 1

En la siguiente tabla se enumeran los servicios Web que brinda la Plataforma de la Escuela Superior Politécnica de Chimborazo sus estudiantes, docentes, etc.

Tabla 7-3 Servicios Web

Servicio	URL
Escuela de Postgrado y Educación continua	http://sisepec.espoch.edu.ec/
Infraestructura de Datos Espaciales	http://ide.espoch.edu.ec/
OASIS	http://academicoseg.espoch.edu.ec/
Evaluación Institucional	http://evaluacion.espoch.edu.ec/
Talento Humano	http://recursos.espoch.edu.ec/
Educación Virtual	http://elearning.espoch.edu.ec/
Biblioteca	http://bibliotecas.espoch.edu.ec/
Medico	http://medicina.espoch.edu.ec/
Bienestar Politécnico	http://bienestar.espoch.edu.ec/
Herbario	http://biblioteca.espoch.edu.ec/herbario.htm
Consulta del Estado de Matricula	http://infopagos.espoch.edu.ec/
Bolsa de empleo	http://empleos.espoch.edu.ec/
Passport	http://passportsignin.espoch.edu.ec/

Fuente: www.espoch.edu.ec
Elaborado por: Castillo Jessica, 2016

3.10.2. Activo 2

En la siguiente tabla se detallan los equipos informáticos que posee la institución se tiene los siguientes:

Tabla 8-3 Equipos Informáticos DTIC

Equipos Informáticos	
Servidores (Cantidad 4)	CISCO SYSTEM UCSB-B200-M3 20 CORES EN 2 MICROROCESADOR
Procesador	MICROPROCESADOR INTEL XEON 2.2 GHZ
Memoria	MEMORIA DE 30 GB

Fuente: Alex Tacuri Técnico DTIC
Elaborado por: Castillo Jessica, 2016

Cabe resaltar que cada servidor físico contiene 12 máquinas virtuales, que son utilizadas para la administración de los servicios que presta la DTIC.

3.10.3. Activo 3

En la institución generalmente se utilizan los siguientes dispositivos de almacenamiento que a continuación se enumeran:

- Dispositivos USB
- Material impreso
- Storage
- Cintas y Librerías de Backup
- Discos formato DVD
- Discos formato CD

3.10.4. Activo 4

Aquí citaremos los lugares y su infraestructura donde se colocan los Sistemas de información en nuestro caso será donde se encuentran los servidores web.

La infraestructura donde se localizan los servidores web: Se encuentran ubicados en el segundo piso del Edificio de DTIC, cuenta con piso flotante, las paredes son de cemento, también cuentan sensores de fuego, los técnicos que ingresan deben conocer la clave de acceso y tener permiso del técnico a cargo.

3.10.5. Activo 5

En la siguiente tabla se cita a todo el personal que se encarga de la administración de los servicios web.

Tabla 9-3 Personal

N°-	Nómina Área Servicios Web
1	Alex Tacuri
2	Saúl Yasaca
3	Edison Villa
4	Diego Palacios
5	Juan Carlos Díaz
6	Anita Llalao
7	Fabián Villa

Fuente: Alex Tacuri Técnico DTIC
Elaborado por: Castillo Jessica, 2016

3.10.6. Identificación de activos relevantes:

Para la identificación de amenazas, salvaguardas y vulnerabilidades se realizó un análisis de los activos más importantes con el Ing. Alex Tacuri Técnico de DTIC, mediante entrevistas donde se analizaron las ventajas y desventajas así de definieron los activos relevantes de la Dirección de Tecnologías de la Información y Comunicación. A continuación en la siguiente tabla se enumeran los activos relevantes.

Tabla 10-3 Identificación de Activos relevantes del DTIC

N°-	Activos de Información
1	UPS
2	Planta de energía
3	Servidor 1

4	Servidor 2
5	Servidor 3
6	Servidor 4
7	Memoria 1 (Servidor 1)
8	Memoria 2 (Servidor 2)
9	Memoria 3 (Servidor 3)
10	Memoria 4 (Servidor 4)
11	Storage

Fuente: Alex Tacuri Técnico DTIC
Elaborado por: Castillo Jessica, 2016

A modo de ilustración en la siguiente tabla se muestran los activos de información con sus respectivos administradores.

Tabla 11-3 Activos de Información y Propietarios

Activos de Información	Propietarios (Administradores)
UPS	Alex Tacuri
Planta de energía	Alex Tacuri
Servidor 1	Alex Tacuri
Servidor 2	Alex Tacuri
Servidor 3	Alex Tacuri
Servidor 4	Alex Tacuri
Servidor 1	Alex Tacuri
Memoria 2 (Servidor 2)	Alex Tacuri
Memoria 3 (Servidor 3)	Alex Tacuri
Memoria 4 (Servidor 4)	Alex Tacuri
Storage	Alex Tacuri
Personal	Alex Tacuri Director encargado DTIC

Fuente: Alex Tacuri Técnico DTIC
Elaborado por: Castillo Jessica, 2016

En la cláusula 4.2.1 (d) el ISO 27001:2005 exige que la institución no solo identifique los activos de relevancia sino que también identifique los propietarios en este caso los administradores o quien está a cargo cada activo de información o servidores web.

El administrador o el personal que se encuentra a cargo del activo o de los activos de información debe ser responsable de definir apropiadamente la clasificación de seguridad y los derechos de acceso a los activos, y establecer los sistemas de control.

3.11. Identificación de Amenazas

Luego de identificar los activos, vamos a identificar las amenazas, tomando en cuenta una o varias amenazas que pueden afectar a cada activo. Amenaza son eventos que pueden desatar un incidente dentro de la institución, produciendo daños materiales o pérdida de datos. Para la identificación de las amenazas que pudieren afectar a los activos, conviene clasificar por su naturaleza, para así facilitar su ubicación.

Para la identificación de las amenazas se utilizaran encuestas dirigidas a los técnicos que administran los servidores web de la Dirección de Tecnologías de la Información y Comunicación de la Escuela Superior Politécnica de Chimborazo sobre las diferentes amenazas que existen de acuerdo a la siguiente clasificación:

- Amenazas Naturales
- Amenazas a Instalaciones
- Amenazas Humanas
- Amenazas Tecnológicas
- Amenazas Operacionales|
- Amenazas Sociales

Como se puede observar las amenazas se pueden originar de Fuentes o eventos provisionales o meditados.

Para que una amenaza cause daño a algún activo de información tendría que explotar una o más vulnerabilidades del sistema, aplicaciones o servicios usados por la organización a efectos de poder ser exitosa en su intención de hacer daño.

Vamos a considerar las amenazas obtenidas de las encuestas realizadas al administrador del DTIC.

La degradación mide el daño causado por un incidente en el supuesto de que ocurriera. Se caracteriza con una fracción del valor del activo Para calificar la frecuencia y degradación de las amenazas se realiza de manera manual para su mayor comprensión.

En la siguiente tabla se muestra la escala con la que vamos a medir la degradación de los activos de la Dirección de Tecnologías de la Información y Comunicación - DTIC.

Tabla 12-3 Escala de Degradación

Calificación	Significado
25%	Poco
50%	Medio
75%	Alto
100%	Muy Alto

Fuente: Sitio Web; Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
Elaborado por: Castillo Jessica, 2016

La frecuencia es cada cuanto se materializa la amenaza, se modela como una tasa anual de ocurrencia, siendo valores típicos. En la siguiente tabla se muestra la escala con la que vamos a medir la frecuencia de daños que tienen los activos de relevancia.

Tabla 13-3 Escala de Frecuencia

Calificación	Significado
360	A Diario
12	Mensualmente
4	Cuatro veces al año
2	Dos veces al año
1	Una vez al año
1/12	Cada varios años

Fuente: Portal de Administración Electrónico
Elaborado por: Castillo Jessica, 2016

En la siguiente tabla se detalla la identificación de las amenazas con el grado de frecuencia y el porcentaje de frecuencia que ocurre:

Tabla 14-3 Identificación de Amenazas

Activo	Amenazas	Frecuencia	Degradación
UPS	• Caída de energía • Avería de origen físico o lógica • Acceso no autorizado • Falta de mantenimiento	4	50%
Planta de Energía	• Caída de energía • Avería de origen físico o lógica • Acceso no autorizado • Falta de mantenimiento	4	50%
Servidor 1	• Caída de energía • Avería de origen físico o lógica • Acceso no autorizado • Errores de los usuarios • Errores del Administrador • Errores de configuración • Errores de mantenimiento • Manipulación de la configuración • Hacking • Pérdida de datos	4	25%
Servidor 2	• Caída de energía • Avería de origen físico o lógica • Acceso no autorizado • Errores de los usuarios • Errores del Administrador • Errores de configuración • Errores de mantenimiento • Manipulación de la configuración • Hacking • Pérdida de datos	4	25%
Servidor 3	• Caída de energía • Avería de origen físico o lógica • Acceso no autorizado • Errores de los usuarios • Errores del Administrador • Errores de configuración • Errores de mantenimiento • Manipulación de la configuración • Hacking • Pérdida de datos	4	25%

Servidor 4	• Caída de energía • Avería de origen físico o lógica • Acceso no autorizado • Errores de los usuarios • Errores del Administrador • Errores de configuración • Errores de mantenimiento • Manipulación de la configuración • Hacking • Pérdida de datos	4	25%
Memoria 1	• Caída de energía • Avería de origen físico o lógica • Acceso no autorizado • Pérdida de datos	1	50%
Memoria 2	• Caída de energía • Avería de origen físico o lógica • Acceso no autorizado • Pérdida de datos	1	50%
Memoria 3	• Caída de energía • Avería de origen físico o lógica • Acceso no autorizado • Pérdida de datos	1	50%
Memoria 4	• Caída de energía • Avería de origen físico o lógica • Acceso no autorizado • Pérdida de datos	1	50%
Storage	• Caída de energía • Avería de origen físico o lógica • Acceso no autorizado • Pérdida de datos	1/12	100%
Servicios Web	• Caída de energía • Avería de origen lógica • Acceso no autorizado • Errores de los usuarios • Errores del Administrador • Errores de configuración • Errores de mantenimiento • Manipulación de la	1	100%

	configuración • Hacking • Pérdida de datos		
Personal	• Problemas de transporte • Perdida de personal clave • Falta de capacitación	1	50%

Fuente: Alex Tacuri Técnico DTIC
Elaborado por: Castillo Jessica, 2016

Es necesario mencionar que la existencia de una amenaza con baja posibilidad de ocurrencia puede tener severas consecuencias económicas para la institución.

3.12. Identificación de salvaguardas

Una vez identificadas las amenazas, se identificó los mecanismos de salvaguarda implantados en aquellos activos, describiendo las dimensiones de seguridad que estos mantienen tomando en consideración las siguientes dimensiones: Disponibilidad, Integridad, Confiabilidad, Autenticidad.

Los mecanismos de salvaguarda son procedimientos, dispositivos que ayudan a reducir los riesgos. En la siguiente tabla observamos las diferentes salvaguardas que tienen los activos observados.

Tabla 15-3 Identificación de Salvaguardas

Activos de Información	Salvaguarda	Dimensión
UPS	Protección del equipo dentro de la organización	• Disponibilidad
Planta de energía	Protección del equipo dentro de la organización	• Disponibilidad
Servidor 1	Claves Protección del equipo dentro de la organización	• Disponibilidad • Autenticidad • Confiabilidad
Servidor 2	Claves Protección del equipo dentro de la organización	• Disponibilidad • Autenticidad • Confiabilidad
Servidor 3	Claves Protección del equipo dentro de la organización	• Disponibilidad • Autenticidad • Confiabilidad
Servidor 4	Claves	• Disponibilidad

	Protección del equipo dentro de la organización	• Autenticidad • Confiabilidad
Memoria 1	Protección del equipo dentro de la organización	• Disponibilidad • Integridad • Confiabilidad
Memoria 2	Protección del equipo dentro de la organización	• Disponibilidad • Integridad • Confiabilidad
Memoria 3	Protección del equipo dentro de la organización	• Disponibilidad • Integridad • Confiabilidad
Memoria 4	Protección del equipo dentro de la organización	• Disponibilidad, • Integridad • Confiabilidad
Storage	Protección del equipo dentro de la organización	• Disponibilidad • Autenticidad • Confiabilidad • Integridad
Servicios Web	Protección del servicio dentro de la organización	• Disponibilidad • Autenticidad • Integridad • Confiabilidad
Personal	Plan de contingencia	• Disponibilidad • Integridad • Confiabilidad

Fuente: Alex Tacuri Técnico DTIC
Elaborado por: Castillo Jessica, 2016

3.13. Identificación de Vulnerabilidades

Para la identificación de las vulnerabilidades se utilizó la plataforma VEGA para identificar las vulnerabilidades en los Servicios Web, utilizamos VEGA ya que es un escáner de código y pruebas de plataforma libre y abierta para probar la seguridad de las aplicaciones web. Para medir la seguridad se utilizó el VEGA escaneando los URLs de los Servicios Web de la Espoch.

A continuación se enumera los servicios y en qué estado se encuentran.

Tabla 16-3 Estado de los Servicios Web

Servicios Web	Estado
http://sisepec.espoch.edu.ec/	Activo
http://ide.espoch.edu.ec/	Pasivo
http://academicoseg.espoch.edu.ec/	Activo
http://evaluacion.espoch.edu.ec/	Activo
http://recursos.espoch.edu.ec/	Activo
http://elearning.espoch.edu.ec/	Activo
http://bibliotecas.espoch.edu.ec/	Activo
http://medicina.espoch.edu.ec/	Activo
http://bienestar.espoch.edu.ec/	Activo
http://biblioteca.espoch.edu.ec/herbario.htm	Pasivo
http://infopagos.espoch.edu.ec/	Pasivo
http://empleos.espoch.edu.ec/	Activo
http://passportsignin.espoch.edu.ec/	Activo

Fuente: Sitio Web ESPOCH
Elaborado por: Castillo Jessica, 2016

Para la identificación de las vulnerabilidades se utilizó el escáner VEGA de Linux, estas pruebas se realizaron a 10 de los 13 servicios web que se encontraron activos.

En el escáner VEGA se introduce la URL de cada servicio web donde vamos a identificar las vulnerabilidades, cada escaneo duro más de 48 horas.

A continuación se detallan las pruebas realizadas y los resultados obtenidos de las diferentes URLs de los servicios web de la Escuela Superior Politécnica de Chimborazo.

- **SERVICIO WEB:** Escuela de Postgrado y Educación Continua
- **URL:** http://sisepec.espoch.edu.ec/

Tabla 17-3 Identificación de Vulnerabilidades

Nombre	Grado	Numero	Descripción
Page Fingerprint Differential Detected	High	5	• Se detectó una huella dactilar respuesta diferente en relación a un archivo local que incluye un intento de inyección. Esto puede indicar que un archivo local incluye la vulnerabilidad. • Si esto se debe a un archivo local, la explotación del archivo local incluye vulnerabilidades que pueden permitir a los atacantes obtener acceso no autorizado a los archivos, que también puede ayudar en otros ataques. • Diferentes respuestas también pueden indicar la presencia de una vulnerabilidad de enumeración de archivos, que en lugar de permitir al atacante obtener acceso a los archivos contenidos, les permita determinar si existen archivos en el sistema.

Fuente: VEGA
Elaborado por: Castillo Jessica, 2016

Tabla 18-3 Resumen de Vulnerabilidades

NOMBRE	GRADO	NUMERO
Page Fingerprint Differential Detected	High	5

Fuente: VEGA
Elaborado por: Castillo Jessica, 2016

- **SERVICIO WEB:** OASIS
- **URL:** http://academicoseg.espoch.edu.ec/

Tabla 19-3 Identificación de Vulnerabilidades OASIS

Nombre	Grado	Número	Descripción
Cleartext Password over HTTP	High	1	Se detectó una forma que pueda causar una presentación de contraseña a través de un canal no seguro. Esto podría ser la divulgación de contraseñas a los espías de la red.
SQL Injection	High	2	Se detectó una posible vulnerabilidad de inyección SQL. Estas vulnerabilidades pueden ser explotadas por atacantes remotos para ganar lectura no autorizada o acceso de escritura a la base de datos. Explotación de vulnerabilidades de inyección SQL también puede permitir ataques contra la lógica de la aplicación. Los atacantes pueden ser capaces de obtener acceso no autorizado al servidor que aloja la base de datos.
Local Filesystem Paths Found	Medium	1	Se detectó lo que puede ser caminos de sistemas de archivos absolutas en el contenido escaneado. La divulgación de estos caminos revela información sobre el diseño del sistema de archivos. Esta información puede ser sensible, su divulgación puede aumentar las posibilidades de éxito para otros ataques.
From Password Field with Autocomplete Enable	Low	1	Un valor de la contraseña se puede almacenar en el sistema de archivos local del cliente. Localmente contraseñas almacenadas podrían ser recuperados por otros usuarios o código malicioso.

Fuente: VEGA
Elaborado por: Castillo Jessica, 2016

Tabla 20-4 Resumen de Vulnerabilidades OASIS

Nombre	Grado	Número
Cleartext Password over HTTP	High	1
SQL Injection	High	2
Local Filesystem Paths Found	Medium	1
From Password Field with Autocomplete Enable	Low	1

Fuente: VEGA
Elaborado por: Castillo Jessica, 2016

- **SERVICIO WEB:** Evaluación Institucional
- **URL:** http://evaluacion.espoch.edu.ec/

Tabla 21-3 Identificación de Vulnerabilidades Evaluación Institucional

Nombre	Grado	Número	Descripción
Shell Injection	High	4	Se detectó una posible vulnerabilidad de inyección de comandos. Los atacantes pueden ser capaces de ejecutar comandos en el servidor. La explotación puede provocar el acceso remoto no autorizado.
SQL Injetion	High	9	Se detectó una posible vulnerabilidad de inyección de comandos. Los atacantes pueden ser capaces de ejecutar comandos en el servidor. La explotación puede provocar el acceso remoto no autorizado. Explotación de vulnerabilidades de inyección SQL también puede permitir ataques contra la lógica de la aplicación. Los atacantes pueden ser capaces de obtener acceso no autorizado al servidor que aloja la base de datos.
HTTP Trace Support Detected	Medium	1	Permitir HTTP TRACE puede permitir el rastreo de cross-site. Los atacantes pueden ser capaces de utilizar en sitios cruzados trazando con cross-site scripting recuperar el valor de HttpOnly cookies.
Local Filesystem Phaths Found	Medium	62	Se detectó lo que puede ser caminos de sistemas de archivos en el contenido escaneado. La divulgación de estos caminos revela información sobre el diseño del sistema de archivos. Esta información puede ser sensible, su divulgación puede aumentar las posibilidades de éxito para otros ataques.
PHP Error Detected	Medium	61	Se detectó la firma de una página de error de PHP. Páginas de error generados automáticamente pueden filtrar información sensible. La información puede incluir ajustes de configuración y la base de datos o la estructura del sistema de archivos.
Possible XML Injection	Medium	3	Se detectó que puede ser posible para corromper la estructura de un documento XML del lado del

			servidor. Esto podría afectar a la lógica de la aplicación, dependiendo de cómo se usa el documento XML. Una vulnerabilidad de inyección XML puede conducir a una pérdida de la integridad de los datos utilizados o almacenados por la aplicación. XML puede ser un vector de inyección que no pasa por los filtros de contenido.
Directory Listing Detected	Low	6	El servidor está enviando el contenido de los directorios. Esto podría exponer archivos no destinados a la recuperación de usuario. El listado del directorio puede proporcionar además información útil sobre el diseño y las características del sistema, como la nomenclatura utilizadas por los desarrolladores y administradores. Esta información puede aumentar la probabilidad de éxito para ataques.

Fuente: VEGA
Elaborado por: Castillo Jessica, 2016

Tabla 22-3 Resumen de Vulnerabilidades Evaluación Institucional

nombre	grado	número
shell injection	high	4
sql injetion	high	9
http trace support detected	medium	1
local filesystem phaths found	medium	62
php error detected	medium	61
possible xml injection	medium	3
directory listing detected	low	6

Fuente: VEGA
Elaborado por: Castillo Jessica, 2016

- **SERVICIO WEB:** Talento Humano
- **URL:** http://recursos.espoch.edu.ec/

Tabla 23-3 Identificación de Vulnerabilidades Talento Humano

Nombre	Grado	Número	Descripcion
Cleartext Password over HTTP	High	1	Se detectó una forma de proteger la contraseña a través de un canal no seguro. Esto podría resultar una divulgación de contraseñas a los espías de la red.
Cross Site Scripting	High	7	XSS es generalmente una amenaza para las aplicaciones web que se han autenticado usuarios o son de otro modo de seguridad sensibles. El código malicioso puede ser capaz de manipular el contenido de la página, cambiar su apariencia y/o función para otro usuario. Esto incluye la modificación del comportamiento de la aplicación web. El código también puede ser capaz de realizar acciones dentro de la aplicación sin el conocimiento del usuario. Código de secuencias de comandos también puede obtener y retransmitir los valores de cookie si no se han establecido HttpOnly.
Page Fingerprint Differential Detected	High	2	Se detectó una huella dactilar respuesta diferente en relación a un archivo local incluyen intento de inyección. Esto puede indicar que un archivo local incluye la vulnerabilidad, aunque esto no está confirmado. Si esto se debe a un archivo local, puede permitir a los atacantes obtener acceso no autorizado a los archivos, que también puede ayudar en otros ataques. Diferentes respuestas también pueden indicar la presencia de una vulnerabilidad de enumeración de archivos, que en lugar de permitir al atacante obtener acceso a los archivos contenidos, les permita determinar si existen archivos en el sistema.
URL Injection	Medium	3	Un enlace suministrado desde el exterior se ha utilizado como un atributo (por ejemplo, src, href, valor) en una etiqueta HTML. Esto puede tener una variedad de posibles consecuencias buena a

			grave, dependiendo de la etiqueta. Los impactos pueden incluir la búsqueda automática de contenido malicioso remoto. Estos podrían ser utilizados para phishing o, posiblemente, ataques entre dominios.
Directory Listing Detected	Low	3	El servidor está enviando el contenido de los directorios. Esto podría exponer archivos no destinados a la recuperación de usuario. El listado del directorio puede proporcionar además información útil sobre el diseño y las características del sistema, como la nomenclatura utilizadas por los desarrolladores y administradores. Esta información puede aumentar la probabilidad de éxito para ataques ciegos y ataques por fuerza bruta.
From Password Field with Autocomplete Enabled	Low	1	Un valor de la contraseña se puede almacenar en el sistema de archivos local del cliente. Localmente contraseñas almacenadas podrían ser recuperados por otros usuarios o código malicioso.

Fuente: VEGA
Elaborado por: Castillo Jessica, 2016

Tabla 24-3 Resumen de Vulnerabilidades Talento Humano

Nombre	Grado	Numero
Cleartext Password over HTTP	High	1
Cross Site Scripting	High	7
Page Fingerprint Differential Detected	High	2
URL Injection	Medium	3
Directory Listing Detected	Low	3
From Password Field with Autocomplete Enabled	Low	1

Fuente: VEGA
Elaborado por: Castillo Jessica, 2016

- **SERVICIO WEB:** Educación Virtual
- **URL:** http://elearning.espoch.edu.ec/

Tabla 25-3 Identificación de Vulnerabilidades Educación Virtual

Nombre	Grado	Numero	Descripción
Cleartext Password over HTTP	High	3	Se detectó una forma que pueda causar una presentación contraseña a través de un canal no seguro. Esto podría resultar en la divulgación de contraseñas a los espías de la red.
SQL Injetion	High	32	Se detectó una posible vulnerabilidad de inyección de comandos. Los atacantes pueden ser capaces de ejecutar comandos en el servidor. La explotación puede provocar el acceso remoto no autorizado. Explotación de vulnerabilidades de inyección SQL también puede permitir ataques contra la lógica de la aplicación. Los atacantes pueden ser capaces de obtener acceso no autorizado al servidor que aloja la base de datos.
Shell Injection	High	68	Se detectó una posible vulnerabilidad de inyección de comandos. Los atacantes pueden ser capaces de ejecutar comandos en el servidor. La explotación puede provocar el acceso remoto no autorizado.
HTTP Trace Support Detected	Medium	1	Permitir HTTP TRACE puede permitir el rastreo de cross-site. Los atacantes pueden ser capaces de utilizar en sitios cruzados trazando con cross-site scripting recuperar el valor de HttpOnly cookies.
Local Filesystem Paths Found	Medium	4	Se detectó lo que puede ser caminos de sistemas de archivos absolutas en el contenido escaneado. La divulgación de estos caminos revela información sobre el diseño del sistema de archivos. Esta información puede ser sensible, su divulgación puede aumentar las posibilidades de éxito para otros ataques.
Possible XML Injection	Medium	31	Se detectó una posible vulnerabilidad de inyección XML. Inyección XML puede ocurrir cuando se utiliza datos suministrados externamente que no ha sido suficientemente validado para crear un documento XML. Es posible que estos datos puedan corromper la estructura de los documentos. Las

			posibles consecuencias dependen del documento XML y para qué se utiliza.
Directory Listing Detected	Low	1166	El servidor está enviando el contenido de los directorios. Esto podría exponer archivos no destinados a la recuperación de usuario. El listado del directorio puede proporcionar además información útil sobre el diseño y las características del sistema, como las convenciones de nomenclatura utilizadas por los desarrolladores y administradores. Esta información puede aumentar la probabilidad de éxito para ataques ciegos y ataques de fuerza bruta.
Form Password Field with Autocomplete Enabled	Low	3	Un valor de la contraseña se puede almacenar en el sistema de archivos local del cliente. Localmente contraseñas almacenadas podrían ser recuperados por otros usuarios o código malicioso.

Fuente: VEGA
Elaborado por: Castillo Jessica, 2016

Tabla 26-3 Resumen de Vulnerabilidades Educación Virtual

Nombre	Grado	Número
Cleartext Password over HTTP	High	3
SQL Injetion	High	32
Shell Injection	High	68
HTTP Trace Support Detected	Medium	1
Local Filesystem Paths Found	Medium	4
Possible XML Injection	Medium	31
Directory Listing Detected	Low	1166
Form Password Field with Autocomplete Enabled	Low	3

Fuente: VEGA
Elaborado por: Castillo Jessica, 2016

- **SERVICIO WEB:** Biblioteca
- **URL**: http://bibliotecas.espoch.edu.ec/

Tabla 27-3 Identificación de vulnerabilidades Biblioteca

Nombre	Grado	Numero	Descripción
Cleartext Password over HTTP	High	269	Se detectó una forma que pueda causar una presentación de contraseña a través de un canal no seguro. Esto podría ser la divulgación de contraseñas a los espías de la red. Esto podría resultar una divulgación de contraseñas a los espías de la red.
Cross Site Scripting	High	2	XSS es generalmente una amenaza para las aplicaciones web que se han autenticado usuarios o son de otro modo de seguridad sensibles. El código malicioso puede ser capaz de manipular el contenido de la página, cambiar su apariencia y / o función para otro usuario. Esto incluye la modificación del comportamiento de la aplicación web. El código también puede ser capaz de realizar acciones dentro de la aplicación sin el conocimiento del usuario. Código de secuencias de comandos también puede obtener y retransmitir los valores de cookie si no se han establecido HttpOnly.
SQL Injection	High	5	Se detectó una posible vulnerabilidad de inyección SQL. Estas vulnerabilidades pueden ser explotadas por atacantes remotos para ganar lectura no autorizada o acceso de escritura a la base de datos. Explotación de vulnerabilidades de inyección SQL también puede permitir ataques contra la lógica de la aplicación. Los atacantes pueden ser capaces de obtener acceso no autorizado al servidor que aloja la base de datos.
Local Filesystem Paths Found	Medium	2	Se detectó lo que puede ser caminos de sistemas de archivos absolutas en el contenido escaneado. La divulgación de estos caminos revela información sobre el diseño del sistema de archivos. Esta información puede ser sensible, su divulgación puede aumentar las posibilidades de éxito para otros ataques.

Form Password Field with Autocomplete Enabled	Low	268	Un valor de la contraseña se puede almacenar en el sistema de archivos local del cliente. Localmente contraseñas almacenadas podrían ser recuperados por otros usuarios o código malicioso.

Fuente: VEGA
Elaborado por: Castillo Jessica, 2016

Tabla 28-3 Resumen de Vulnerabilidades Biblioteca

Nombre	Grado	Numero
Cleartext Password over HTTP	High	269
Cross Site Scripting	High	2
SQL Injection	High	5
Local Filesystem Paths Found	Medium	2
Form Password Field with Autocomplete Enabled	Low	268

Fuente: VEGA
Elaborado por: Castillo Jessica, 2016

- **SERVICIO WEB:** Médico
- **URL**: http://medicina.espoch.edu.ec/

Tabla 29-3 Identificación de Vulnerabilidades Médico

NOMBRE	GRADO	NUMERO	DESCRIPCION
Local Filesystem Paths Found	Medium	1	Se detectó lo que puede ser caminos de sistemas de archivos absolutas en el contenido escaneado. La divulgación de estos caminos revela información sobre el diseño del sistema de archivos. Esta información puede ser sensible, su divulgación puede aumentar las posibilidades de éxito para otros ataques.
Possible Source Code Disclosure	Medium	1	Podría dar lugar a la revelación de información sensible, resultado en la divulgación de información sensible a los atacantes. Fragmentos de código Fuente puede incluir información sobre el diseño / estructura de la aplicación, incluyendo el uso de componentes de terceros.

Fuente: VEGA
Elaborado por: Castillo Jessica, 2016

Tabla 30-3 Resumen de Vulnerabilidades Médico

NOMBRE	GRADO	NUMERO
Local Filesystem Paths Found	Medium	1
Possible Source Code Disclosure	Medium	1

Fuente: VEGA
Elaborado por: Castillo Jessica, 2016

- **SERVICIO WEB:** Bienestar Politécnico
- **URL:** http://bienestar.espoch.edu.ec/

Tabla 31-3 Identificación de Vulnerabilidades Bienestar Politécnico

Nombre	Grado	Número	Descripción
HTTP Trace Support Detected	Medium	1	Permitir HTTP TRACE puede permitir el rastreo de cross-site. Los atacantes pueden ser capaces de utilizar en sitios cruzados trazando con cross-site scripting recuperar el valor de HttpOnly cookies.
Local Filesystem Paths Found	Medium	1	Se detectó lo que puede ser caminos de sistemas de archivos absolutas en el contenido escaneado. La divulgación de estos caminos revela información sobre el diseño del sistema de archivos.
Directory Listing Detected	Low	2	El servidor está enviando el contenido de los directorios. Esto podría exponer archivos no destinados a la recuperación de usuario. El listado del directorio puede proporcionar además información útil sobre el diseño y las características del sistema.
Email Addresses Found	Low	1	Las direcciones de correo electrónico expuestos a Internet se rasparon por spam y se agregan a las listas de spam. Las direcciones de correo electrónico también se pueden utilizar en los ataques dirigidos y phishing. Las direcciones de correo electrónico podrían ser utilizadas para adivinar con más exactitud los nombres de usuario de la aplicación.

Fuente: VEGA
Elaborado por: Castillo Jessica, 2016

Tabla 32-3 Identificación de Vulnerabilidades Bienestar Politécnico

Nombre	Grado	Número
HTTP Trace Support Detected	Medium	1
Local Filesystem Paths Found	Medium	1
Directory Listing Detected	Low	2
Email Addresses Found	Low	1

Fuente: VEGA
Elaborado por: Castillo Jessica, 2016

- **SERVICIO WEB:** Bolsa de Empleos
- **URL:** http://empleos.espoch.edu.ec/

Tabla 33-3 Identificación de Vulnerabilidades Bolsa de Empleos

Nombre	Grado	Número	Descripción
Cleartext Password over HTTP	High	3	Se detectó una forma que pueda causar una presentación de contraseña a través de un canal no seguro. Esto podría ser la divulgación de contraseñas a los espías de la red.
Local Filesystem Paths Found	Medium	2	Se detectó lo que puede ser caminos de sistemas de archivos absolutas en el contenido escaneado. La divulgación de estos caminos revela información sobre el diseño del sistema de archivos.
Form Password Field with Autocomplete Enabled	Low	3	Un valor de la contraseña se puede almacenar en el sistema de archivos local del cliente. Localmente contraseñas almacenadas podrían ser recuperados por otros usuarios o código malicioso.

Fuente: VEGA
Elaborado por: Castillo Jessica, 2016

Tabla 34-3 Resumen de Vulnerabilidades Bolsa de Empleos

Nombre	Grado	Número
Cleartext Password over HTTP	High	3
Local Filesystem Paths Found	Medium	2
Form Password Field with Autocomplete Enabled	Low	3

Fuente: VEGA
Elaborado por: Castillo Jessica, 2016

- **SERVICIO WEB:** Passport
- **URL:**http://passportsignin.espoch.edu.ec

Tabla 35-3 Identificación de Vulnerabilidades Passport

Nombre	Grado	Número	Descripción
Cleartext Password over HTTP	High	2	Se detectó una forma que pueda causar una presentación de contraseña a través de un canal no seguro. Esto podría ser la divulgación de contraseñas a los espías de la red.
Page Fingerprint Differential Detected	High	1	Se detectó una huella dactilar respuesta diferente en relación a un archivo local incluyen intento de inyección. Esto puede indicar que un archivo local incluye la vulnerabilidad, aunque esto no está confirmado.
ASP/ASPX Error Detected	Low	1	Salida de error detallado. Los datos en esta salida podría revelar información sensible acerca de la aplicación que podría ayudar a los ataques más complejos.
Form Password Field with Autocomplete Enabled	Low	2	Un valor de la contraseña se puede almacenar en el sistema de archivos local del cliente. Localmente contraseñas almacenadas podrían ser recuperados por otros usuarios o código malicioso.

Fuente: VEGA
Elaborado por: Castillo Jessica, 2016

Tabla 36-3 Resumen de Vulnerabilidades Passport

Nombre	Grado	Número
Cleartext Password over HTTP	High	2
Page Fingerprint Differential Detected	High	1
ASP/ASPX Error Detected	Low	1
Form Password Field with Autocomplete Enabled	Low	2

Fuente: VEGA
Elaborado por: Castillo Jessica, 2016

A continuación se realiza una tabla de resumen en la cual se detalla el valor total de las vulnerabilidades encontradas en los 10 servicios web escaneados por VEGA .

Esta información permitirá identificar, mitigar y eliminar las vulnerabilidades encontradas.

Tabla 37-3 Total de Vulnerabilidades

Nombre	Grado
ALTAS	416
MEDIAS	175
BAJAS	1457

Fuente: VEGA
Elaborado por: Castillo Jessica, 2016

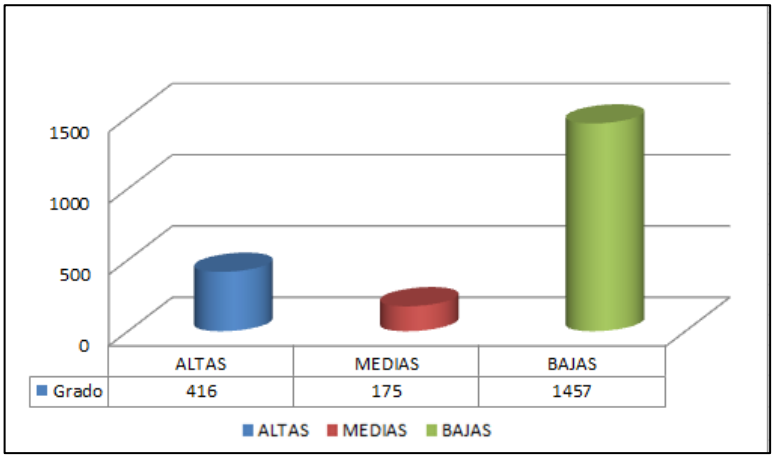


Gráfico 3-3 Total de Vulnerabilidades

Fuente: VEGA
Elaborado por: Castillo Jessica, 2016

Análisis:

Del total de las vulnerabilidades encontradas podemos evidenciar que el 20% de las vulnerabilidades son Altas, el 9% son Medias y el 71% de las vulnerabilidades son bajas.

Hay que tomar en consideración que las vulnerabilidades que se deben reducir o mitigar son las altas puesto que el impacto potencial de daño sería más grave para los servicios web de la Espoch, las vulnerabilidades medias y bajas deben ser controladas a corto plazo tomando medidas que minimicen su impacto. (Ver gráfico 4.3)

3.14. Identificación de vulnerabilidades después de aplicar la propuesta de solución para la reducción de riesgos de seguridad informática en servicios web de la Escuela Superior politécnica de Chimborazo

A continuación se detallan las vulnerabilidades encontradas después de la aplicación de la propuesta de reducción de riesgos en dos de sus Servicios Web.

- **SERVICIO WEB**: Educación Virtual
- **URL: http:**//elearning.espoch.edu.ec/

Tabla 38-3 Vulnerabilidades después de la aplicación de la propuesta de solución de Educación Virtual

Nombre	Grado	Número
Cleartext Password over HTTP	High	3
SQL Injetion	High	12
Shell Injection	High	5
HTTP Trace Support Detected	Medium	1
Local Filesystem Paths Found	Medium	3
Possible XML Injection	Medium	1
Directory Listing Detected	Low	157
Form Password Field with Autocomplete Enabled	Low	3

Fuente: VEGA
Elaborado por: Castillo Jessica, 2016

- **SERVICIO WEB:** Bienestar Politécnico
- **URL:** http://bienestar.espoch.edu.ec/

Tabla 39-3 Vulnerabilidades después de la aplicación de la propuesta de solución de Bienestar Politécnico

Nombre	Grado	Número
HTTP Trace Support Detected	Medium	1
Local Filesystem Paths Found	Medium	1
Directory Listing Detected	Low	2

Fuente: VEGA
Elaborado por: Castillo Jessica, 2016

- **SERVICIO WEB:** Talento Humano
- **URL:** http://recursos.espoch.edu.ec/

Tabla 40-3 Vulnerabilidades después de la aplicación de la propuesta de solución de Talento Humano

Nombre	Grado	Numero
Cleartext Password over HTTP	High	1
Cross Site Scripting	High	7
URL Injection	Medium	3
Directory Listing Detected	Low	3
From Password Field with Autocomplete Enabled	Low	1

Fuente: VEGA
Elaborado por: Castillo Jessica, 2016

Tabla 41-3 Reducción de Vulnerabilidades

SERVICIO WEB Servicio de Educación Virtual	
Vulnerabilidades Eliminadas Altas	83
Vulnerabilidades por Eliminar Altas	20
Total de Vulnerabilidades Altas	103

Fuente: VEGA
Elaborado por: Castillo Jessica, 2016

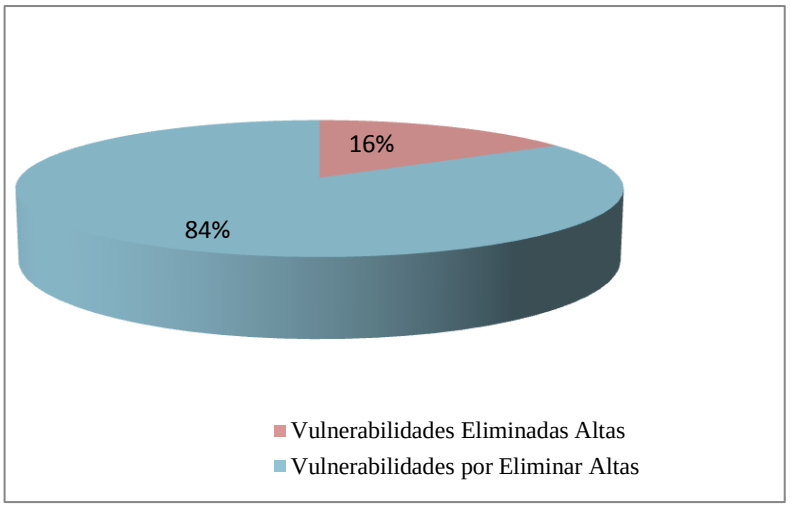


Gráfico 4-3 Reducción de Vulnerabilidades

Fuente: VEGA
Elaborado por: Castillo Jessica, 2016

ANÁLISIS:

Para medir la reducción de las vulnerabilidades se tomó en consideración el SERVICIO WEB: Educación Virtual para lo cual se determinó que del 100% de las vulnerabilidades eliminadas solo el 16% falta mitigar su riesgo es decir que el 84% fue controlado con la propuesta de implementación de un modelo de reducción de riesgos de seguridad informática en servicios web de la ESPOCH.

3.15. Identificación de Impactos

El objetivo de esta actividad es conocer el alcance del daño producido en el dominio (y por lo tanto sobre todos los activos que se encuentran en dicho dominio), como consecuencia de la materialización de las amenazas sobre los activos.

La identificación de los impactos o valoración de los dominios se desarrollara con repercusiones a las dimensiones de valoración que son (D) Disponibilidad, (I) Integridad, (C) Confiabilidad, (A) Autenticidad de la información.

Las dimensiones de valoración son atributos o características que hacen valioso el activo. Las dimensiones se utilizan para valorar las consecuencias de la materialización de una amenaza. La valoración que se recibe es una cierta dimensión, es la medida del perjuicio para la organización si los activos se ven dañados en dicha dimensión.

Para los criterios de valoración realizamos una escala que se encuentre dentro de los límites importantes de los criterios a valorarse.

La escala de valoración que se implementa se muestra en la siguiente tabla:

Tabla 42-3 Escala de criterios de valoración

Valor	Criterio
Alto	Daño grave al ESPOCH
Medio	Daño importante al ESPOCH
Bajo	Daño menos a la ESPOCH
Despreciable	Irrelevante a efectos prácticos

Elaborado por: Castillo Jessica, 2016

A continuación en la siguiente tabla se indica las cuatro dimensiones con sus criterios de valoración del análisis realizado con los técnicos de la DTIC.

Tabla 43-3 Identificación de Impactos

Dimensión	Valoración
Disponibilidad	ALTO
Integridad	ALTO
Confiabilidad	MEDIO
Autenticidad	ALTO

Fuente: Técnico DTIC
Elaborado por: Castillo Jessica, 2016

3.16. Identificación del Riego

En esta actividad, luego del análisis de los activos en los que se refiere a las amenazas, salvaguardas, existentes, vulnerabilidades e identificación de impactos, se identifica los activos y su nivel de riesgo existente. En la siguiente tabla se muestra la escala de daño para identificar los riesgos.

Tabla 44-3 Escala de Daño

VALOR		CRITERIO
7-10	Alto	Daño grave al ESPOCH
4-7	Medio	Daño importante al ESPOCH
1-4	Bajo	Daño menos a la ESPOCH
0-1	Despreciable	Irrelevante a efectos prácticos

Fuente: Alex Tacuri Técnico DTIC
Elaborado por: Castillo Jessica, 2016

La escala para identificar los riesgos es la siguiente:

- [5] Critico
- [4] Muy Alto
- [3] Alto
- [2] Medio
- [1] Bajo
- [0] Despreciable

Cada activo se encontrará con un nivel de riesgo y su valoración como resultado como calificación de la salvaguardas.

En la siguiente tabla se detalla los activos observados con su nivel del riesgo y el rango de valoración:

Tabla 45-3 Nivel de Riesgos

Nivel del Riesgo					
DESPRECIABLE [0]	BAJO [1]	MEDIO [2]	ALTO [3]	MUY ALTO [4]	CRITICO [5]

Fuente: Nivel de Riesgos
Elaborado por: Castillo Jessica, 2016

Tabla 46-3 Dimensión del Riesgo de Activos

Activos	Dimensiones			
	D	**I**	**C**	**A**
UPS	5	0	0	0
Planta de energía	5	0	0	0
Procesador 1 (Servidor 1)	4	3	2	4
Procesador 2 (Servidor 2)	4	3	2	4
Procesador 3 (Servidor 3)	4	3	2	4
Procesador 4 (Servidor 4)	4	3	2	4
Memoria 1 (Servidor 1)	4	4	3	4
Memoria 2 (Servidor 2)	4	4	3	4
Memoria 3 (Servidor 3)	4	4	3	4
Memoria 4 (Servidor 4)	4	4	3	4
Storage ()	4	5	2	5
Personal	3	1	3	0

Fuente: Alex Tacuri Técnico DTIC
Elaborado por: Castillo Jessica, 2016

3.17. Diseño del Modelo de Reducción de Riesgos RERISEIN

El desarrollo de un nuevo modelo de reducción de riesgos basado en la metodología Magerit, va a ir enfocado en el análisis por activo tecnológico, donde se

identificará las posibles amenazas o riesgos a los que están expuestos los elementos de trabajo de la organización.

Basado en este método se trabaja sobre inventario de los activos humanos y tecnológicos, así como: (servicios, hardware, software, soportes de información, personas); se desarrolla una encuesta para obtener el estado situacional de la organización y sus puntos negativos que apoyen a la evaluación del riesgo.

El modelo propuesto va a identificar los activos con obsolescencia tecnológica y llevarlos a cumplir un ciclo de evaluación de riesgos, apoyado en los modelos formales que ayudarán a identificar las amenazas de Activos y a determinar los riesgos frente a las amenazas.

Finalmente el modelo propone una forma estructurada para llevar a cabo una reducción de riesgos y a su vez debe ser capaz de crear protecciones y salvaguardas que apoyan al desarrollo del modelo.

FASE 1: IDENTIFICACIÓN DE ACTIVOS

OBJETIVO: Para establecer las directrices para el modelo de reducción de riesgos, es necesario analizar la seguridad informática con el fin de evaluar la situación actual de la organización.

En la Fase I, para la inicialización del modelo, es necesario identificar el tipo de activos tecnológicos que posee la organización.

Para realizar un Análisis de Riesgos, es sumamente importante identificar los activos que integran el Sistema de Información, estos activos pueden ser:

- Servicios de Red
- Aplicaciones Informáticas. (Software)
- Equipos Informáticos (Hardware)
- Soportes de Información
- Equipamiento Auxiliar
- Las Redes de Comunicación
- Las Instalaciones
- Talento Humano

En la tabla N°- 4.45, se muestra el formato del levantamiento de la información de los Activos.

Tabla 47-3 Formato de Levantamiento de Información de Activos

FICHA DE ACTIVOS				
Fecha	**Tipo de Activo**	**Descripción**	**Custodio**	**La pérdida o daño de este activo repercute a la organización (%)**

Elaborado por: Castillo Jessica, 2016

Las organizaciones deberán evaluar la continuidad del modelo en todas las fases de la evaluación de riesgos, cabe destacar que el trabajo más minucioso que se realiza y que llevará más tiempo es en esta fase.

FASE II: IDENTIFICACIÓN DE AMENZAS

OBJETIVO: Identificar las amenazas potenciales, a las que puede estar expuesta la organización.

En la Fase II, mediante encuestas o entrevistas realizadas a los técnicos que administran los servicios web se identifica las amenazas potenciales, a las que pueden estar expuestas la organización, esto va a facilitar la identificación de las amenazas que afectan a cada activo lo que permitirá tomar contramedidas eficaces para mitigar o contrarrestar las mismas.

Para poder identificar las amenazas se generó el siguiente formato, la misma que fue dirigida a los técnicos de la administración de los servicios web.

Tabla 48-3 Formato Identificar las Amenazas

NOMBRE DEL ACTIVO	AMENAZA	MARQUE (X) LA AMENZA QUE PODRIA DAÑAR SU ACTIVO
	Incendios forestales	
	Fuego	
	Caída de energía	
	Daño de agua	
	Pérdida de acceso	
	Fallas mecánicas	
	Epidemias	
	Materiales peligrosos	
	Problemas de transporte	
	Perdida de personal clave	
	Virus	
	Hacking	
	Perdida de datos	
	Fallas de hardware	
	Fallas de software	
	Fallas en la red	
	Fallas en las líneas telefónicas	
	Crisis financiera	
	Pérdida de suplidores	
	Fallas en equipos	
	Aspectos regulatorios	
	Mala publicidad	
	Motines	
	Protestas	
	Sabotaje	
	Violencia laboral	

Elaborado por: Castillo Jessica, 2016

FASE III: IDENTIFICACIÓN DE SALVAGUARDAS

OBJETIVO: Identificar las salvaguardas con las que se encuentran protegidos los activos de la organización para mitigar los riegos.

Es importante identificar los mecanismos de salvaguarda implantados en aquellos activos, describiendo las dimensiones de seguridad que estos ofrecen (Autenticidad, Confidencialidad, Integridad, Disponibilidad, (A-C-I-D).

Las salvaguardas pueden tener vulnerabilidades por lo que es necesario realizar pruebas y seguimiento de las mismas. La seguridad absoluta no existe, por lo que hay que aceptar riesgos.

Es importante considerar que las salvaguardas son medidas de mitigación que se da a conocer a la organización para que tome medidas de prevención, sin embargo no son obligatorias y se puede optar por tener un enfoque de mitigación de acuerdo a los resultados dados, para lo cual se ha generado un formato de encuestas que nos permitirá conocer las salvaguardas existentes para cada activo de la organización, las mismas que están dirigidas a los Técnicos que administran los servidores del Servicio Web.

Tabla 49-3 Identificación de Salvaguardas

Activos de Información	**Salvaguarda**	**Dimensiones que cubre las salvaguardas**			
		D	I	A	C

Elaborado por: Castillo Jessica, 2016

FASE IV: IDENTIFICACIÓN DE VULNERABILIDADES

OBJETIVO: Estudiar las características de nuestros activos para identificar puntos débiles o vulnerabilidades.

Las vulnerabilidades provocan debilidades en el sistema que pueden explotarse y dar lugar a consecuencias no deseadas.

En esta fase se debe seleccionar la herramienta tecnológica que permita determinar las vulnerabilidades de los servicios Web, Servicios en Línea, etc., es decir todo lo que está relacionado a los servicios vinculados con la internet.

A continuación se mencionan varias herramientas tecnológicas de vulnerabilidades que existen:

NESSUS: Escáner de vulnerabilidades que es desarrollado por Tenable Network Security. Es gratuito para uso personal en un entorno no empresarial.

NEXPOSE: NeXpose es un escáner de vulnerabilidades que verifica los controles que tiene en su lugar y se integra perfectamente con Metasploit, construido en el software de pruebas de penetración más impactante del mundo, para validar la explotabilidad de la vulnerabilidad, los controles del test de efectividad, e impulsar la recuperación efectiva de riesgo comprobado.

GRABBER: Es un escáner de aplicaciones web agradable que puede detectar muchas vulnerabilidades de seguridad en aplicaciones web. Se realiza exploraciones y nos muestra en donde está el error.

VEGA: Es otro escáner de vulnerabilidades web de código y de código abierto. Con esta herramienta, puede realizar pruebas de seguridad de una aplicación web. Esta herramienta está desarrollada en Java y ofrece un entorno basado en GUI. Está disponible para OS X, Linux y Windows.

ATAQUE ZED PROXY: También se conoce como ZAP. Esta herramienta es de código abierto y es desarrollado por AWASP. Está disponible para las plataformas de Windows, Unix / Linux y Macintosh. Personalmente, me gusta esta herramienta.

WAPITI: Es un escáner de vulnerabilidades web agradable que le permite auditar la seguridad de sus aplicaciones web. Se lleva a cabo pruebas de recuadro negro al escanear páginas web y la inyección de datos.

Se puede sugerir la utilización de la plataforma VEGA puesto que este nos proporciona información más detallada como el grado de vulnerabilidad, nos proporciona el tipo específico de vulnerabilidad que está afectando al sistema escaneado.

FASE V: IDENTIFICACIÓN DE IMPACTOS

OBJETIVO: Conocer el alcance del daño producido en el dominio, como consecuencia de la materialización de una amenaza sobre el activo.

El impacto, nos permite observar la gravedad de una agresión, es decir cómo se ve degradado nuestro activo y cómo esta agresión afecta las dimensiones de seguridad en la Organización para lo cual se realiza un levantamiento de información mediante encuestas a los encargados de administrar los servidores físicos que prestan servicios web los mismos que permitirán determinar si se llegó a materializar una amenaza y cuales seria su impacto en la organización, tomando en cuenta las dimensiones de cada activo.

Tabla 50-3 Formato para determinar Impactos

Activo	Dimensión	VALORACIÓN			
		Alto	Medio	Bajo	Despreciable
	Disponibilidad				
	Integridad				
	Confiabilidad				
	Autenticidad				

Elaborado por: Castillo Jessica, 2016

FASE VI: IDENTIFICACIÓN DEL NIVEL DE RIESGO

OBEJTIVO: Identificar y calcular los riesgos basados en la identificación de los activos.

Los riesgos se calculan de la combinación de los valores de los activos, que expresan el impacto de pérdidas por confiabilidad, integridad, disponibilidad y autenticidad y del

cálculo de la posibilidad de que amenazas y vulnerabilidades relacionadas se junten y causen un accidente.

Los niveles de riesgo calculados proveen un medio para poder priorizar los riesgos e identificar aquellos otros riesgos que son más problemáticos para la organización.

Tabla 51-3 Nivel de Riesgos

Nivel del Riesgo					
DESPRECIABLE	BAJO	MEDIO	ALTO	MUY ALTO	CRITICO
[0]	[1]	[2]	[3]	[4]	[5]

Elaborado por: Castillo Jessica, 2016

Tabla 52-3 Dimensión del Riesgo de Activos

Activos	Valor Dimensiones			
	D	I	C	A

Elaborado por: Castillo Jessica, 2016

Una vez calculado el riesgo es necesario iniciar un proceso de toma de decisiones con respecto a cómo se debe tratar el riesgo.

3.18. Comprobación de hipótesis

Para la comprobación de la Hipótesis General la propuesta de un modelo de reducción de riesgos informáticos mejorará el nivel de seguridad en los servicios web de la Espoch, se utilizó la estadística inferencial, se aplicó el Chi Cuadrado, luego de haber realizado un análisis de los resultados obtenidos de la vulnerabilidades de los servicios Web de la Escuela Superior Politécnica de Chimborazo se determinó la siguiente hipótesis nula H_o y la Alternativa H_1 que son:

La hipótesis Nula (H_o) La propuesta de un modelo de reducción de riesgos informáticos no mejorará el nivel de seguridad en los servicios web de la Espoch, con un nivel de significancia del 5% en la prueba de chi cuadrado X^2.

La hipótesis Alternativa de investigación (H_1) La propuesta de un modelo de reducción de riesgos informáticos si mejorará el nivel de seguridad en los servicios web de la Espoch, con un nivel de significancia del 5% en la prueba de chi cuadrado X^2.

Para comprobar la hipótesis se utilizó la herramienta Vega que es un escáner que permitió visualizar las vulnerabilidades de los servicios Web de la escuela Superior Politécnica de Chimborazo.

Donde se obtuvo los siguientes resultados preliminares que consideramos como valores Observados.

Tabla 53-3 Valores Observados

Valores Observados			
	Antes	**Después**	**Total**
Vulnerabilidades Altas	103	20	123
Vulnerabilidades Eliminadas	0	83	83
TOTAL	103	103	206

Fuente: VEGA
Elaborado por: Castillo Jessica, 2016

Los valores esperados se obtienen de la siguiente manera:

$$E(Si\ Antes) = \frac{103 * 123}{206} = 61.5$$

$$E(No\ Antes) = \frac{103 * 83}{206} = 41.5$$

$$E(Si\ Despues) = \frac{103 * 123}{206} = 61.5$$

$$E(No\ Después) = \frac{103 * 83}{206} = 41.5$$

Tabla 54-3 Valores Esperados

Valores Esperados			
	Antes	**Después**	**Total**
Vulnerabilidades Altas	61.5	61.5	123
Vulnerabilidades Eliminadas	41.5	41.5	83
TOTAL	103	103	206

Fuente: VEGA
Elaborado por: Castillo Jessica, 2016

Una vez obtenido los Valores Esperados el siguiente paso es determinar el valor de X^2 prueba Chi cuadrado prueba para lo cual se aplica la siguiente Ecuación:

$$X^2 = \sum_{i=1}^{r}\sum_{j=1}^{k}\frac{(O_{ij} - E_{ij})^2}{E_{ij}}$$

Dónde:

O_{ij} denota a las frecuencias observadas. Es el número de casos observados clasificados en la fila i de la columna j.

E_{ij} denota a las frecuencias esperadas o teóricas. Es el número de casos esperados correspondientes a cada fila y columna. Se puede definir como aquella frecuencia que se observaría si ambas variables fuesen independientes.

$$X^2 = \frac{(O_{11} - E_{11})^2}{E_{11}} + \frac{(O_{22} - E_{22})^2}{E_{22}} + \cdots \frac{(O_{rk} - E_{rk})^2}{E_{rk}}$$

$$X^2 = \frac{(103 - 61.5)^2}{61.5} + \frac{(0 - 41.5)^2}{41.5} + \frac{(20 - 61.5)^2}{61.5} + \frac{(83 - 41.5)^2}{41.5}$$

$$X^2 = 28{,}004 + 41{,}5 + 28.004 + 41.5$$

$$X^2 = 139.01$$

$$\boldsymbol{X^2 calculado = 139.01}$$

Ahora el siguiente paso es determinar el valor de chi cuadrado de la Tabla $X^2 tabla$ para lo cual se necesita los grados de libertad (*gl*) y el nivel de significancia que es del 5% es decir 0,05 para determinar los *gl* se utiliza la siguiente formula:

$$gl = (r - 1) * (k - 1)$$

Donde r=N° de columnas y k= N° de filas para este caso tenemos:

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

$$gl = 1$$

Por lo tanto buscando en la tabla de chi - cuadrado en el anexo N° 1 el valor para X^2 de la tabla:

$$\boldsymbol{X^2 tabla = 3,841}$$

$X^2 calculado = 139.01 < X^2 tabla = 3,84$ Se rechaza la hipótesis nula

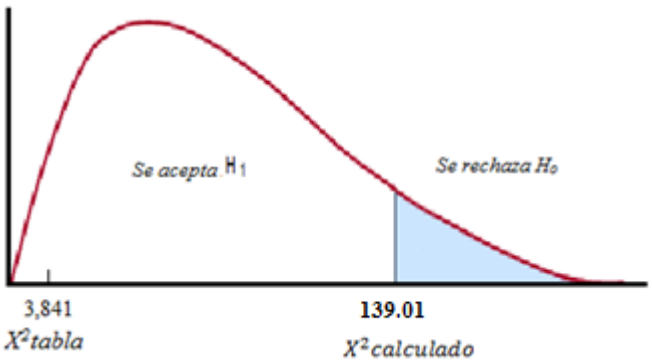


Gráfico 5-3 Distribución Chi Cuadrado Hipótesis General

Elaborado por: Castillo Jessica, 2016

ANÁLISIS:

De acuerdo a los datos obtenidos en el cálculo del X^2 de la tabla y X^2 calculado podemos llegar a la conclusión de que se rechaza la hipótesis nula y se acepta la hipótesis alternativa, es decir que la propuesta de un modelo de reducción de riesgos informáticos si mejorará el nivel de seguridad en los servicios web de la Espoch, con un nivel de significancia del 5% en la prueba de chi cuadrado X^2.

La comprobación de la hipótesis por el método del X^2 permite identificar que existe si la Escuela Superior Politécnica de Chimborazo implementa esta propuesta se lograra mitigar el riesgo informático logrando así mejorar la seguridad de los servicios Web.

CAPITULO IV

RESULTADOS Y DISCUSIÓN

Tomando como base fundamental el Diseño del Modelo de Reducción de Riesgos RERISEIN descrito en el capítulo IV constituimos la propuesta de implementación de un modelo para la reducción de Riesgos de seguridad informática en servicios web de la ESPOCH., con la finalidad de minimizar los riesgos en los servicios Web.

A continuación, se detallan la propuesta de soluciones encontradas en las vulnerabilidades, riesgos de la DTIC de la ESPOCH y de esta manera se resalta el uso de esta herramienta para objetivos instructivos de organizaciones que manejan sistemas informáticos y detengan la necesidad de mantener un nivel de control de su información.

4.1. Exposición de la propuesta para la reducción de riesgos

Este capítulo refleja el producto de la investigación, conforma una propuesta de herramienta metodológica de reducción de riesgos para los servicios web de la Escuela Superior Politécnica de Chimborazo.

La iniciativa de este trabajo nace con el afán de materializar el diseño de una propuesta que permita reducir el riesgo que mantiene los servicios web de la Escuela Superior Politécnica de Chimborazo con la finalidad de que los servicios que preste la institución sean confiables, seguros, de buena calidad y óptimos al momento de ser utilizados por la comunidad politécnica: estudiantes, docentes, empleados administrativos, etc.

Es importante que toda institución que utiliza servicios Web pueda contar con una herramienta metodológica que permita mitigar, las vulnerabilidades de los riegos de los servicios Web, la misma que permita conservar la privacidad y proteger de manera idónea la información de los beneficiarios de los servicios Web, además se hace imprescindible que el personal encargado de administrar estas herramientas mantengan

sus conocimientos actualizados mediante una capacitación continua sobre temas de seguridad informática actuales.

Otra debilidad que se encontró en el desarrollo de la investigación es que la Dirección de Tecnologías de la Información y Comunicación solo cuenta con un Sistema de Alimentación Ininterrumpida y con una Planta de Energía, los mismos que no tienen sistemas de BACKUP lo que provoca que se presenten fallas de energía, yéndose en contra de lo que tácitamente se expresa en las normal de seguridad internacionales.

Además es importante resaltar que en la entrevista realizada al administrador de la Dirección de Tecnologías de la Información y Comunicación el Ingeniero Alex Tacuri manifestó que solo disponen de un dispositivo de almacenamiento de información, el mismo que está en un 85% de su capacidad.

A continuación se detalla la propuesta para la reducción de riesgos para los servicios web de la Escuela Superior Politécnica de Chimborazo.

4.2. Propuesta para la reducción de riesgos para los servicios web de la escuela superior politécnica de Chimborazo

Tomando en consideración que la Escuela Superior Politécnica de Chimborazo se encuentra vulnerable en un 40% a los riesgos en sus servicios Web se ha diseñado una propuesta que brindara posibles soluciones para las diferentes vulnerabilidades encontradas.

En coordinación con los objetivos, estrategias y políticas de la Dirección de Tecnologías de la Información y Comunicación, las actividades de gestión de riesgos permiten elaborar un plan de seguridad que implantado y operado, satisfaga los objetivos propuestos con un nivel de riesgo inferior que el que obtuvimos en el análisis preliminar.

El plan de Seguridad propuesto que a continuación se detalla consta de:

- Propuesta de solución a las vulnerabilidades existentes en los Servicios Web de la Escuela Superior Politécnica de Chimborazo.

- Propuesta de un plan de Capacitación del Personal Técnico de la Dirección de Tecnologías de la Información y Comunicación.

4.2.1 Propuestas de Solución a las Vulnerabilidades

En esta fase se detallan cada una de las vulnerabilidades encontradas en cada uno de los servicios Web analizados con sus posibles soluciones.

- **SERVICIO WEB:** Escuela de Postgrado y Educación Continua
- **URL:** http://sisepec.espoch.edu.ec/

Tabla 55-4 Propuesta de Solución Escuela de Postgrado y Educación Continua

Vulnerabilidad	Propuesta de Solución
Page Fingerprint Differential Detected	1. Para evitar este tipo de vulnerabilidad, el desarrollador debe predeterminar el camino de cualquier recurso del sistema de archivos que tiene una trayectoria compuesta de entrada suministrada externamente y luego realizar una comprobación de autorización previa para el acceso. 2. Cuando se desarrolle en PHP, Perl y Python se debe utilizar la función realpath (), cuando se utilice aplicaciones ASP.NET se debe utilizar la función GetFullPath (), cuando se utiliza en código Java se utilizar la función getCanonicalPath () estas funciones devuelven la ruta predeterminada así se evita este tipo de vulnerabilidad. 3. Protección adicional contra el acceso no autorizado al sistema de ficheros de recursos se puede obtener mediante el uso de chroot () o mecanismos similares para limitar el acceso del sistema de archivos para el proceso de servidor de aplicaciones web y http, aunque esto puede ser difícil de manejar.

Fuente: Análisis de los Servicios Web realizados con VEGA
Elaborado por: Castillo Jessica, 2016

- **SERVICIO WEB:** OASIS
- **URL:** http://academicoseg.espoch.edu.ec/

Tabla 56-3 Propuesta de Solución OASIS

Vulnerabilidad	Propuesta de Solución
Cleartext Password over HTTP	1. Las contraseñas nunca deben ser enviadas a través de texto plano. 2. Elaborar contraseñas fuertes y cifrarlas. 3. Una contraseña fuerte debe contener mínimo 8 caracteres: 2 caracteres especiales, 2 números, 2 letras mayúsculas y 2 minúsculas.
SQL Injection	1. La mejor defensa contra las vulnerabilidades de SQL Injection es utilizar instrucciones con parámetros. 2. Las variables de tipos de cadenas deben ser filtrados, y tipos numéricos deben ser evaluados para verificar que son válidos.(Ejemplo ‘ , “) 3. El uso de procedimientos almacenados puede simplificar consultas complejas y permitir la configuración de control de acceso más estricto. 4. Configuración de los controles de acceso de base de datos puede limitar el impacto de las vulnerabilidades explotadas.
Local Filesystem Paths Found	1. Cuando se obtenga una salida de error que contiene información confidencial, como rutas de sistema absolutos no debería ser enviada a los clientes remotos en servidores de producción. 2. Esta salida debe ser enviada a otra log de salida, como un registro de errores.
From Password Field with Autocomplete Enable	1. El valor del atributo de autocomplete en el formulario debe tener el valor "off". 2. No generar autocomplete.

Fuente: Análisis de los Servicios Web realizados con VEGA
Elaborado por: Castillo Jessica, 2016

- **SERVICIO WEB:** Evaluación Institucional
- **URL:** http**:**//evaluacion.espoch.edu.ec/

Tabla 57-4 Propuesta de Solución Evaluación Institucional

Vulnerabilidad	Propuesta de Solución
Shell Injection	1. Los desarrolladores deben examinar el código correspondiente a la página en detalle para determinar si existe la vulnerabilidad. 2. La ejecución de comandos de sistema a través de un intérprete de comandos, como por ejemplo con el system (), debe ser evitado. 3. El desarrollador debe validar las entradas antes de que se pasa al intérprete.
SQL Injetion	1. La mejor defensa contra las vulnerabilidades de SQL Injection es utilizar instrucciones con parámetros. 2. Las variables de tipo cadena, caracteres especiales deben ser filtrados, y tipos numéricos deben ser evaluados para verificar que son válidos. 3. El uso de procedimientos almacenados puede simplificar consultas complejas y permitir la configuración de control de acceso más estricto. 4. Configuración de los controles de acceso de base de datos puede limitar el impacto de las vulnerabilidades explotadas. 5. Esta es una estrategia atenuante que puede emplearse en entornos en los que el código no es modificable.
HTTP Trace Support Detected	1. Para los servidores basados en Apache, la función TraceEnable () se puede utilizar para desactivar el soporte para HTTP TRACE. 2. Para los servidores basados en IIS, la función EnableTraceMethod () se puede utilizar para desactivar el soporte para HTTP TRACE.
Local Filesystem Paths Found	1. Cuando se obtenga una salida de error que contiene información confidencial, como rutas de sistema absolutos no debería ser enviada a los clientes remotos en servidores de producción. 2. Esta salida debe ser enviada a otra log de salida, como un registro de errores.

PHP Error Detected	1. El manual de PHP recomienda la desactivación de "display_errors" en servidores expuestos a Internet. Para PHP 5.2.4 y sus versiones, el parámetro del archivo de configuración "php.ini" se debe establecer en "stderr" (flujo de salida de error), en lugar de "stdout" (flujo de salida enviado a los clientes). Para versiones anteriores, "display_errors" es un tipo booleano, y se debe configurar como "False" para desactivarlo. El ajuste también se puede desactivar en tiempo de ejecución usando ini_set () desde un script PHP.
Possible XML Injection	1. Los desarrolladores deben investigar el código para verificar manualmente que existe una vulnerabilidad de XML injection. 2. Caracteres que se pueden interpretar como XML deben ser filtrados como por ejemplo >, <, ‘ , ”, etc.
Directory Listing Detected	1. Para Apache, realice una de las siguientes opciones: añadir "IndexIgnore " para archivo .htaccess del directorio, o bien eliminar "Índices" de la línea "Opciones Todos los índices FollowSymLinks MultiView" en su archivo de configuración de Apache.

Fuente: Análisis de los Servicios Web realizados con VEGA
Elaborado por: Castillo Jessica, 2016

- **SERVICIO WEB:** Talento Humano
- **URL**: http://recursos.espoch.edu.ec/

Tabla 58-4 Propuesta de Solución Talento Humano

Vulnerabilidad	Propuesta de Solución
Cleartext Password over HTTP	1. Las contraseñas nunca deben ser enviadas a través de texto plano. 2. Elaborar contraseñas fuertes y cifrarlas. 3. Una contraseña fuerte debe contener mínimo 8 caracteres: 2 caracteres especiales, 2 números, 2 letras mayúsculas y 2 minúsculas.
Cross Site Scripting	1. No confiar nunca en datos que se obtenga de los usuarios o de cualquier Fuente de datos externa. 2. Filtrar datos poco confiables que son generados por el

	cliente. 3. Esta regla es la única que tenemos que seguir para prevenir los ataques XSS. Para evitar ataques XSS, se debe llevar a cabo la validación de datos, el saneamiento y escapar lo que se va a mostrar.
Page Fingerprint Differential Detected	1. Para evitar este tipo de vulnerabilidad, el desarrollador debe predeterminar el camino de cualquier recurso del sistema de archivos que tiene una trayectoria compuesta de entrada suministrada externamente y luego realizar una comprobación de autorización previa para el acceso. 2. Cuando se desarrolle en PHP, Perl y Python se debe utilizar la función realpath (), cuando se utilice aplicaciones ASP.NET se debe utilizar la función GetFullPath (), cuando se utiliza en código Java se utilizar la función getCanonicalPath () estas funciones devuelven la ruta predeterminada así se evita este tipo de vulnerabilidad. 3. Protección adicional contra el acceso no autorizado al sistema de ficheros de recursos se puede obtener mediante el uso de chroot () o mecanismos similares para limitar el acceso del sistema de archivos para el proceso de servidor de aplicaciones web y http, aunque esto puede ser difícil de manejar.
URL Injection	1. El desarrollador debe examinar la etiqueta y determinar las posibles implicaciones de seguridad de la utilización de un URI suministrado de forma remota.
Directory Listing Detected	1. Para Apache, realice una de las siguientes opciones: añadir "IndexIgnore" para archivo .htaccess del directorio, o bien eliminar "Índices" de la línea "Opciones Todos los índices FollowSymLinks MultiView" en su archivo de configuración de Apache.
From Password Field with Autocomplete Enabled	1. El valor del atributo de autocomplete en el formulario debe tener el valor "off". 2. No generar autocomplete.

Fuente: Análisis de los Servicios Web realizados con VEGA
Elaborado por: Castillo Jessica, 2016

- **SERVICIO WEB:** Educación Virtual
- **URL: http**://elearning.espoch.edu.ec/

Tabla 59-4 Propuesta de Solución Educación Virtual

Vulnerabilidad	Propuesta de Solución
Cleartext Password over HTTP	1. Las contraseñas nunca deben ser enviadas a través de texto plano. 2. Elaborar contraseñas fuertes y cifrarlas. 3. Una contraseña fuerte debe contener mínimo 8 caracteres: 2 caracteres especiales, 2 números, 2 letras mayúsculas y 2 minúsculas.
SQL Injetion	1. La mejor defensa contra las vulnerabilidades de SQL Injection es utilizar instrucciones con parámetros. 2. Las variables de tipo cadena, caracteres especiales deben ser filtrados, y tipos numéricos deben ser evaluados para verificar que son válidos.(Ej ‘ , “) 3. El uso de procedimientos almacenados puede simplificar consultas complejas y permitir la configuración de control de acceso más estricto. 4. Configuración de los controles de acceso de base de datos puede limitar el impacto de las vulnerabilidades explotadas. 5. Esta es una estrategia atenuante que puede emplearse en entornos en los que el código no es modificable
Shell Injection	1. Los desarrolladores deben examinar el código correspondiente a la página en detalle para determinar si existe la vulnerabilidad. 2. La ejecución de comandos de sistema a través de un intérprete de comandos, como por ejemplo con el system (), debe ser evitado. 3. El desarrollador debe validar las entradas antes de que se pasa al intérprete.
HTTP Trace Support Detected	1. Para los servidores basados en Apache, la función TraceEnable () se puede utilizar para desactivar el soporte para HTTP TRACE.

	2. Para los servidores basados en IIS, la función EnableTraceMethod () se puede utilizar para desactivar el soporte para HTTP TRACE.
Local Filesystem Paths Found	1. Cuando se obtenga una salida de error que contiene información confidencial, como rutas de sistema absolutos no debería ser enviada a los clientes remotos en servidores de producción. 2. Esta salida debe ser enviada a otra log de salida, como un registro de errores.
Possible XML Injection	1. Los desarrolladores deben investigar el código para verificar manualmente que existe una vulnerabilidad de XML injection. 2. Caracteres que se pueden interpretar como XML deben ser filtrados como por ejemplo >, <, ‘ , ”, etc.
Directory Listing Detected	1. Para Apache, realice una de las siguientes opciones: añadir "IndexIgnore" para archivo .htaccess del directorio, o bien eliminar "Índices" de la línea "Opciones Todos los índices FollowSymLinks MultiView" en su archivo de configuración de Apache.
Form Password Field with Autocomplete Enabled	1. El valor del atributo de autocomplete en el formulario debe tener el valor "off". 2. No generar autocomplete.

Fuente: Análisis de los Servicios Web realizados con VEGA
Elaborado por: Castillo Jessica, 2016

- **SERVICIO WEB:** Biblioteca
- **URL:** http://bibliotecas.espoch.edu.ec/

Tabla 60-4 Propuesta de Solución Biblioteca

Vulnerabilidad	Propuesta de Solución
Cleartext Password over HTTP	1. Las contraseñas nunca deben ser enviadas a través de texto plano. 2. Elaborar contraseñas fuertes y cifrarlas. 3. Una contraseña fuerte debe contener mínimo 8 caracteres: 2 caracteres especiales, 2 números, 2 letras mayúsculas y 2 minúsculas.

Cross Site Scripting	1. No confiar nunca en datos que se obtenga de los usuarios o de cualquier Fuente de datos externa. 2. Filtrar datos poco confiables que son generados por el cliente. 3. Esta regla es la única que tenemos que seguir para prevenir los ataques XSS. Para evitar ataques XSS, se debe llevar a cabo la validación de datos, el saneamiento y escapar lo que se va a mostrar.
SQL Injection	1. La mejor defensa contra las vulnerabilidades de SQL Injection es utilizar instrucciones con parámetros. 2. Las variables de tipo cadena, caracteres especiales deben ser filtrados, y tipos numéricos deben ser evaluados para verificar que son válidos. 3. El uso de procedimientos almacenados puede simplificar consultas complejas y permitir la configuración de control de acceso más estricto. 4. Configuración de los controles de acceso de base de datos puede limitar el impacto de las vulnerabilidades explotadas. 5. Esta es una estrategia atenuante que puede emplearse en entornos en los que el código no es modificable.
Local Filesystem Paths Found	1. Cuando se obtenga una salida de error que contiene información confidencial, como rutas de sistema absolutos no debería ser enviada a los clientes remotos en servidores de producción. 2. Esta salida debe ser enviada a otra log de salida, como un registro de errores.
Form Password Field with Autocomplete Enabled	1. El valor del atributo de autocomplete en el formulario debe tener el valor "off". 2. No generar autocomplete.

Fuente: Análisis de los Servicios Web realizados con VEGA
Elaborado por: Castillo Jessica, 2016

- **SERVICIO WEB**: Médico
- **URL:** http://medicina.espoch.edu.ec/

Tabla 61-4 Propuesta de Solución Médico

Vulnerabilidad	Propuesta de Solución
Local Filesystem Paths Found	1. Cuando se obtenga una salida de error que contiene información confidencial, como rutas de sistema absolutos no debería ser enviada a los clientes remotos en servidores de producción. 2. Esta salida debe ser enviada a otra log de salida, como un registro de errores.
Possible Source Code Disclosure	1. Los desarrolladores deben verificar si es código Fuente de la aplicación si no lo es el material debe ser removido.

Fuente: Análisis de los Servicios Web realizados con VEGA
Elaborado por: Castillo Jessica, 2016

- **SERVICIO WEB:** Bienestar Politécnico
- **URL: http://**bienestar.espoch.edu.ec/

Tabla 62-4 Propuesta de Solución Bienestar Politécnico

Vulnerabilidad	Propuesta de Solución
HTTP Trace Support Detected	1. Para los servidores basados en Apache, la función TraceEnable () se puede utilizar para desactivar el soporte para HTTP TRACE. 2. Para los servidores basados en IIS, la función EnableTraceMethod () se puede utilizar para desactivar el soporte para HTTP TRACE.
Local Filesystem Paths Found	1. Cuando se obtenga una salida de error que contiene información confidencial, como rutas de sistema absolutos no debería ser enviada a los clientes remotos en servidores de producción. 2. Esta salida debe ser enviada a otra log de salida, como un registro de errores.
Directory Listing Detected	1. Para Apache, realice una de las siguientes opciones: añadir "IndexIgnore" para archivo .htaccess del directorio, o bien eliminar "Índices" de la línea "Opciones Todos los 2. índices FollowSymLinks MultiView" en su archivo

	de configuración de Apache.
Email Addresses Found	1. Las direcciones de correo electrónico incrustados en el contenido proporcionado por el usuario deben ser filtrados para evitar la divulgación no intencional. 2. No es recomendable mostrar las librerías de javascript ya que el servidor automáticamente puede mostrar direcciones de correo.

Fuente: Análisis de los Servicios Web realizados con VEGA
Elaborado por: Castillo Jessica, 2016

- **SERVICIO WEB:** Bolsa de Empleos
- **URL:** http://empleos.espoch.edu.ec/

Tabla 63-4 Propuesta de Solución Bolsa de Empleos

Vulnerabilidad	Propuesta de Solución
Cleartext Password over HTTP	1. Las contraseñas nunca deben ser enviadas a través de texto plano. 2. Elaborar contraseñas fuertes y cifrarlas. 3. Una contraseña fuerte debe contener mínimo 8 caracteres: 2 caracteres especiales, 2 números, 2 letras mayúsculas y 2 minúsculas.
Local Filesystem Paths Found	1. Cuando se obtenga una salida de error que contiene información confidencial, como rutas de sistema absolutos no debería ser enviada a los clientes remotos en servidores de producción. 2. Esta salida debe ser enviada a otra log de salida, como un registro de errores.
Form Password Field with Autocomplete Enabled	1. El valor del atributo de autocomplete en el formulario debe tener el valor "off". 2. No generar autocomplete.

Fuente: Análisis de los Servicios Web realizados con VEGA
Elaborado por: Castillo Jessica, 2016

- **SERVICIO WEB:** Passport
- **URL:** http://passportsignin.espoch.edu.ec/

Tabla 64-4 Propuesta de Solución Resumen de vulnerabilidades Passport

Vulnerabilidad	Propuesta de Solución
Cleartext Password over HTTP	1. Las contraseñas nunca deben ser enviadas a través de texto plano. 2. Elaborar contraseñas fuertes y cifrarlas. 3. Una contraseña fuerte debe contener mínimo 8 caracteres: 2 caracteres especiales, 2 números, 2 letras mayúsculas y 2 minúsculas.
Page Fingerprint Differential Detected	1. Para evitar este tipo de vulnerabilidad, el desarrollador debe predeterminar el camino de cualquier recurso del sistema de archivos que tiene una trayectoria compuesta de entrada suministrada externamente y luego realizar una comprobación de autorización previa para el acceso. 2. Cuando se desarrolle en PHP, Perl y Python se debe utilizar la función realpath (), cuando se utilice aplicaciones ASP.NET se debe utilizar la función GetFullPath (), cuando se utiliza en código Java se utilizar la función getCanonicalPath () estas funciones devuelven la ruta predeterminada así se evita este tipo de vulnerabilidad. 3. Protección adicional contra el acceso no autorizado al sistema de ficheros de recursos se puede obtener mediante el uso de chroot () o mecanismos similares para limitar el acceso del sistema de archivos para el proceso de servidor de aplicaciones web y http, aunque esto puede ser difícil de manejar
ASP/ASPX Error Detected	1. Desactive los mensajes de error para los usuarios remotos. 2. Configurar el servidor y el marco para mostrar los mensajes de error de seguridad que no incluyen información sensible, o enviar a otra página que no sea la que es por defecto.
Form Password Field with Autocomplete Enabled	1. El valor del atributo de autocomplete en el formulario debe tener el valor "off". 2. No generar autocomplete.

Fuente: Análisis de los Servicios Web realizados con VEGA
Elaborado por: Castillo Jessica, 2016

4.2.2 Propuesta de un Plan de Capacitación para el personal técnico de la Dirección de Tecnologías de la Información y Comunicación (DTIC) de la Escuela Superior Politécnica de Chimborazo.

En la actualidad para toda institución contar con un personal capacitado es fundamental puesto que es una fortaleza que se debe aprovechar para el crecimiento institucional.

La capacitación es una actividad sistemática, planificada y permanente cuyo propósito general es preparar, desarrollar e integrar al factor humano al proceso productivo, mediante la entrega de conocimientos, desarrollo de habilidades y actitudes necesarias para el mejor desempeño del personal técnico en las funciones que desempeñan y a su vez adaptarlos a las exigencias cambiantes del entorno**.**

En el análisis preliminar se evidenció la falta de actualización y capacitación que poseen los empleados que administran la Dirección de Tecnologías de la Información y Comunicación en los diferentes procesos internos que cumplen:

Tomando en consideración las debilidades que se presentan el personal técnico por la falta de capacitación se ha desarrollado una propuesta de plan de capacitación la misma que estará enfocada de acuerda a las necesidades, competencias y los cambios que se presentan en el entorno.

Tabla 65-4 Acción Formativa DTIC

NOMBRE	HORAS	GRUPOS	TIPO DE FORMACIÓN
SEGURIDAD A NIVEL DE APLICACIONES	40	1	**ESPECÍFICA**
COLECTIVO	**CAUSA QUE ORIGINAN LA FORMACIÓN**		
Dirección de Tecnologías de la Información y Comunicación	Falta de conocimientos en las técnicas requeridas para un adecuado desempeño en los procesos internos que desarrollan en su lugar de trabajo.		

OBJETIVOS DE LA CAPACITACIÓN

- Contar con los conocimientos tecnológicos y prácticos para contrarrestar el riesgo continuo de las vulnerabilidades en los sistemas informáticos de las empresas, y la actividad de personas mal intencionadas que explotan las vulnerabilidades y debilidades de los sistemas informático

CONOCIMIENTOS DE LA FORMACIÓN

- Podrá planear y administrar sistemas seguros de la información con el objetivo de precautelar la integridad de la información.
- Tener una óptica clara respecto a lo que es proteger y defender toda la información almacenada en los sistemas informáticos de la empresa.
- Detectar y contrarrestar a tiempo todos los tipos de ataques a la seguridad de la información defendiendo a los sistemas de ataques como virus, troyanos, gusanos, etc.
- Conocerá los sistemas de defensa más sofisticados y de última generación para la detección y prevención de intrusos a los sistemas informáticos

CONTENIDO DE LA CAPACITACIÓN

- Conceptos de Aplicaciones. Conceptos de Base de Datos,
- Conceptos de Sistemas Operativos
- Conceptos de Programación Orientada a Objetos
- Conceptos de Java
- Vulnerabilidades, Amenazas.
- Seguridad en Base de Datos, Controles de Desarrollo de Sistemas.

OBSERVACIÓN	PRESUPUESTO	
	Instructor	1100
	Materiales	300
	Refrigerios	120
	Total	**1520**

Fuente: Información de la Escuela Superior Politécnica de Chimborazo.
Elaborado por: Castillo Jessica, 2016

Tabla 66-4 Acción Formativa DTIC

NOMBRE	HORAS	GRUPOS	TIPO DE FORMACIÓN
CONTROL DE ATAQUES	40	1	**GENERAL**
COLECTIVO	**CAUSA QUE ORIGINAN LA FORMACIÓN**		
Dirección de Tecnologías de la Información y Comunicación	Falta de conocimientos en las técnicas requeridas para un adecuado control de ataques.		

OBJETIVOS DE LA CAPACITACIÓN

- Contar con los conocimientos tecnológicos y prácticos para mitigar un ataque informático y controlar ,los mismos con la finalidad de detectar posibles fallas dentro del software, en el hardware, e incluso, en las persona s que forman parte de un ambiente informático; a fin de obtener un beneficio, por lo general de índole económico, causando un efecto negativo en la seguridad del sistema, que luego repercute directamente en los activos de la institución.

CONOCIMIENTOS DE LA FORMACIÓN

- Podrá identifique cuál es y dónde está la información más crítica o sensible para la institución. Esto le permitirá enfocarse en asegurar que la información crítica o sensible siempre tenga la más alta prioridad frente a cualquier actividad sospechosa.
- Analizar las amenazas de los últimos ataques contra las mayores debilidades en el ambiente. Si lo hace, le ayudará a identificar dónde empezar la defensa y/o la limpieza.
- Tener una óptica clara respecto a lo que es proteger y defender toda la información almacenada en los sistemas informáticos de la empresa.
- Implementar la autenticación con privilegios mínimos y control de acceso. Es decir, no se debe dar a los usuarios acceso a recursos que no utilizan. Esto ayudará a reducir el daño del siguiente ataque APT.
- Asegurarse de parchar todo. Especialmente, aquellos complementos de los exploradores populares.
- Implementar el control de aplicaciones de listas blancas.

CONTENIDO DE LA CAPACITACIÓN

- Sistema Detección de Intrusos.
- IDS basado en conocimiento
- IDS basado en comportamiento.
- IDS Host, IDS Red. IDS pasivo, IDS reactivo.
- Firewalls, Categorías de Firewalls, Firewall Packet-filter (Screening Router). Firewall Capa Aplicación (Proxy), Firewall Stateful Inspection, Firewall Dynamic packet-filtering

OBSERVACIÓN	PRESUPUESTO	
	Instructor	1200
	Materiales	400
	Refrigerios	120
	Total	**1520**

Fuente: Información de la Escuela Superior Politécnica de Chimborazo.
Elaborado por: Castillo Jessica, 2016

Tabla 67-4 Acción Formativa DTIC

NOMBRE	HORAS	GRUPOS	TIPO DE FORMACIÓN
PREVENCIÓN DE RIESGOS TECNOLÓGICOS	40	1	**ESPECÍFICA**
COLECTIVO	**CAUSA QUE ORIGINAN LA FORMACIÓN**		
Dirección de Tecnologías de la Información y Comunicación	Falta de utilización la seguridad informática como herramienta para mitigar riesgos de fuga de información sensible, robo de identidad o actividades ilícitas.		

OBJETIVOS DE LA CAPACITACIÓN

- Contar con los conocimientos para la toma de decisiones cuando se trata de salvaguardar la información sensible y datos confidenciales de personas y grupos vulnerables

CONOCIMIENTOS DE LA FORMACIÓN

- Utilizar la seguridad informática como herramienta para mitigar riesgos de fuga de
- información sensible, robo de identidad o actividades ilícitas.
- Conocer la legislación vigente y la responsabilidad que conlleva para el usuario y la
- empresa el robo de información sensible.
- Familiarizarse con los posibles tipos de ataques, técnicas maliciosas que los intrusos
- informáticos pueden utilizar para introducirse en ordenadores.
- Aprender desde un HackLab las técnicas utilizadas por los Crakers cuando planean e
- intentan un ataque a páginas Web, servidores de correo, bases de datos y sistemas de
- redes de ordenadores, así como las contramedidas necesarias para abortar dichos
- ataques.
- Adquirir los conocimientos para la toma de decisiones cuando se trata de salvaguardar la información sensible y datos confidenciales de personas, la institución o empresa a la que pertenecen. Aprenderán sobre seguridad y penetración a redes inalámbricas Wifi.
- Distintas herramientas de seguridad de que disponen los usuarios, tales como antivirus, vacunas, antimalware, pruebas de seguridad, etc.
- Saber configurar la privacidad y seguridad en las principales redes sociales

CONTENIDO DE LA CAPACITACIÓN

- Introducción al hacking ético, Fases de un ataque
- Hacker VS Cracker
- Estafas y ataques: Ingeniería social, Phishing, robo de contraseñas, keylogger, enlaces maliciosos, metadatos, redes envenenadas, xploit.
- Malware: Virus, troyanos, spam, gusanos, etc.
- Contramedidas, Contraseñas seguras; Principales consejos de seguridad.
- Responsabilidad legal de los usuarios y empresas en el robo de información.
- Uso de herramientas de seguridad para usuarios y prueba Eicar.
- Políticas de seguridad lógica, Botnet y ordenadores zombis.
- Demostraciones prácticas de distintos ataques en laboratorio Hacker

OBSERVACIÓN	PRESUPUESTO	
	Instructor	1100
	Materiales	300
	Refrigerios	120
	Total	**1520**

Fuente: Información de la Escuela Superior Politécnica de Chimborazo.
Elaborado por: Castillo Jessica, 2016

CONCLUSIONES

- La aplicación de la propuesta de implementación de un modelo para la reducción de riesgos de seguridad informática en servicios web de la Escuela Superior politécnica de Chimborazo permitió reducir en un 84% de las vulnerabilidades altas encontradas teniendo en cuenta que se debe llegar a la máxima mitigación de riesgos para así llegar al nivel más alto de seguridad.

- Como total de vulnerabilidades se encontraron 416 vulnerabilidades altas, 175 vulnerabilidades medias y 1457 vulnerabilidades bajas.

- Las tres vulnerabilidades más frecuentes: SQL Injection, PHP Error Detected y Directory Listing Detected.

- El personal técnico de la Dirección de Tecnologías de la Información y Comunicación de la Escuela Superior Politécnica de Chimborazo no dispone de conocimientos técnicos avanzados lo que es una vulnerabilidad más en el servicio.

- A pesar de que existen un sin número de Metodologías de reducción de riesgos se analizaron MEGERIT y OCTAVE que son las más utilizadas a nivel de Latinoamérica.

- Se utilizó la herramienta VEGA ya que es un escáner de vulnerabilidades de páginas web gratuito.

RECOMENDACIONES

- Se recomienda aplicar el Plan de Mejoras propuesto para minimizar los riesgos.

- Se recomienda aplicar el Plan de Capacitación propuesto al personal técnico de la Dirección de Tecnologías de la Información y Comunicación de la Escuela Superior Politécnica de Chimborazo para que puedan minimizar los riegos y vulnerabilidades en los servicios analizados.

- Se recomienda que el análisis de vulnerabilidades en los servicios web utilizando la herramienta VEGA se lo realice de manera trimestral para verificar que el Plan propuesto si reduce los riesgos.

- Se recomienda como trabajos futuros analizar las vulnerabilidades del servicio IP, Redes inalámbricas, correo electrónico, etc de la Escuela Superior Politécnica de Chimborazo.

BIBLIOGRAFÍA

AGUILAR, J. E. (2010). Toerías del comporatamiento organizacional. México: asociacion Oaxaqueña de Psicología A.C. (fecha de consulta 2/12/2015).

AMENAZAS INFORMATICAS Y SEGURIDAD DE LA INFORMACIÓN. (2012). Obtenido de Amenazas Informaticas y Seguridad de la Información: (fecha de consulta 12/12/2015) dialnet.unirioja.es/descarga/articulo/3311853.pdf

ERB, M. (2014). Gestión de Riesgo en la Seguridad Informática. Obtenido de Gestión de Riesgo en la Seguridad Informática, (fecha de consulta 12/09/2015), https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/

GESTIÓN DE RIESGO EN LA SEGURIDAD INFORMÁTICA. (2014). Obtenido de Amenazas y Vulnerabilidades, (fecha de consulta 10/08/2015) https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/

ISO 27000.es. (2013). Obtenido de El portal de ISO 27001 en Español: (fecha de consulta 12/12/2015) http://www.iso27000.es/sgsi.html

IVANCEVICH, John M; **KONOPASKE**, Robert; **MATTESON**, Michael T. (2006). Comportamiento Organizacional. México: MacGraw Hill Interamericana.

KWAN, T., & Leung, H. (2010). A Risk Management Methodology for Project Risk Dependencies. IEEE Transactions on Software Engineering, (págs. 635-648) (fecha de consulta 12/1/2015).

LALANNE, V., MUNIER, M., & GABILLON, A. (2013). Information Security Risk Management in a World of Services. International Conference on Social Computing (SocialCom), (págs. 586-593) (fecha de consulta 2/12/2015).

LEUNG, Kwan, T. W., & Hareton, K. (2011). A Risk Management Methodology for Project Risk Dependencies. Software Engineering, IEEE Transactions, 635-648(fecha de consulta 12/12/2015) (fecha de consulta 12/12/2015).

MÉNDEZ ÁLVAREZ, C. E. (2009). Tecnologias y herramientas de gestion. Bogotá: Editorial Universidad del Rosario.

METODOLOGIAS DE ANALISIS DE RIESGOS: MAGERIT y OCTAVE. (2011). Obtenido de Metodologias de Analisis de Riesgos: MAGERIT y OCTAVE, (fecha de consulta 12/10/2015), https://seguridadenlasredes.wordpress.com/2010/08/12

MIRANDA GONZALEZ, F., Chamorro Mera, A., & Rubio Lacoba, S. (2007). Introducción a la gestión de la calidad. Madrid: Delta Publicaciones.

MÜNCH, L. (2010). Administración gestión organizacional, enfoques y proceso administrativo. México : Pearson Educación de México S.A. de C.V.

OCTAVE VSR CRAMM APOYO ISO 270001. (2011). Obtenido de https://www.clubensayos.com/Tecnolog%C3%ADa/OCTAVE-VRS-CRAMM-APOYO-ISO-270001/11555.html(fecha de consulta 12/12/2015)

PRAT CANET, J. (2008). Benchmarking: Un método para aprender de las mejores empresa. México: Granica. (fecha de consulta 12/12/2015)

QUINN, F., THOMPSON, S., & MICHAEL, M. (2009). Un modelo operativo de competencias. España: Diaz de Santos S.A. (fecha de consulta 12/02/2016)

SERVICIOS WEB. (2014). Obtenido de Beneficios de los servicios web, (fecha de consulta 12/02/2016), :

http://www.eumed.net/tesis-doctorales/2007/cavl/Beneficios%20de%20los%20servicios%20Web.htm

SOFTWARE ENGINEERING INSTITUTE. (2013). Obtenido de Octave, (fecha de consulta 02/09/2015), : http://www.cert.org/resilience/products-services/octave/

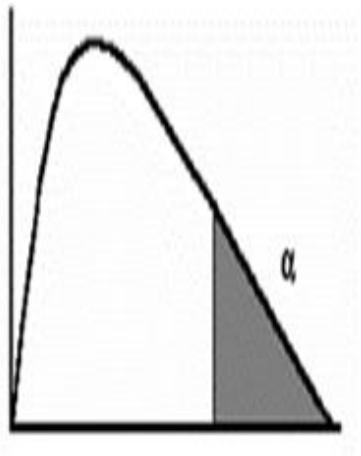
VADILLO, S. (2009). La Adminitraciónde Remuneraciones. México: Limusa S.A. de C.V. Grupo Noriega. (fecha de consulta 10/12/2015)

VARELA JUAREZ, R. (2009). Administración de la compensación: sueldos, salarios y prestaciones . México: Perason Educación (fecha de consulta 12/12/2015).

ANEXOS

ANEXOS A:

CHI CUADRADO

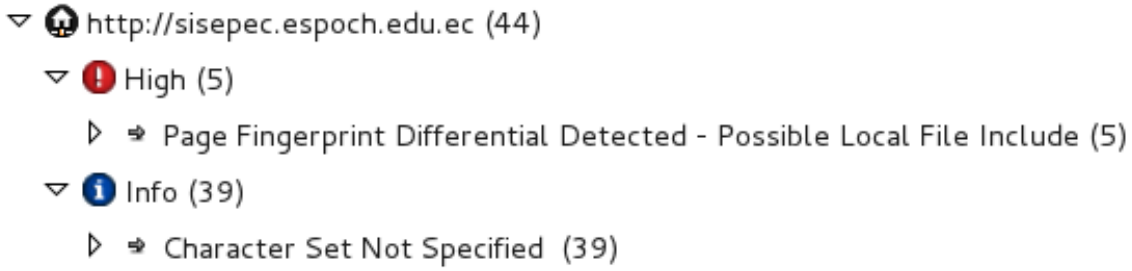


Grados de libertad	α=.995	α=.99	α=.975	α=.95	α=.90	α=.10	α=.05	α=.025	α=.01	α=.005
1	0.0000	0.0002	0.0010	0.0039	0.0158	2.7055	3.8415	5.0239	6.6349	7.8794
2	0.0100	0.0201	0.0506	0.1026	0.2107	4.6052	5.9915	7.3778	9.2103	10.597
3	0.0717	0.1148	0.2158	0.3518	0.5844	6.2514	7.8147	9.3484	11.345	12.838
4	0.2070	0.2971	0.4844	0.7107	1.0636	7.7794	9.4877	11.143	13.277	14.860
5	0.4117	0.5543	0.8312	1.1455	1.6103	9.2364	11.070	12.833	15.086	16.750
6	0.6757	0.8721	1.2373	1.6354	2.2041	10.645	12.592	14.449	16.812	18.548
7	0.9893	1.2390	1.6899	2.1673	2.8331	12.017	14.067	16.013	18.475	20.278
8	1.3444	1.6465	2.1797	2.7326	3.4895	13.362	15.507	17.535	20.090	21.955
9	1.7349	2.0879	2.7004	3.3251	4.1682	14.684	16.919	19.023	21.666	23.589

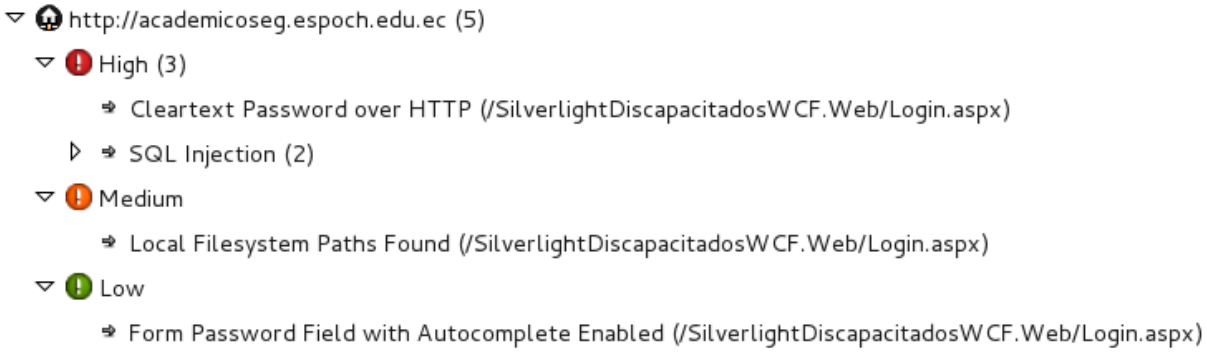
ANEXOS B:

RESULTADOS DE VULNERABILIDADES SERVICIOS WEB ACTIVOS

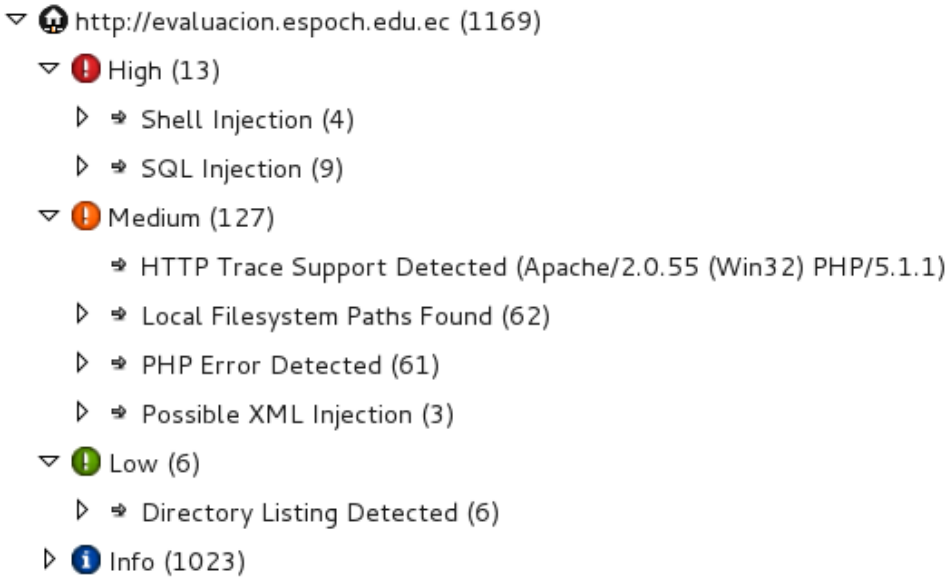
URL: http://sisepec.espoch.edu.ec/



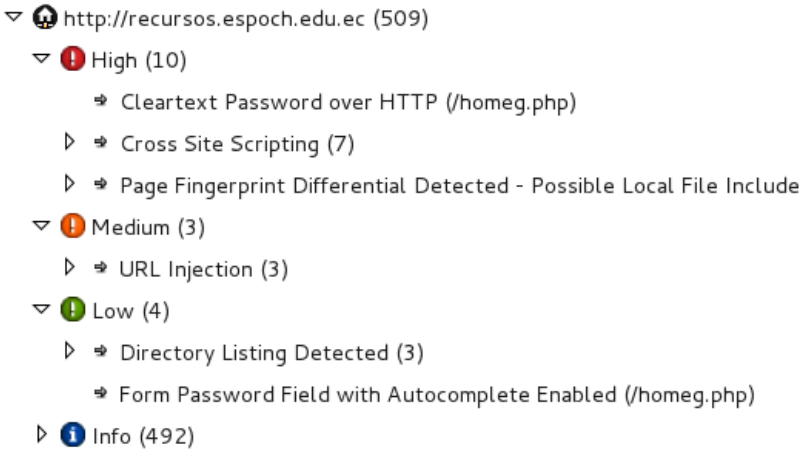
http://academicoseg.espoch.edu.ec/



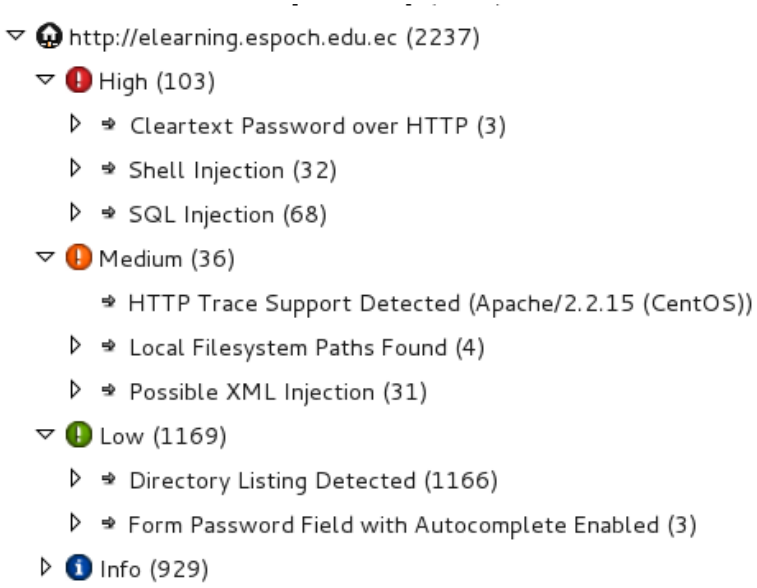
http://evaluacion.espoch.edu.ec/



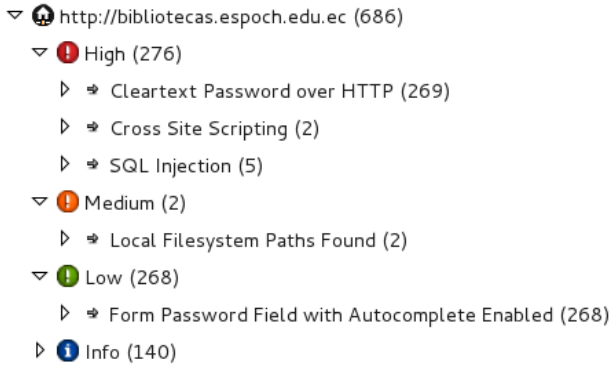
http://recursos.espoch.edu.ec/



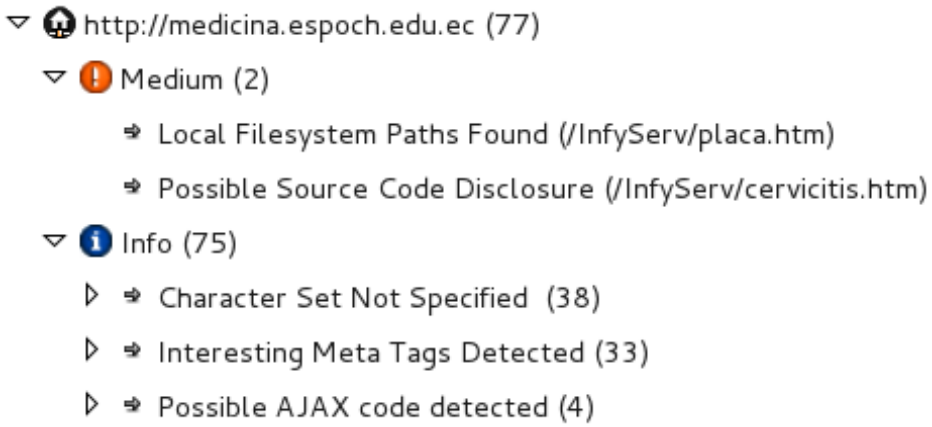
http://elearning.espoch.edu.ec/



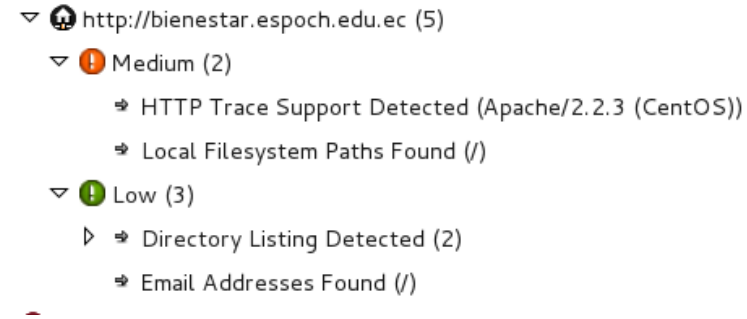
http://bibliotecas.espoch.edu.ec/



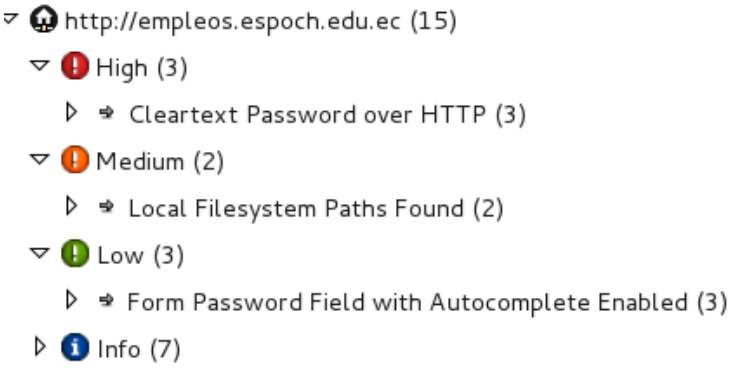
http://medicina.espoch.edu.ec/



http://bienestar.espoch.edu.ec/



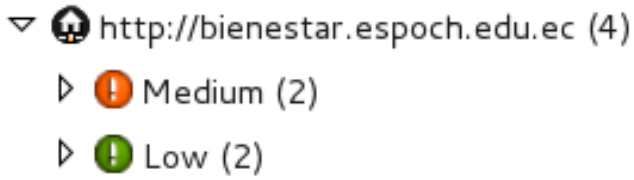
http://empleos.espoch.edu.ec/



ANEXO 3:

RESULTADOS DE VULNERABILIDADES SERVICIOS WEB ACTIVOS DESPUES DE LA APLICACIÓN DEL PLAN DE POSIBLES SOLUCIONES

http://bienestar.espoch.edu.ec/



http://recursos.espoch.edu.ec/