UNIVERSIDAD TECNOLÓGICA ISRAEL

TRABAJO DE TITULACIÓN EN OPCIÓN AL GRADO DE:

INGENIERO EN SISTEMAS INFORMÁTICOS

TEMA:

DIAGNÓSTICO DE LAS VULNERABILIDADES INFORMÁTICAS EN LAS APLICACIONES WEB DE LA UNIVERSIDAD CENTRAL DEL ECUADOR

AUTORES:

MARÍA JOSÉ ANDRADE RODRÍGUEZ

GRACE MARCELA ZAMBRANO VÉLEZ

TUTOR:

MSc. ING. PABLO RECALDE

QUITO, ECUADOR

2019

DECLARACIÓN DE AUTORÍA

El documento de tesis con título: "DIAGNÓSTICO DE LAS VULNERABILIDADES INFORMÁTICAS EN LAS APLICACIONES WEB DE LA UNIVERSIDAD CENTRAL DEL ECUADOR", ha sido desarrollado por las señoritas María José Andrade Rodríguez con C.C. No. 1722339817 y Grace Marcela Zambrano Vélez con C.C. No. 1719346973 personas que poseen los derechos de autoría y responsabilidad, restringiéndose la copia o utilización de la información de esta tesis sin previa autorización.

_____ _____

María José Andrade Rodríguez Grace Marcela Zambrano Vélez

UNIVERSIDAD TECNOLÓGICA ISRAEL

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del Trabajo de Titulación certifico:

Que el trabajo de titulación **"DIAGNÓSTICO DE LAS VULNERABILIDADES INFORMÁTICAS EN LAS APLICACIONES WEB DE LA UNIVERSIDAD CENTRAL DEL ECUADOR"**, presentado por las señoritas María José Andrade Rodríguez y Grace Marcela Zambrano Vélez, estudiantes de la Carrera Ingeniería en Sistemas Informáticos, reúne los requisitos y méritos suficientes para ser sometido a la evaluación del Tribunal de Grado, que se designe, para su correspondiente estudio y calificación.

Quito D. M, Febrero, 2019

TUTOR

Mg. Pablo Recalde

AGRADECIMIENTOS

Con gratitud y respeto presentamos el siguiente trabajo, que va especialmente dirigido a nuestros distinguidos Maestros, forjadores de una juventud noble y justa que mañana harán del Ecuador una Patria más libre y próspera.

A nuestros compañeros y amigos a quienes llevamos en el corazón con mucho recuerdo.

A nuestra querida Universidad Israel, cuyas aulas son testigos de sueños que hoy los vemos realizados.

DEDICATORIA

Una nueva etapa de nuestra vida termina y es por eso que dedicamos con mucho amor y cariño este trabajo a nuestros padres, hermanos, quienes con su esfuerzo y sacrificio hicieron posible este logro.

Son ustedes un ejemplo a seguir en cada momento, y sobre todo la fuerza que nos impulsa a un futuro.

TABLA DE CONTENIDOS

LISTA DE FIGURAS

LISTA DE TABLAS

RESUMEN

Las aplicaciones se desarrollan de acuerdo con los requisitos del campo de garantía de calidad; los requisitos que surgen de cada dependencia de una institución, tanto académica como administrativa, si se verifican la viabilidad y la rentabilidad, se establecen procesos generales y específicos, reflejados en documentos con requisitos funcionales transferidos al desarrollar un dominio para el análisis y diseño de una base de datos y, finalmente, para el desarrollo de un sistema, siendo el objetivo de la investigación analizar las vulnerabilidades de las aplicaciones web desarrolladas en la Universidad Central del Ecuador, aplicando una investigación contrastiva y aplicada, utilizando como base el Top 10 de OWASP – 2017, concluyendo que se revelan como de vital importancia además que el manejo de información es elevado dado que son sistemas que se actualizan periódicamente significando los mismos la posibilidad de brindar un funcionamiento óptimo para dicha institución.

PALABRAS CLAVES: Vulnerabilidad, aplicaciones, riesgos, informática, metodología OWASP, desarrollo web.

ABSTRACT

The applications are developed in accordance with the requirements of the field of quality assurance; the requirements that arise from each dependency of an institution, both academic and administrative, if feasibility and profitability are verified, general and specific processes are established, reflected in documents with functional requirements transferred when developing a domain for the analysis and design of a database and, finally, for the development of a system, the research objective being to analyze the vulnerabilities of the web applications developed at the Central University of Ecuador, applying a contrastive and applied research, using as a base the Top 10 of OWASP, concluding that they reveal that it is of vital importance that the handling of information is high, given that they are systems that are periodically updated, meaning that they can provide an optimal functioning for said institution.

KEYWORDS: Vulnerability, applications, risks, information technology, OWASP methodology, web development.

INTRODUCCIÓN

ANTECEDENTES DE LA SITUACIÓN OBJETO DE ESTUDIO

La Universidad Central del Ecuador, es la universidad más antigua y la segunda más grande por número de estudiantes de la República del Ecuador. Se ubica en el centro-norte de la ciudad de Quito, en la llamada ciudadela universitaria, además cuenta con sedes en la ciudad de Santo Domingo de los Colorados, y en las Islas Galápagos. Afiliada desde 2012 a la Red Ecuatoriana de Universidades para Investigación y Postgrados.

Sus orígenes se remontan a la Universidad Central de Quito. La cual se originó de la unión de las Universidades: Seminario de San Luis y San Gregorio Magno fundada en 1651 por los Jesuitas y la Santo Tomás de Aquino, fundada en 1681 por los Dominicos. Sobre la base de la Real Universidad Pública Santo Tomas se fundó la Universidad Central de Quito. para en el año 1836, mediante decreto del presidente Vicente Rocafuerte se cambie la palabra Quito, por Ecuador y surge ya de forma definitiva la Universidad Central del Ecuador (UCE).

Cuenta con 21 Facultades, 72 Carrera y 45000 estudiantes matriculados de grado y posgrado. Las aplicaciones desarrolladas son desplegadas a toda la Comunidad Universitaria.

Actualmente las aplicaciones se desarrollan de acuerdo a los requerimientos levantados por el área de QA; requerimientos que nacen de cada una de las Dependencias de la Institución sean estas académicas o administrativas, si se verifica la factibilidad y viabilidad de los mismos, se establecen los procesos generales y específicos que son plasmados en los documentos de requerimiento funcional, los mismos que son pasados al área de desarrollo para el análisis y diseño de la base de datos y finalmente para la elaboración del Sistema.

PLANTEAMIENTO DEL PROBLEMA

Con el paso del tiempo el uso del Internet se ha incrementado, generando una demanda de aplicativos Web cada vez mayor. Todo se maneja desde una terminal (laptop, pc, celular) conectada al Internet facilitando el logro de una actividad en específico al usuario.

Durante el tiempo de funcionamiento, la Universidad Central llevaba sus procesos y registros de manera manual aumentando tiempo de respuestas y generando malestar en sus usuarios.

Con estos antecedentes, la UCE ha desarrollado varios aplicativos que le permiten generar tareas específicas a sus usuarios finales que van desde personal administrativo hasta los estudiantes; con el fin de optimizar tiempos y recursos. Estas aplicaciones han logrado sistematizar los procesos críticos y con ello obtener mejores resultados, pero al mismo tiempo abrir una brecha a los riesgos y vulnerabilidades externos que puedan presentar. Es por todo esto que resulta relevante realizar el análisis propuesto en el presente trabajo de investigación para identificar dichas brechas en la seguridad de los aplicativos más críticos dentro de su catálogo de plataformas Web de la Universidad.

JUSTIFICACIÓN

Con el desarrollo de este análisis se pretende detectar riesgos y vulnerabilidades en los aplicativos Web de la Universidad Central del Ecuador lo cual permitirá realizar rectificaciones a futuro en sus políticas y procedimientos actuales en lo que respecta a la seguridad dentro del desarrollo de aplicativos. Así también ayudará a educar a sus programadores en cuanto a estas políticas.

OBJETIVOS

La presente investigación es de gran importancia para el correcto funcionamiento de la Universidad Central del Ecuador, de ahí que se plantearon los siguientes objetivos:

OBJETIVO GENERAL

Diagnosticar las vulnerabilidades de las aplicaciones web desarrolladas en la Universidad Central del Ecuador.

OBJETIVOS ESPECÍFICOS

- Determinar las aplicaciones web críticas a través de una matriz de riesgos.
- Analizar cada una de las vulnerabilidades que presenten las aplicaciones seleccionadas.
- Sugerir buenas prácticas de seguridad para el desarrollo de futuros aplicativos.
- Generar recomendaciones de seguridad para las vulnerabilidades identificadas.

DESCRIPCIÓN DE LOS CAPÍTULOS

A continuación, una breve descripción de cada uno de los capítulos contenidos en el presente trabajo de investigación.

Capítulo I: FUNDAMENTACIÓN TEÓRICA: en la que se establece el estado del arte, la línea del negocio, herramientas técnicas y alternativas de solución.

Capítulo II. MARCO METODOLÓGICO: se establece el tipo de investigación a desarrollar, los métodos que se utilizarán en cada parte de la investigación.

Capítulo III. PROPUESTA, se desarrolla el diagnóstico de la situación actual, la factibilidad técnica, operacional, económica y el modelo estándar a aplicar.

Capítulo IV. IMPLEMENTACIÓN: Se desarrolla la metodología a utilizar, así como los factores de riesgo para la estimación, los cuales son: factores relacionados con el agente causante de la amenaza, factores para estimar el impacto, factores de impacto sobre el negocio, determinación de la gravedad del riesgo, así como el diseño de la propuesta de solución en la que se desarrollan las buenas prácticas de seguridad para el desarrollo web, estrategias a implementar y la generación de buenas prácticas en el desarrollo del software. Finalmente se establecen las conclusiones y recomendaciones.

1. CAPÍTULO I. FUNDAMENTACIÓN TEÓRICA

A continuación, se desarrollan conceptos importantes para la investigación, de tal manera que se puedan sentar las bases teóricas que respaldan el estudio.

1.1 MARCO REFERENCIAL

1.1.1 INTRODUCCIÓN A LAS APLICACIONES WEB Y LA SEGURIDAD

El éxito de las aplicaciones web se debe a lo práctico de utilizar un navegador web como un Cliente ligero, son multiplataforma, es decir, existe completa independencia del Sistema operativo, así como a la sencillez con las que se actualiza y mantiene las aplicaciones web, sin necesidad de la instalación de software en los cientos de usuarios que podrían existir.

Es necesario mencionar que una Aplicación Web puede contener recursos que permitan una comunicación interactiva entre el usuario y la información. Con esto, la aplicación responderá a cada una de las acciones que realice el usuario, como por ejemplo registro y envío de información, participación en juegos diversos y acceso a los gestores de base de datos.

Al iniciar la Web era únicamente un conjunto de páginas estáticas, recopilación de documentos, o sitios de consulta o descarga. El salto a la evolución fue la implementación de mecanismos para la elaboración de páginas dinámicas, permitiendo que lo visualizado se convierta en dinámico.

Al hablar de aplicaciones para la web se pueden considerar varias ventajas entre ellas se menciona, son multiplataforma, permiten el acceso de un sin número de usuarios de forma concurrente (se sujeta a las características del servidor), la información permanece en línea, actualización y mantenimiento de forma sencilla.

El acceso a las aplicaciones web se realiza mediante Internet, con ello las mismas quedan expuestas a un sin número de amenazas que pueden llegar desde cualquier origen; en tal virtud, el término de aplicación web se encuentra estrechamente ligado la seguridad, derivando los ataques a nivel de aplicación, que se han convertido en una

amenaza de incremento constante contra la seguridad Web. Estos ataques utilizan una variedad de mecanismo para dejar offline un sitio Web o para inmiscuirse en él, lo que puede conllevar a inconvenientes que van desde una disminución del rendimiento del sitio, usurpación de información o hasta desprotección de la infraestructura tecnológica. (Mateu, 2012, pág. 11)

1.1.2 APLICACIONES WEB

Es un conjunto de herramientas orientadas al usuario con el fin de que este pueda acceder a un servidor mediante el uso de un navegador que se conecta a Internet o bien a una intranet.

Las aplicaciones web son muy exitosas debido a su independencia del sistema operativo que tenga instalado el usuario y porque pueden encontrarse de cualquier tipo: web-mails, tiendas on-line, gestión bancaria, blogs, foros. Basan su éxito en el concepto de interactividad que mantienen las aplicaciones web con el usuario. Un ejemplo es el uso de formularios o gestionar bases de datos.

Las ventajas que se encuentran a la hora de diseñar aplicaciones Web son varias, entre las principales se pueden considerar las siguientes (Cardador, 2014):

- No es necesario instalar nada de parte del cliente.
- No es necesario que el cliente actualice nada.
- No hay problema de actualización de versiones. Todos usan la misma versión
- Centralización de la información
- No se requiere un sistema operativo determinado, ni software ni hardware determinado.
- Se puede trabajar donde se quiera siempre que se disponga de un equipo y conexión de red.

Al momento de utilizar aplicaciones Web se pueden presentar algunas desventajas, entre las que se puede mencionar:

- Requieren de una conexión de red.
- Su desarrollo es complejo, dado que hay que garantizar la compatibilidad con los sistemas operativos. Software y hardware de los clientes.

- Su tiempo de respuesta suele ser algo más lento, aunque hoy en día la capacidad de respuesta no tiene nada que envidiar a las aplicaciones de escritorio.

1.1.3 EVOLUCIÓN DE LAS APLICACIONES WEB

Apareciendo en los años 90, la web 1.0 fue la primera forma de acceso a la información, contando en su totalidad con páginas estáticas de solo lectura. Para el año 2004 se acuña el término de la Web 2.0, un fenómeno social que cambió para siempre la relación entre la información y la comunicación con el usuario, ya que lo hizo parte de ella.

En el año 2010 fue operativa la Web 3.0, es asociada a la web semántica refiriéndose al uso de un lenguaje en la red, es decir realiza búsqueda de contenidos a través de palabras clave. Al comienzo del año 2016 comienza a reconocerse una nueva etapa, la Web 4.0 que propende a la inteligencia con característica de predicción (Latorre, 2018, págs. 2-7), en la tabla 1 se puede observar un resumen acerca de la evolución de la web.

Tabla 1.1. Evolución de la Web

La Web	Características	Ventajas	Desventajas
Web 1.0	Estática Centralizada Secuencial Solo lectura No Interactiva	Mostraba información al usuario sobre temáticas requeridas.	No permitía la interacción entre el Sitio y los usuarios. Universo de datos que en su mayoría eran estáticos.
Web 2.0	Colaborativa Intercambio ágil de Información. Dinámica Interactiva	Cambia la forma en la que los usuarios perciben la información en línea. Basa su funcionamiento en comunidades de usuarios. Cuenta con nuevos servicios como:	Al basar su funcionamiento en comunidades de usuarios no todo en la red es lo que parece, así que se introducen los términos de suplantación de identidad, cyberacoso y demás

		Redes sociales, Blogs, wikis, chat, foros, galerías fotográficas, entre otros	
Web 3.0	Aplicaciones web interconectadas Conocida como la Web semántica	Es interoperativa, se gestiona en la nube y se emplea desde cualquier dispositivo	Los usuarios pueden ser rastreados por sistemas de procesamiento gracias a los metadatos
Web 4.0	Comportamiento más inteligente y más predictivo	Ofrece soluciones a partir de la información que proporcionamos. Permite adelantarse a situaciones cotidianas Todos aprenden todos enseñan Se relaciona con la IA	Dependencia absoluta de conexiones a portales. Información de ubicación prácticamente pública.

Fuente: Autores

1.1.4 MODELO OSI

El Modelo de Referencia de Interconexión de Sistemas Abiertos, conocido como Modelo OSI (*Open System Interconnection*), creado por la ISO (*Organizacion Estandar Internacional*), en él pueden modelarse o referenciarse diversos dispositivos que reglamenta la ITU (Unión de Telecomunicación Internacional), con el fin de poner orden entre todos los sistemas y componentes requeridos en la transmisión de datos, además de simplificar la interrelación entre fabricantes.

El Modelo OSI se compone por 7 capas:

- Capa de Aplicación
- Capa de Presentación
- Capa de Sesión
- Capa de Transporte
- Capa de Red
- Capa de Enlace de Datos

- Capa Física

Capa Física. Es el primer nivel del modelo OSI y en él se definen y reglamentan todas las características físicas-mecánicas y eléctricas que debe cumplir el sistema para poder operar. Como es el nivel más bajo, es el que se va a encargar de las comunicaciones físicas entre dispositivos y de cuidar su correcta operación. Es bien sabido que la información computarizada es procesada y transmitida en forma digital siendo esta de bits: 1 y 0. Por lo que, toda aplicación que se desee enviar, será transmitida en forma serial mediante la representación de unos y ceros. En síntesis, la capa Físico transmite el flujo de bits sobre un medio físico y aquella que representa el cableado, las tarjetas y las señales de los dispositivos.

Capa de Enlace de Datos. Conocido también como nivel de Trama (Frame) o Marco, es el encargado de preparar la información codificada en forma binaria en formatos previamente definidos por el protocolo a utilizar.

Se puede concebir a ésta como una cadena de bits que marchan en una fila inmensa (para el caso de transmisiones seriales), cadena que carece de significado hasta el momento en que las señales binarias se agrupan bajo reglas, a fin de permitir su interpretación en el lado receptor de una manera constante. Este nivel ensambla los datos en tramas y las transmite a través del medio (LAN o WAN). Por lo tanto, se puede decir que la capa de Enlace de Datos es aquella que transmite la información como grupos de bits, es decir, transforma los bits en frames o paquetes por lo cual, si se recibe, se espera en conjunto de señales para convertirlos en caracteres, mientras que, si se envía, se convierte directamente cada carácter en señales ya sean digitales o analógicos.

Capa de Red. la capa de Red es la encargada de la información de enrutador e interceptores y aquella que maneja el Hardware (HW), ruteadores, puentes, multiplexores para mejorar el enrutamiento de los paquetes.

Capa de Transporte. En este nivel se realiza y se garantiza la calidad de la comunicación, ya que asegura la integridad de los datos. Es aquí donde se realizan las retransmisiones cuando la información fue corrompida o porque alguna trama (del nivel 2) detectó errores en el formato y se requiere volver a enviar el paquete o datagrama.

El nivel de transporte notifica a las capas superiores si se está logrando la calidad requerida. Este nivel utiliza reconocimientos, números de secuencia y control de flujo. En tal virtud, la capa de Transporte es la integridad de datos de extremo a extremo, es decir que se encarga el flujo de datos del transmisor al receptor verificando la integridad de los mismos por medio de algoritmos de detección y corrección de errores.

Capa de Sesión. Se encarga de proveer servicios de conexión entre las aplicaciones, tales como iniciar, mantener y finalizar una sesión. Establece, mantiene, sincroniza y administra el diálogo entre aplicaciones remotas. Cuando se establece una comunicación y que se nos solicita un comando como login, estamos iniciando una sesión con un host remoto y podemos referenciar esta función con el nivel de sesión del modelo OSI. Del mismo modo, cuando se nos notifica de una suspensión en el proceso de impresión por falta de papel en la impresora, es el nivel de sesión el encargado de notificarnos de esto y de todo lo relacionado con la administración de la sesión.

Capa de Presentación. Se refiere a la forma en que los datos son representados en una computadora. Proporciona conversión de códigos y reformateo de datos de la aplicación del usuario. Es sabido que la información es procesada en forma binaria y en este nivel se llevan a cabo las adaptaciones necesarias para que pueda ser presentada de una manera más accesible. Códigos como ASCII (*American Standard Code for Information Interchange*) y EBCDIC (*Extended Binary Coded Decimal Interchange Code*), que permiten interpretar los datos binarios en caracteres que puedan ser fácilmente manejados, tienen su posicionamiento en el nivel de presentación del modelo OSI.

Capa de Aplicación. Es el nivel más cercano al usuario y a diferencia de los demás niveles, por ser el más alto o el último, no proporciona un servicio a ningún otro nivel. Cuando se habla de aplicaciones lo primero que viene a la mente son las aplicaciones que procesamos, es decir, nuestra base de datos, una hoja de cálculo, un archivo de texto, etc., lo cual tiene sentido ya que son las aplicaciones que finalmente deseamos transmitir. Sin embargo, en el contexto del Modelo de Referencia de Interconexión de Sistemas Abiertos, al hablar del nivel de Aplicación no nos estamos refiriendo a las aplicaciones que acabamos de citar. En el modelo OSI el nivel de aplicación se refiere a las aplicaciones de red que vamos a utilizar para transportar las aplicaciones del usuario, por ejemplo, FTP (File Transfer Protocol), Mail, Rlogin,

Telnet, son entre otras las aplicaciones incluidas en la capa siete del modelo OSI y sólo cobran vida al momento de requerir una comunicación entre dos entidades. Sintetizando, se puede decir que la capa de Aplicación se dice que es una sesión específica de aplicación (API), es decir, son los programas que ve el usuario. (Hernández, 2017)

1.1.5 ARQUITECTURAS CLIENTE – SERVIDOR

Es un modelo mediante el cual se desarrollan aplicaciones distribuidas; en el mismo, las actividades se distribuyen entre los servidores, y los solicitantes, que se denominan clientes. El software Cliente realiza peticiones a uno o varios servidores, que necesariamente deben estar en línea para solventar las demandas.

El modelo Cliente/Servidor permite diversificar el trabajo que realiza cada aplicación, de forma que los Clientes no se sobrecarguen, cosa que ocurriría si ellos mismos desempeñan las funciones que le son proporcionadas de forma directa y transparente. En esta arquitectura la capacidad de proceso está repartida entre los clientes y los servidores, aunque son más importantes las ventajas de tipo organizativo debidas a la centralización de la gestión de la información y la separación de responsabilidades, lo que facilita y clarifica el diseño del sistema. Tanto el Cliente como el Servidor son entidades abstractas que pueden residir en la misma máquina o en máquinas diferentes. (Marini, 2012)

1.1.6 PROTOCOLO HTTP Y HTTPS

HTTP es un protocolo de transferencia de hipertexto perteneciente a la capa de aplicación del modelo TCP/IP (Transmission control protocol/Internet protocol) y es el corazón de la Web y define la forma como los clientes Web realizan peticiones a los servidores y cómo los servidores los transfieren a los clientes. Los programas cliente HTTP son conocidos como navegadores de Internet. (Montoya, Uribe, & Rodríguez, 2013)

En virtud de la comunicación, HTTP se soporta en las conexiones TCP/IP, y su funcionamiento se realiza de la misma forma que los demás servicios Sistemas Operativos basados en UNIX: un proceso principal o servidor escucha a un puerto que

por defecto es el 80, que trata conexiones TCP y se encuentra esperando las peticiones uno o varios clientes. Toda vez que la conexión se establece, el propósito del protocolo TCP es mantener la comunicación garantizando el intercambio de información sin errores.

Es necesario especificar el funcionamiento de estos protocolos con más profundidad, los protocolos HTTP y HTTPS son la cara visible del Internet y basan su trabajo en sencillas operaciones de petición/respuesta. El cliente debe establecer la conexión con el servidor, enviando un mensaje con los datos de la petición. El servidor debe responder con el estado del proceso de la transacción y un resultado tentativo como se observa en la figura 1.1.

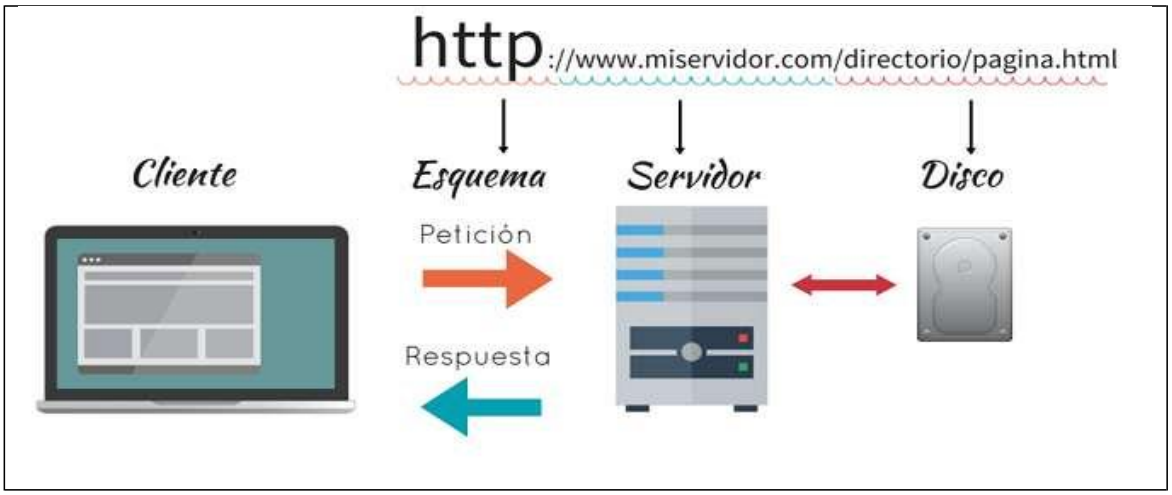


Figura 1.1. Esquema de una petición Web
Fuente: (Cabré, 2015)

La principal diferencia entre el protocolo HTTP y el protocolo seguro de transferencia de hipertexto, conocido como HTTPS, es que él realiza el mismo proceso, pero con datos cifrados al momento de transmitirlos creando una forma más segura a través de Internet. HTTPS se utiliza generalmente en instituciones que requieran solicitar datos personales y contraseñas o cualquier sitio que necesite información personal para completar transacciones en línea.

1.1.7 ARQUITECTURA EN CAPAS EN JAVA

La plataforma Java EE provee un modelo multicapa y distribuido, esto quiere decir que diferentes partes de una aplicación pueden estar corriendo en diferentes

dispositivos. La arquitectura define una capa cliente, una capa intermedia (compuestas por una o más subcapas) y una capa de datos, también conocida como la capa de información empresarial (IE), como se identifica en la figura 1.2.

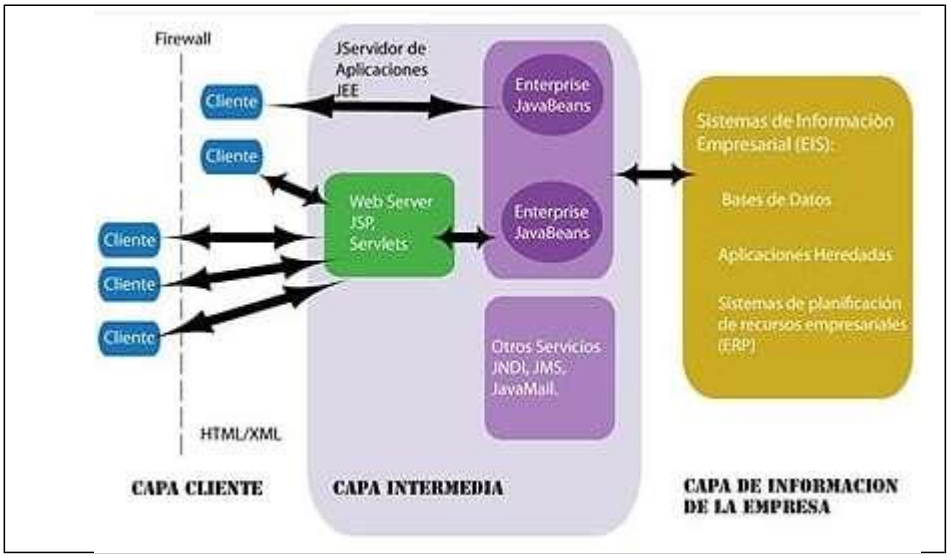


Figura 1.1. Arquitectura Multicapa JEE
Fuente: Arquitectura de desarrollo de Software – Universidad Central del Ecuador

Capa cliente. Esta capa cliente la integran aplicaciones clientes que acceden al servidor Java EE y normalmente se encuentran en una máquina diferente a la del servidor. Los clientes hacen peticiones al servidor el cual las procesa y las responde. Hay muchos tipos de aplicaciones diferentes que pueden ser clientes Java EE, y no tienen por qué ser aplicaciones Java EE, es más, a menudo no lo suelen ser. Los clientes pueden ser un navegador web, una aplicación autónoma, o incluso otros servidores que estén corriendo en otra máquina diferente de donde se encuentra el servidor Java EE.

Capa intermedia. El desarrollo de las aplicaciones Java EE se centran en esta capa, con el fin de realizar aplicaciones empresariales que sean fáciles de gestionar, más robustas y más seguras. Esta capa puede estar formada por más de una subcapa, normalmente una capa Web y otra que se centra en los procesos de negocio, como se puede ver en la figura 1.3.

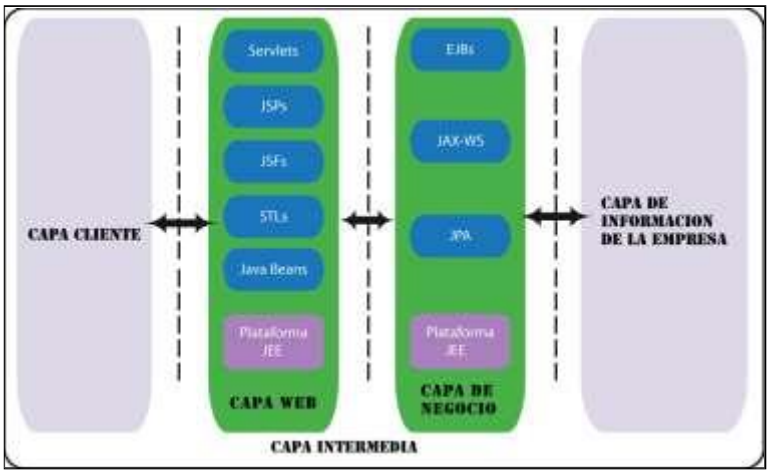


Figura 1.2. Arquitectura Multicapa JEE- Capa Intermedia
Fuente: Arquitectura de desarrollo de Software – Universidad Central del Ecuador

Capa Web. La capa o nivel Web, consiste en el conjunto de componentes que capturan la interacción entre los clientes y la capa de negocio. Sus principales tareas son las siguientes:

- Generación dinámica del contenido, en varios formatos, para el cliente.
- Recoger las entradas de los usuarios de la interfaz de las aplicaciones cliente y devolver los resultados apropiados desde los componentes de la capa de negocio.
- Controlar el flujo de pantallas o páginas en el cliente.
- Mantener el estado de los datos para una sesión de un usuario.
- Realizar algunas operaciones básicas pertenecientes a la lógica de la aplicación y guardar temporalmente alguna información (usando JavaBeans).

Las tecnologías más comunes de la capa de presentación o Web son:

- **Servlets,** procesan dinámicamente las peticiones y construyen las respuestas de los clientes, comúnmente utilizado con páginas HTML.
- **JavaServerPages,** definen como el contenido dinámico puede ser añadido a las páginas estáticas.
- **JavaServer Faces,** componente framework de la interfaz de usuario para aplicaciones web, que permite la inclusión de componentes de interfaz de usuario (como pueden ser botones) en una página, convierte y valida datos de los componentes IU, etc.
- **JavaServerPagesStandarTag Library,** una librería de tags que encapsula

las funcionalidades principales más comunes de las páginas JSP.

- **JavaBeans Components,** objetos que temporalmente almacenan lo datos de las páginas de una aplicación.

Capa de Negocio. La capa de Negocio está integrada por componentes que proveen la lógica de negocio para una aplicación. La lógica de negocio es el código que provee las funcionalidades para un particular dominio del negocio, como puede ser finanzas o un sitio de e-commerce. En un diseño correcto de una aplicación empresarial, las principales funcionalidades se encuentran en los componentes de la capa de negocio.

Las tecnologías más comunes de la capa de negocio son:

- Enterprise JavaBeans (EJB). Abstraen los problemas generales de una aplicación empresarial (concurrencia, transacciones, persistencia, seguridad, etc.).
- JAX-WS, web service endpoints. API de Java para la creación de servicios web.
- Java Persistence API entities. Entidades del API de persistencia que permite la representación objetual de los datos relacionales (BD) en aplicaciones Java.

Capa de Datos o del Sistema de Información Empresarial. La capa de datos está integrada por los servidores de bases de datos, sistemas ERP y otras fuentes de datos ya existentes, como mainframes. Habitualmente, estos recursos están situados en una máquina independiente de en la que se encuentra el servidor Java EE, y se acceden a ellos a través de la capa de negocio. Las tecnologías más comunes de la capa de datos son:

- **Java Database Connectivity API (JDBC).** API que permite la ejecución de operaciones sobre bases de datos desde el lenguaje de programación Java

- **Java Persistence API.** API de persistencia que permite el manejo de datos relacionales en aplicaciones Java.

- **J2EE ConnectorArchitecture.** Solución tecnológica que permite conectar

servidores de aplicaciones y sistemas de información empresarial (EIS) como parte de soluciones de integración de aplicación de empresa (EAI).

- **Java Transaction API (JTA).** API que permite la administración de recursos, transacciones de servidores de aplicación y transacciones de aplicación (Mateu, 2012).

1.2 ESTADO DEL ARTE

1.2.1 SEGURIDAD EN LAS APLICACIONES WEB

Todas las organizaciones que exponen sus servicios de información deben tener acceso a las redes para no escatimar esfuerzos para garantizar la protección de la información y los recursos. Internet es un factor de comunicación importante, así como un claro riesgo potencial de acceso y mal uso de los servicios e información disponibles. Por supuesto, los sistemas más importantes están catalogados contra otros cuya seguridad debe ser muy importante, pero en general, todas las aplicaciones web deben estar protegidas contra ataques fundamentales (Rodríguez, 2017).

En la aplicación web, la seguridad se comparte en:

- **Accesibilidad:** la propiedad o característica de un activo compuesto por personas autorizadas o procesos con acceso a la solicitud.
- **Autenticación:** la característica es que la entidad es la que llama o proporciona la fuente para la cual se recibieron los datos.
- **Confidencialidad:** propiedad impide la divulgación de la información a personas, organizaciones o procesos no autorizados.
- **Trazabilidad:** propiedad o característica que las actividades de la organización pueden atribuirse exclusivamente a esta organización.

1.2.2 SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información tiene como prioridad las medidas de prevención y respuesta para las organizaciones y los sistemas tecnológicos que protegen la información, al tiempo que buscan preservar la confidencialidad, la disponibilidad y la integridad de los datos y de la información. (Mateu C. , 2014).

El concepto de seguridad de la información no debe confundirse con la seguridad de la información, ya que solo se refiere a la seguridad en un entorno de información, pero la información se puede encontrar en diferentes entornos o módulos, no solo en los entornos informáticos. La seguridad de la información tiene un impacto significativo en su privacidad y puede determinar los diferentes elementos que dependen de la cultura.

El campo de la seguridad de la información se ha expandido considerablemente desde la Segunda Guerra Mundial y es una carrera reconocida en todo el mundo. Esta área ofrece una amplia gama de áreas de experiencia, incluida la revisión de sistemas de información, la planificación de la continuidad del negocio, la administración forense digital y la seguridad administrativa, entre otras (Cardador, 2014).

1.2.3 REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

Los requisitos de seguridad para el acceso del cliente a los recursos de información de la organización pueden variar considerablemente según el tipo de herramienta de procesamiento de información y el tipo de información recibida. Los requisitos de seguridad se definen en el anexo del acuerdo obtenido por la autoridad contratante e indican claramente todos los riesgos y requisitos de seguridad, otras partes podrán participar en acuerdos celebrados por terceros, en dichos acuerdos, es necesario garantizar que el acceso de terceros se realice con la autorización expresa de la organización que establece las condiciones de acceso (Areito, 2016).

De conformidad con los acuerdos ISO / IEC 17799 con terceros, el acceso, procesamiento, transmisión o administración de información comercial o servicios de procesamiento de información, así como la adición de productos para cumplir con los

requisitos de seguridad más importante, el acuerdo que alcancen debe garantizar que no haya interrupciones entre la organización y terceros.

Al final del contrato, se definen ciertas condiciones que determinan los requisitos de seguridad de la información: estrategia de seguridad de la información, controles que protegen al usuario, métodos, procedimientos y seguridad, así como proporcionar a los usuarios información sobre problemas y responsabilidades relacionadas con la seguridad de la información (Quero, García, & Peña, 2017).

Crea una estructura, enumera los procesos de gestión del cambio, establece una política de control de acceso, organiza informes e investiga diversos incidentes informativos, así como describe el producto presentado y cree una descripción de la información disponible con la clasificación de seguridad preparada por la organización, de igual manera consigue el objetivo de niveles de servicio y niveles inaceptables.

Establecer los parámetros de referencia, monitorear y verificar los informes, tiene derecho a verificar y cancelar todas las actividades relacionadas con los recursos de información de la compañía, como resultado estos controles son realizados por terceros. De igual manera instala el procedimiento necesario para resolver los problemas lo más rápido posible, identificando los requisitos de mantenimiento continúo que incluyen disponibilidad y confiabilidad.

1.2.4 SEGURIDAD INFORMÁTICA

La seguridad informática es definida como un proceso de prevención y detección de uso no autorizado de un sistema informático, incluye un proceso para eliminar a los intrusos de nuestros recursos informáticos con fines malintencionados o beneficios, o incluso para acceder a ellos accidentalmente para protegerlos (Mateu, 2012).

La seguridad informática es en realidad un término más general, con seguridad de la información, aunque los dos términos se usan a menudo en la práctica, incluye un intervalo de seguridad, así como las medidas de seguridad de la computadora tales como programas antivirus, firewalls y otras medidas, que dependen del usuario, como la

activación de la desactivación de ciertas funciones del software, como Java Script, ActiveX, el uso adecuado de una computadora, recursos web o en Internet.

Evite el robo de datos, como números de cuentas bancarias, información de tarjetas de crédito, contraseñas, documentos de trabajo, hojas de cálculo, etc., que son necesarios para la comunicación moderna, muchas de las actividades diarias dependen de la seguridad de los datos y como uno de los puntos de partida en la ruta, los datos en la computadora no están autorizados (Mateu C. , 2014).

Una amenaza puede alterar y modificar el código fuente del programa y usted puede usar su propia foto o crear cuentas de correo electrónico maliciosas, como imágenes pornográficas o cuentas sociales incorrectas. Un delincuente cibernético que intenta acceder a computadoras con propósitos maliciosos, como ataques informáticos, sitios web o cualquier otra red, pero también crea caos (Rodríguez, 2017).

Los hackers pueden bloquear un sistema informático para mitigar la pérdida de datos pueden realizar ataques para garantizar que no se puede acceder a las páginas web cuando el servidor también falla, todos estos factores han subrayado la necesidad de mantener los datos seguros y confidenciales, y la necesidad, por lo tanto, de la protección del equipo, lo que significa que es necesario e importante para todo lo relacionado con la seguridad informática.

1.2.5 SEGURIDAD EN LAS APLICACIONES INFORMÁTICAS

En la actualidad, Internet tiene un impacto directo en la seguridad de la información procesada diariamente, los sitios web, servicios, bancos e incluso redes sociales contienen información secreta que es muy importante en la mayoría de los casos (Latorre, 2018).

Se puede decir que son uno de los problemas de seguridad de Internet más importantes que afectan directamente a los usuarios, en este caso los servidores web, a menudo se escuchan errores en los sistemas de seguridad de los servidores más utilizados, como Apache, NGINX, IIS, etc., o en los lenguajes de programación en los que se ejecutan las aplicaciones. Sin embargo, ninguna de estas partes constituye la

mayoría de los problemas encontrados en los servicios en línea, lo que lleva a prácticas de programación deficientes.

Se debe entender que las aplicaciones de los programas no son fáciles de programar porque los programadores no solo deben lograr el objetivo principal del funcionamiento de la aplicación, sino también una comprensión general de los riesgos de divulgación de la información procesada con el sistema.

1.2.6 RIESGOS Y VULNERABILIDADES

En el área de la informática mencionar la existencia de un riesgo, puede implicar la probabilidad de que una amenaza se produzca, conllevando a un ataque al equipo o a un servidor; no siendo nada más que la posibilidad de que ocurra el ataque por parte de la amenaza. Al realizar un análisis del riesgo existente se puede tomar decisiones para asegurar mejor al sistema (Marini, 2012).

Las vulnerabilidades no son más que puntos débiles en el software que se identifican permitiendo que un atacante pueda llegar a comprometer la integridad, disponibilidad o confidencialidad de un Sistema o Aplicativo. Algunas de las vulnerabilidades más fuertes permiten la ejecución de una serie de códigos por parte del atacante, convirtiéndose en vulnerabilidades de seguridad.

1.2.7 RIESGOS DE SEGURIDAD PARA APLICACIONES

Para las Instituciones que manejan información crítica este es uno de los temas más sensibles de manejar, ya que, nombres, direcciones, números de tarjetas de crédito o cualquier otro tipo de información valiosa podría ser utilizada de forma incorrecta y con esto perjudicar a los usuarios (Mateu, 2012).

Al contar con aplicaciones poco seguras o vulnerables las Instituciones podrían enfrentar muchos problemas, la mayoría de estos se dan por el desconocimiento de las empresas acerca de cuáles son los riesgos y los principales problemas de seguridad que enfrentan sus aplicaciones hoy en día; además de una deficiente validación de la información que se manipula. Los atacantes pueden, potencialmente, utilizar diferentes rutas a través de su aplicación para perjudicar su negocio u organización. Cada uno de

estos caminos representa un riesgo que puede o no ser suficientemente grave como para merecer atención (OWASP, 2017). Lo cual se ilustra en la figura 1.4.

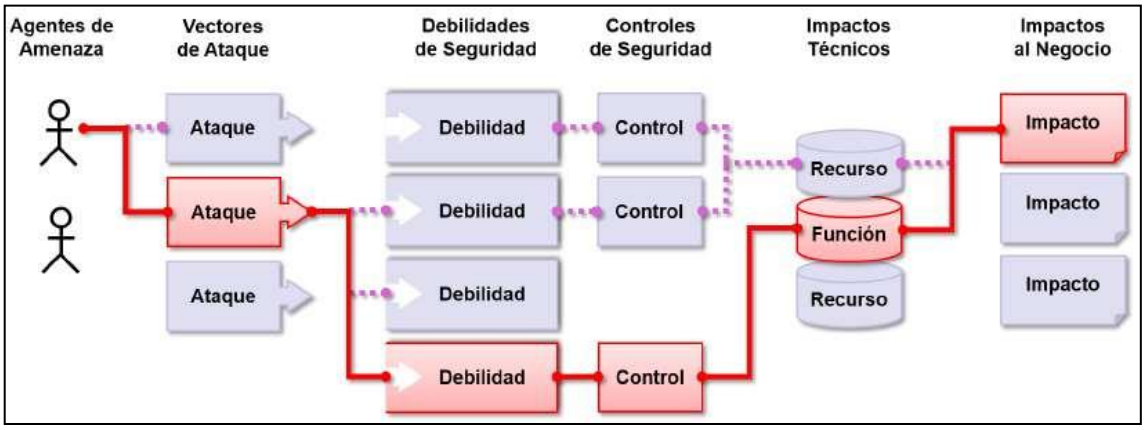


Figura 1.3. Riesgos de seguridad de Aplicaciones.
Fuente: OWASP Top Ten (2017)

1.2.8 VULNERABILIDADES EN APLICACIONES

Las aplicaciones web pueden presentar diversas vulnerabilidades, las cuales ocurren de acuerdo a los servicios que prestan. Según OWASP (Acrónimo de *Open Web Application Security Project* en inglés, Proyecto de seguridad de aplicaciones web abiertas"), las vulnerabilidades que prevalecen sobre el tiempo son:

- Inyección
- Pérdida de Autenticación
- Exposición de datos sensibles
- Entidades Externas XML (XXE)
- Pérdida de control de acceso
- Configuración de Seguridad Incorrecta
- Secuencia de Comandos en Sitios Cruzados (XSS)
- Deserialización Insegura
- Componentes con vulnerabilidades conocidas
- Registro y Monitoreo Insuficientes

1.2.9 OWASP TOP 10 – 2017

El Proyecto Abierto de Seguridad en Aplicaciones Web (OWASP por sus siglas en inglés) es una comunidad abierta dedicada a permitir que las organizaciones desarrollen, adquieran y mantengan aplicaciones y APIs en las que se pueda confiar.

Inyección A1:2017

Las falencias realizadas por inyección, como SQL, NoSQL, OS o LDAP se presentan cuando se envían datos no confiables a un intérprete, como parte de un comando o consulta. Los datos dañinos del atacante pueden engañar al intérprete para que ejecute comandos involuntarios o acceda a los datos sin la debida autorización, como se observa en la figura 1.5.

Figura 1.4. Inyección de código
Fuente: OWASP Top 10 2017 Los diez riesgos más críticos en Aplicaciones Web

Pérdida de Autenticación A2:2017

Las funciones de la aplicación relacionadas a autenticación y gestión de sesiones son implementadas incorrectamente, permitiendo a los atacantes comprometer usuarios y contraseñas, token de sesiones, o explotar otras fallas de implementación para asumir la identidad de otros usuarios (temporal o permanentemente), lo cual se verifica en la figura 1.6.

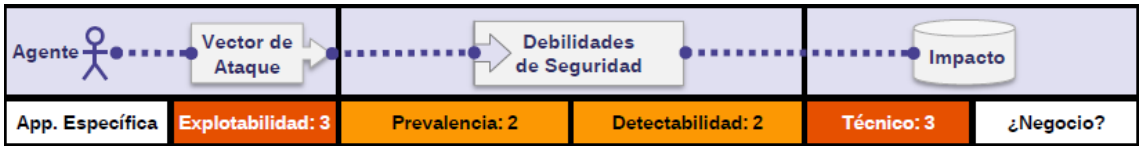


Figura 1.5. Pérdida de Autenticación
Fuente: OWASP Top 10 2017 Los diez riesgos más críticos en Aplicaciones Web

Exposición de datos sensibles A3:2017

Muchas aplicaciones web y APIs no protegen adecuadamente datos sensibles, tales como información financiera, de salud o Información Personalmente Identificable (PII). Los atacantes pueden robar o modificar estos datos protegidos inadecuadamente

para llevar a cabo fraudes con tarjetas de crédito, robos de identidad u otros delitos. Los datos sensibles requieren métodos de protección adicionales, como el cifrado en almacenamiento y tránsito, representado en la figura 1.7.

Figura 1.6 Exposición de datos sensibles
Fuente: OWASP Top 10 2017 Los diez riesgos más críticos en Aplicaciones Web

Entidades Externas XML (XXE) A4:2017

Muchos procesadores XML antiguos o mal configurados evalúan referencias a entidades externas en documentos XML. Las entidades externas pueden utilizarse para revelar archivos internos mediante la URI o archivos internos en servidores no actualizados, escanear puertos de la LAN, ejecutar código de forma remota y realizar ataques de denegación de servicio (DoS), evidenciando en la figura 1.8.

Figura 1.7. Entidades Externas XML (XXE)
Fuente: OWASP Top 10 2017 Los diez riesgos más críticos en Aplicaciones Web

Pérdida de control de acceso A5:2017

Las restricciones sobre lo que los usuarios autenticados pueden hacer no se aplican correctamente. Los atacantes pueden explotar estos defectos para acceder, de forma no autorizada, a funcionalidades y/o datos, cuentas de otros usuarios, ver archivos sensibles, modificar datos, cambiar derechos de acceso y permisos, etc, expuesto en la figura 1.9.

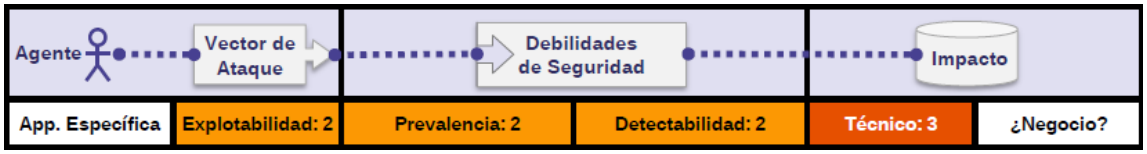


Figura 1.8. Pérdida de control de acceso
Fuente: OWASP Top 10 2017 Los diez riesgos más críticos en Aplicaciones Web

Configuración de Seguridad Incorrecta A6:2017

La configuración de seguridad incorrecta es un problema muy común y se debe en parte a establecer la configuración de forma manual, ad hoc o por omisión (o directamente por la falta de configuración). Son ejemplos: S3 buckets abiertos, cabeceras HTTP mal configuradas, mensajes de error con contenido sensible, falta de parches y actualizaciones, frameworks, dependencias y componentes desactualizados, etc, demostrado en la figura 1.10.

Figura 1.9. Configuración de Seguridad Incorrecta
Fuente: OWASP Top 10 2017 Los diez riesgos más críticos en Aplicaciones Web

Secuencia de Comandos en Sitios Cruzados (XSS) A7:2017

Los XSS ocurren cuando una aplicación toma datos no confiables y los envía al navegador web sin una validación y codificación apropiada; o actualiza una página web existente con datos suministrados por el usuario utilizando una API que ejecuta JavaScript en el navegador. Permiten ejecutar comandos en el navegador de la víctima y el atacante puede secuestrar una sesión, modificar (defacement) los sitios web, o redireccionar al usuario hacia un sitio malicioso, expuesta en la figura 1.11.

Figura 1.10. Secuencia de Comandos en Sitios Cruzados (XSS)
Fuente: OWASP Top 10 2017 Los diez riesgos más críticos en Aplicaciones Web

Deserialización Insegura A8:2017

Estos defectos ocurren cuando una aplicación recibe objetos serializados dañinos y estos objetos pueden ser manipulados o borrados por el atacante para realizar ataques de repetición, inyecciones o elevar sus privilegios de ejecución. En el peor de los casos, la deserialización insegura puede conducir a la ejecución remota de código en el servidor, señalado en la figura 1.12.

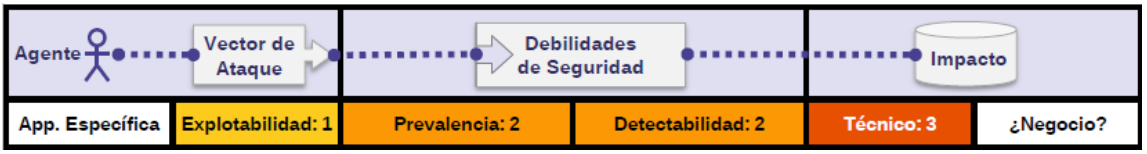


Figura 1.11. Deserialización Insegura
Fuente: OWASP Top 10 2017 Los diez riesgos más críticos en Aplicaciones Web

Componentes con vulnerabilidades conocidas A9:2017

Los componentes como bibliotecas, frameworks y otros módulos se ejecutan con los mismos privilegios que la aplicación. Si se explota un componente vulnerable, el ataque puede provocar una pérdida de datos o tomar el control del servidor. Las aplicaciones y API que utilizan componentes con vulnerabilidades conocidas pueden debilitar las defensas de las aplicaciones y permitir diversos ataques e impactos, explicada en la figura 1.13.

Figura 1.12. Componentes con vulnerabilidades conocidas
Fuente: OWASP Top 10 2017 Los diez riesgos más críticos en Aplicaciones Web

Registro y Monitoreo Insuficientes A10:2017

El registro y monitoreo insuficiente, junto a la falta de respuesta ante incidentes permiten a los atacantes mantener el ataque en el tiempo, pivotear a otros sistemas y manipular, extraer o destruir datos. Los estudios muestran que el tiempo de detección de una brecha de seguridad es mayor a 200 días, siendo típicamente detectado por terceros en lugar de por procesos internos, indicada en la figura 1.14.

Figura 1.13. Registro y Monitoreo Insuficientes

Fuente: OWASP Top 10 2017 Los diez riesgos más críticos en Aplicaciones Web

1.3 LÓGICA DEL NEGOCIO

La Universidad Central del Ecuador se rige por la Constitución de la República, la Ley de Educación Superior y su reglamento General, los reglamentos y las resoluciones expedidas por el Consejo de Educación Superior y por el Consejo de Evaluación,

Acreditación y Gestión de la Calidad de la Educación Superior, el Estatuto Universitario, los reglamentos expedidos por el Honorable Consejo Universitario y las resoluciones de sus autoridades.

La Universidad Central del Ecuador tiene la facultad dentro del marco constitucional y legal de expedir sus normas jurídicas, consistentes en su Estatuto, reglamentos e instructivos, a través de acuerdos y resoluciones emanadas por autoridad competente; de regirse por sí misma tomando sus propias decisiones en los órdenes académicos, científico, técnico, administrativo y económico. El orden interno es de exclusiva competencia y responsabilidad de sus autoridades.

La Dirección de Tecnologías de Información y Comunicación (DTIC), corresponde a la Dirección proponer al Honorable Consejo Universitario la planificación, regulación, control y la gestión estratégica de los recursos tecnológicos orientados al uso y transferencia de la información en los procesos académicos, de investigación y administrativos, así como garantizar la continuidad, el óptimo funcionamiento de la infraestructura tecnológica de la Institución y sus servicios.

Actualmente las aplicaciones se desarrollan de acuerdo a los requerimientos levantados por el área de Proyectos y Producción; requerimientos que nacen de cada una de las Dependencias de la Institución sean estas académicas o administrativas, si se verifica la factibilidad y viabilidad de los mismos, se establecen los procesos generales y específicos que son plasmados en los documentos de requerimiento funcional, los mismos que son pasados al área de Desarrollo para el análisis y diseño de la base de datos y finalmente para la elaboración del Sistema.

La creación de los proyectos de desarrollo en la Universidad Central del Ecuador, están basados completamente en configuraciones manuales, además de que pretenden cubrir la estructura de proyecto que podemos observar en la siguiente figura que ha sido planteada en la Institución, expuesta en la figura 1.15.

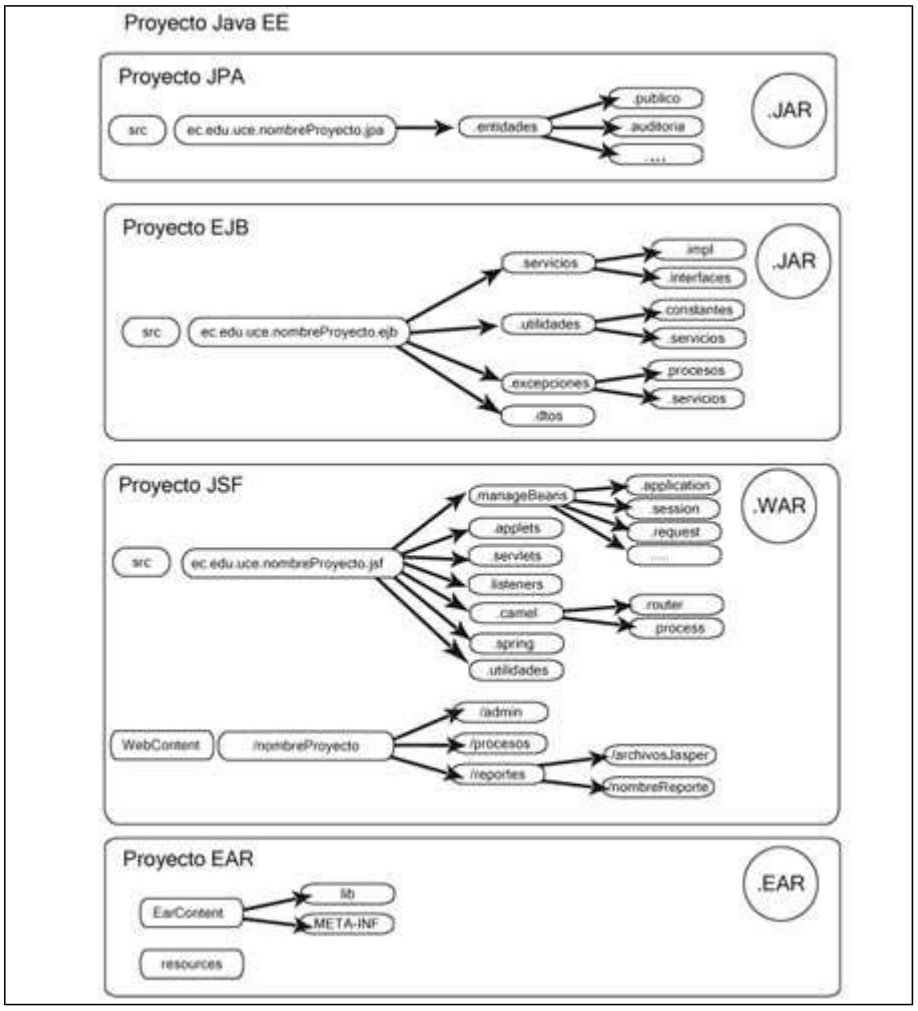


Figura 1.14. Configuración de un Proyecto JavaEE
Fuente: Universidad Central del Ecuador – Dirección de Tecnología – Área de Desarrollo

1.4 HERRAMIENTAS TÉCNICAS

OWASP ZAP viene del acrónico OWASP Zed Attack Proxy Project, es una herramienta de código abierto, Desarrollada por el Open Web Aplication Security Project, que básicamente es un proyecto para la auditoría de aplicaciones Web, la herramienta cuenta con un alcance y potencial basto permitiendo realizar pruebas de penetración, encontrando vulnerabilidades en las aplicaciones Web.

La herramienta está diseñada de tal manera que sea utilizada por personas con un amplio espectro de experiencia en temas de seguridad, también es ideal para los desarrolladores y personas quienes realizan pruebas funcionales siendo nuevos también en los temas de pruebas de penetración.

Zap proporciona escáneres automáticos como también un conjunto de diversas herramientas para encontrar vulnerabilidades en seguridad de manera manual. Entre las características más importantes se puede mencionar: es Open Source, es multiplataforma, quiere decir que lo podemos utilizar en diferentes Sistemas Operativos, facilidad al momento de instalar, completamente libre, facilidad de uso, toda vez que se entienda su funcionamiento, páginas de ayuda completos traducidos a 20 lenguas que alojan en el Sitio Web del proyecto, es un proyecto que se encuentra activo y en desarrollo permanente.

ZAP es un proxy de interceptación, el mismo que permite observar todas las solicitudes realizadas hacia la aplicación Web y todas las respuestas recibidas desde esta, cuenta con dos modos de ataque, modo de ataque activo y un modo de ataque pasivo. Permite definir break points, los mismos que permiten interceptar una solicitud desde el navegador y cambiarlo antes de ser enviado hacia la aplicación en evaluación. También permite cambiar las respuestas recibidas desde la aplicación. La solicitud o respuesta se mostrará en la pestaña break, la cual permite cambiar campos ocultos o deshabilitados, permitiendo evitar validaciones en el lado del cliente, lo que consiste en una técnica esencial en las pruebas de penetración, expuesta en la figura 1.16

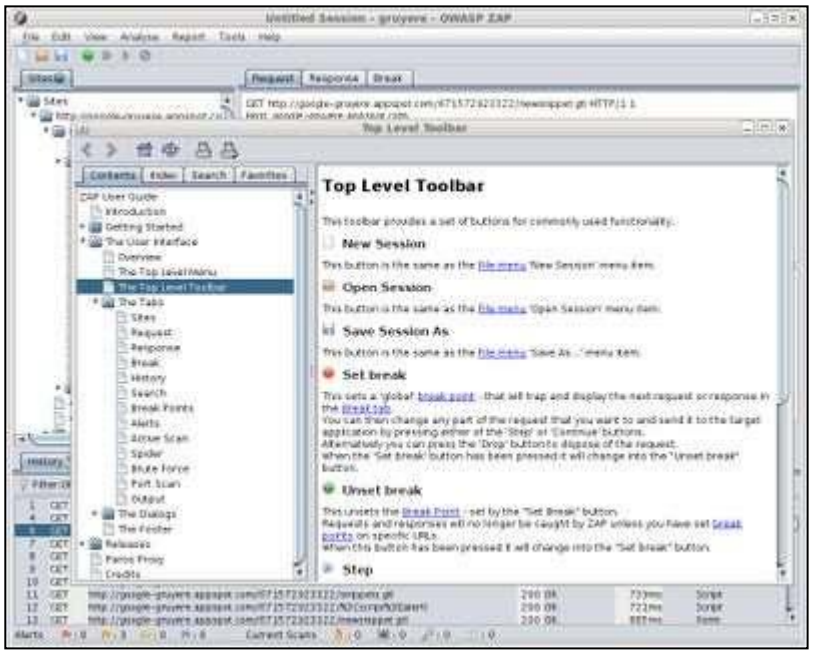


Figura 1.15. Ventana de OWASP ZAP
Fuente: Owasp Zed Attack Project

1.5 ALTERNATIVAS DE SOLUCIÓN

Los riesgos y las vulnerabilidades a los que información o la infraestructura tecnológica de una Institución pueden estar expuestos afectan a la seguridad, es por ello que se deben establecer restricciones. Las mismas definen por lo general protocolos, horarios de funcionamiento, denegaciones, planes de emergencia y, perfiles de usuario, autorizaciones para garantizar un alto nivel de seguridad informática en las organizaciones requeridas; con el objetivo fundamental de minimizar el impacto de los riesgos en el desempeño de la actividad organizacional.

Con este propósito se pretende alinear un conjunto de buenas prácticas al momento de desarrollar aplicaciones dentro de la UCE, de tal forma que la información que se maneja esté segura e íntegra.

Como estudios similares se han encontrado los trabajos de titulación de los estudiantes de la Escuela Politécnica del Ejército con el tema "ANÁLISIS DE LAS APLICACIONES WEB DE LA SUPERINTENDENCIA DE BANCOS Y SEGUROS, UTILIZANDO LAS RECOMENDACIONES TOP TEN DE OWASP PARA DETERMINAR LOS RIESGOS MÁS CRÍTICOS DE SEGURIDAD E IMPLEMENTAR BUENAS PRÁCTICAS DE SEGURIDAD PARA EL DESARROLLO DE SUS APLICATIVOS" y de la Universidad Nacional de Chimborazo con el tema "ANÁLISIS DE VULNERABILIDADES DE SOFTWARE PARA MEJORAR LA SEGURIDAD EN LOS SISTEMAS INFORMÁTICOS" (ver anexo #11), los mismos que hablan acerca del análisis de vulnerabilidades, con el objetivo de la identificación de riesgos; en ellos se detecta una versión desactualizada de la metodología OWASP Top Ten, versión 2010 y 2013 respectivamente; impidiéndoles profundizar en la identificación de vulnerabilidades y riesgos, mientras que en la presente Investigación se utiliza la metodología OWASP Top Ten 2017, lo que permitió determinar de una forma más concreta las vulnerabilidades o amenazas y los riesgos que éstas implican para las aplicaciones Web. Finalmente se concluye que es mejor utilizar una metodología de detección actualizada, ya que las amenazas cambian constantemente aumentando riesgos que pueden llegar a ser críticos.

2 CAPÍTULO II. MARCO METODOLÓGICO

El marco metodológico permite establecer la secuencia investigativa que realizarán las investigadoras, de tal manera que se desarrollen lógicamente los parámetros investigativos.

2.1 TIPO DE INVESTIGACIÓN

La metodología que fue seleccionada para este proyecto de tesis se basa en la Investigación Contrastiva e investigación Aplicada. La investigación contrastiva, permite encontrar los errores de las teorías, con el objetivo de eliminarlas, reajustarlas o aumentar su veracidad.

La investigación aplicada, se fundamenta en que, dentro de la secuencia de trabajo, existen teorías cuya veracidad se ha elevado gracias a un cierto número de aplicaciones y, además, de que en el mundo de las necesidades de desarrollo existen requerimientos que pueden ser satisfechos aprovechando esas teorías.

Su objetivo central está en proveer tecnologías o esquemas de acción derivados de los conocimientos teóricos construidos dentro de la secuencia de la línea. Esta investigación tiende a establecer una relación productiva, ingeniosa y creativa, entre las posibilidades de un modelo teórico, por un lado, y las necesidades que se confrontan en el terreno de la práctica.

En resumen, la investigación contrastiva se utilizará en la primera etapa del proyecto de tesis, luego de un análisis identificar los riesgos y vulnerabilidades encontradas en el proceso de desarrollo de aplicaciones web de la Universidad Central del Ecuador, en base al Top 10 de OWASP, lo cual se puede observar en el Anexo #1.

En la segunda parte del proyecto se utilizará la investigación aplicativa ya que el fin del proyecto de tesis es empezar a establecer un conjunto de buenas prácticas en el desarrollo de las aplicaciones web de acuerdo al Top 10 de OWASP.

Se pueden destacar los Métodos Científicos utilizados en la investigación:

Métodos Lógicos: Este es un tipo de razonamiento comparativo lógico, por lo que también se llama método comparativo. Es importante tener en cuenta que éste es un método de investigación.

Método Analítico-Sintético: es una combinación de dos formas de investigación utilizadas para desarrollar trabajos formales que requieren un esquema para lograr los objetivos.

Métodos Empíricos: es un modelo de investigación científica basado en lógica experimental y empírica que, con la observación de los fenómenos y su análisis estadístico, se usa más ampliamente en las ciencias sociales y naturales.

Método Experimental: Es un modelo de investigación científica basado en lógica experimental y empírica que, con la observación de los fenómenos y su análisis estadístico, se usa más ampliamente en las ciencias sociales y naturales.

Método Hipotético-Deductivo: sobre la base de ciertas hipótesis teóricas, extrae ciertas conclusiones mediante un procedimiento de inferencia o un cálculo formal.

En la presente investigación se ha utilizado el método analítico-sintético el cual permite descomponer el problema en elementos por separado y profundizar en el estudio de cada uno de ellos de forma independiente, para luego sintetizarlos en la solución de la propuesta. El método Hipotético Deductivo, se utilizó en el trabajo de investigación para la elaboración de la hipótesis central de la investigación y desarrollar procedimientos que arriben a conclusiones particulares, mientras que el método empírico permitió realizar el análisis de las aplicaciones Web de la UCE identificando los riesgos de seguridad más comunes mediante el top ten de *OWASP* y las principales dificultades existentes para el aseguramiento de las aplicaciones. Con el método experimental se evaluó resultados a partir de la experimentación y valoración de las muestras.

2.2 RECOPILACIÓN DE INFORMACIÓN

Para la recolección de datos se usan varios procedimientos que permite obtener y evaluar información para realizar juicios de determinados temas. Dentro de las más usadas se encuentran las entrevistas, encuestas y cuestionarios.

2.2.1 TÉCNICAS DE RECOPILACIÓN DE INFORMACIÓN

Dentro del desarrollo del presente documento se hizo uso de la entrevista (ver anexo #9) para obtener información preliminar de los aplicativos y las formas de desarrollo que tienen dentro de la Universidad Centra del Ecuador, así como también, información relevante acerca de los procesos y técnicas de programación y seguridad que aplica el Área de Desarrollo (ver anexos #3 y #4)

2.2.2 ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

La Universidad Central del Ecuador dedicada al campo de la enseñanza y catalogada como una de las principales y más representativas del Ecuador, con un aproximado de 66000 (http://datosabiertos.uce.edu.ec/Indicadores) estudiantes en total en las diferentes facultades y un total de docentes de 2200 aproximadamente.

Dentro de la oferta académica tienen diferentes carreras como Administración de Empresas, Administración Pública, Arquitectura, Ciencias del Lenguaje y Literatura, Ciencias Policiales y Seguridad Ciudadana, Contabilidad y Auditoría; entre otras. Siendo las ciencias Administrativas y Médicas las de mayor demanda, como muestra la figura 2.1.

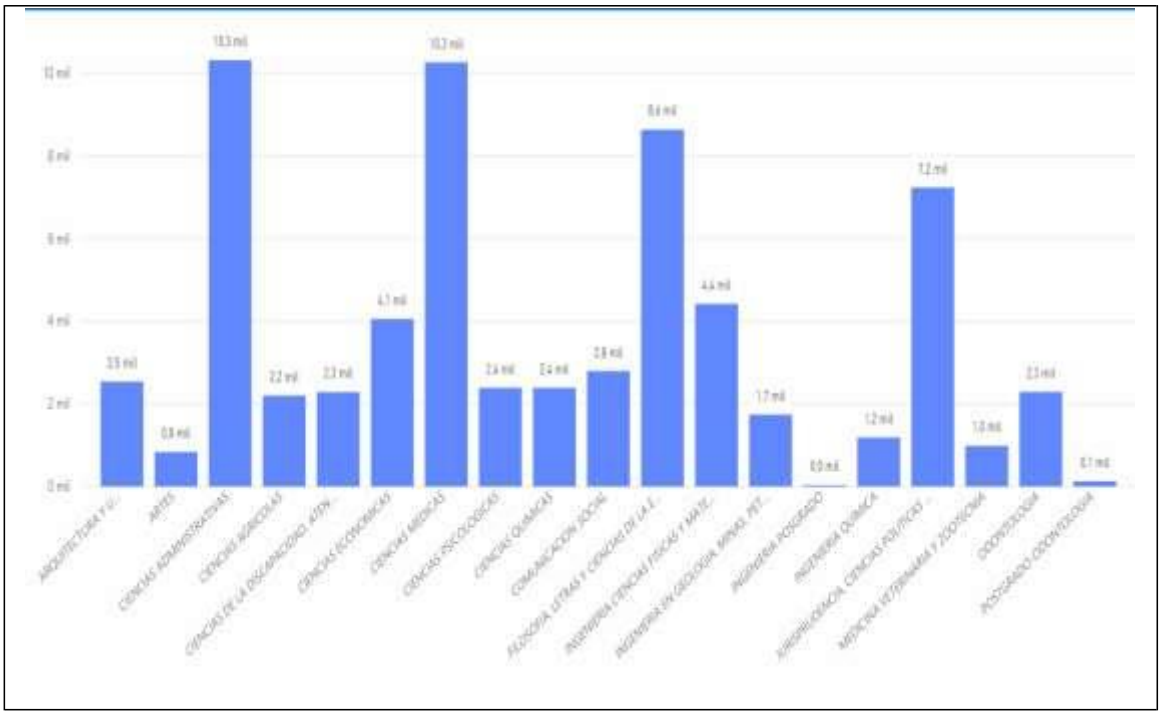


Figura 2.1. Total estudiantes por facultad
Fuente: http://datosabiertos.uce.edu.ec/Indicadores

Su parte organizacional y de administración se da por Rector, Vicerrector Académico y de Investigación y; vicerrector Administrativo y Financiero.

Todos los campus se encuentran comunicados y conectados a través de redes tanto LAN como WAN; de la misma manera, la Universidad junto con su equipo tecnológico ha desarrollado cada uno de los aplicativos según se ha ido presentado la necesidad de automatizar o mejorar sus procesos tanto internos como externos.

El Área de Desarrollo tiene definidas buenas prácticas y procedimientos que deben ser aplicados y respetados como parte del proceso de lanzar un nuevo sistema o brindar soporte a cualquiera de ellos. En gran mayoría los sistemas que se manejan son orientados a la Web.

Su parte organizacional y de administración se da por Rector, Vicerrector Académico y de Investigación y; vicerrector Administrativo y Financiero. (Colocar lo del consejo universitario)

Se encuentra ubicada en la avenida América, el predio abarca varios edificios donde se ubican las diferentes facultades y personal administrativo. Ciertas facultades

se encuentran fuera de este campus como es el caso de las Ciencias Agrícolas que está ubicada al nor-oriente de la ciudad de Quito.

Todos los campus se encuentran comunicados y conectados a través de redes tanto LAN como WAN; De la misma manera, la Universidad junto con su equipo tecnológico ha desarrollado cada uno de los aplicativos según se ha ido presentado la necesidad de automatizar o mejorar sus procesos tanto internos como externos.

El Área de Desarrollo tiene definidas buenas prácticas y procedimientos que deben ser aplicados y respetados como parte del proceso de lanzar un nuevo sistema o brindar soporte a cualquiera de ellos. En gran mayoría los sistemas que se manejan son orientados a la Web.

3 CAPÍTULO III. PROPUESTA

La propuesta de la investigación se sustenta en el desarrollo del diagnóstico de la situación inicial, el cual apoya la necesidad de desarrollar un análisis efectivo de las vulnerabilidades de las aplicaciones web de la Universidad Central del Ecuador.

3.1 FACTIBILIDAD

3.1.1 FACTIBILIDAD TÉCNICA

Tomando en consideración el volumen de información que es manejada por la Universidad diariamente y lo invaluable que es, se vuelve fundamental e indispensable asegurar que no será blanco de ataques, como por ejemplo DDOS (*Distributed Denial of Service*) o Ataques de Negación de Servicio Distribuido, haciendo que se envíen varias peticiones al servidor para que este colapse y deje de funcionar o también haciendo que el envío de los paquetes sean demasiados lentos y así el servidor se queda esperando infinitamente una respuesta de una IP falsa provocando la caída de la página web.

Hay infinidad de delitos informáticos que se pueden presentar, es por lo que se propone la oportunidad de realizar un análisis de las vulnerabilidades que los aplicativos más críticos puedan presentar.

Este análisis pretende identificar brechas o puntos críticos en la seguridad de información que se encuentran expuestas hacia el interior o exterior de la Universidad; así como también, facilitar la toma de decisiones al personal involucrado en cuanto a las mejoras o acciones correctivas que se deban aplicar.

Debido a la gran cantidad de peticiones que reciben estos sistemas, la Universidad propone que el análisis se lo haga a nivel de ambiente de pruebas; de esta manera no se interrumpe las actividades diarias y las observaciones o recomendaciones que puedan surgir del presente análisis las irán implementando en los aplicativos de producción de manera gradual.

3.1.2 FACTIBILIDAD OPERACIONAL

Se debe considerar y tomar en cuenta, que la vulnerabilidad crítica para un tipo de negocio o empresa no va a ser necesariamente lo mismo para otro. Es decir, hay que adaptar la metodología pretendida al giro de negocio que tiene la Universidad.

De manera operacional, el análisis a las vulnerabilidades debe abarcar dos frentes; esto lo que permitirá es reducir la efectividad de los ataques que se puedan presentar. Entre los principales frentes a mencionar están la Seguridad Lógica, aquí se aplicarán barreras y elaboran procedimientos que protejan la información como son los documentos de políticas y estándares; y la auditoría que no es más que la revisión y evaluación de estos controles, políticas y estándares planteados.

Se encuentra de manera implícita que las personas que tendrán acceso a los resultados, conclusiones y recomendaciones arrojadas por el análisis, como personal administradores, desarrolladores y QA´s deben tener los conocimientos básicos en cuanto a la rama de Sistemas Informáticos se refiere; esto con el fin de no crear o realizar actividades no adecuadas respecto a lo requerido (Montoya, Uribe, & Rodríguez, 2013).

3.1.3 FACTIBILIDAD ECONÓMICA

Teniendo en cuenta los diferentes aspectos anteriormente mencionados, solo empresas con suficiente capital podrían implementar una solución de seguridad que contemple todo lo necesario; en estos momentos y a pesar de estar conscientes de la importancia que debe tener la seguridad informática; no es una prioridad inmediata para la Universidad invertir en este rubro.

Por tal motivo, se ha considerado indispensable la elaboración del presente análisis para satisfacer esta necesidad, así como mejorar los ambientes de seguridad a un bajo costo, dándole de esta manera, un enfoque social.

3.1.4 MODELO O ESTÁNDAR A APLICAR

Los atacantes pueden usar diferentes formas en su aplicación para afectar su negocio u organización. Los riesgos están en cada una de estas formas que pueden ser o podrían ser graves para actuar.

En muchos casos, estos modos son fáciles de encontrar y usar, pero en otros casos son muy complejos, de la misma manera, el daño puede ser causado por alguien que ha hecho negocios. Para identificar el riesgo de su organización, puede evaluar la probabilidad de cada agente de amenaza, la vulnerabilidad del ataque y el vector de seguridad, y asociarlo con una evaluación del impacto técnico y comercial de su organización. Estos factores garantizan el riesgo global.

La última actualización de OWASP para 2017 se centra en identificar los riesgos más graves para muchas organizaciones para cada uno de estos riesgos, la información general está disponible en el significado y en el impacto técnico.

Aunque las versiones anteriores de Top 10 OWASP fueron diseñadas para identificar las vulnerabilidades más comunes, también fueron diseñadas para el riesgo. Los 10 nombres de riesgo principales se refieren al tipo de ataque, el tipo de debilidad o el tipo de impacto que pueden causar, además, todos los riesgos se revelan y se menciona su impacto potencial.

El Proyecto de Aplicación de Seguridad Abierta (OWASP) es una comunidad abierta que permite a las organizaciones de aplicaciones desarrollarlas y gestionarlas. Todas las herramientas, documentos, foros y delegaciones de OWASP son gratuitos y están abiertos a quienes desean mejorar la seguridad de la aplicación.

El proyecto OWASP es un nuevo tipo de organización que puede proporcionar información sobre responsabilidades, prácticas y revisiones de aplicaciones. OWASP no está conectado a ninguna compañía de tecnología, aunque puede respaldar el uso de información comercial sobre tecnologías de seguridad. Al igual que muchos otros proyectos de código abierto, OWASP ofrece materiales para el desarrollo cooperativo.

En la actualidad, la incertidumbre de los sistemas de información está causando graves daños a diversas áreas sociales, como salud, protección, finanzas y energía, con el desarrollo de la era digital, cada vez es más difícil crear aplicaciones seguras. OWASP ha diseñado el Top 10 para crear conciencia sobre la seguridad de las aplicaciones al identificar algunos de los riesgos más importantes asociados con las organizaciones. El objetivo principal de TOP-10 es informar a los desarrolladores, diseñadores, arquitectos, gerentes y organizaciones sobre las consecuencias de las vulnerabilidades de seguridad de las aplicaciones web, además, el Top 10 ilustra las principales rutas de protección de áreas de alto riesgo y propone recomendaciones para su mantenimiento. Durante el desarrollo del software, es importante identificar las vulnerabilidades que indican y evaluar el riesgo asociado con el negocio, en las primeras etapas de la vida del desarrollo de software, las técnicas de modelado de amenazas pueden identificar problemas de seguridad en la arquitectura o el diseño. Otros problemas de seguridad pueden detectarse mediante pruebas de verificación o equipos codificados, no se producirá ningún problema hasta que la aplicación se inicie y no detenga su seguridad, como se indica en la figura 3.1.

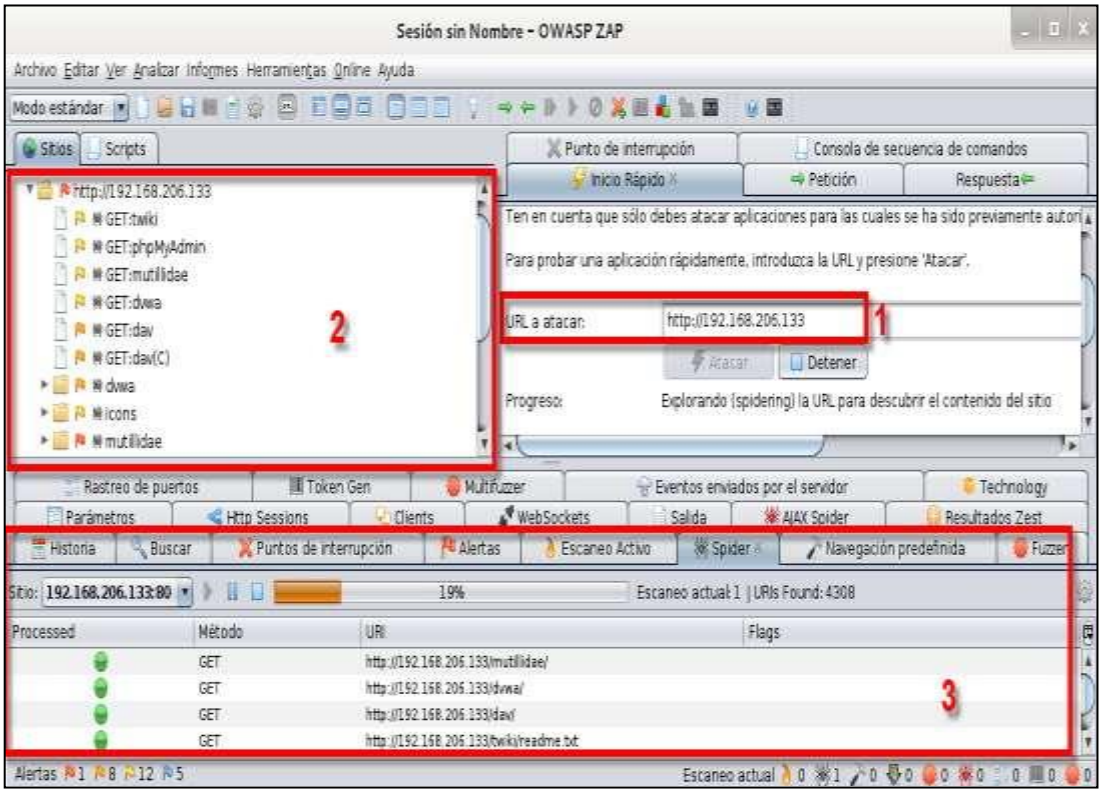


Figura 3.1. Análisis OWASP
Fuente: Autores

4 CAPÍTULO IV. IMPLEMENTACIÓN

El presente capítulo tiene como finalidad realizar el análisis de las vulnerabilidades de las aplicaciones web, para luego establecer las buenas prácticas a desarrollar.

4.1 APLICACIÓN DEL MODELO, ESTÁNDAR O METODOLOGÍA

Las aplicaciones web que actualmente posee la Universidad Central del Ecuador son:

Sistema de Recaudaciones Sysrec: Utilizado para la recaudación y facturación electrónica fue implementado para dar respuesta al cambio del sistema operativo XP a Windows 10 y como respuesta al incremento de los volúmenes de recaudación.

Sistema de Talento Humano - Módulo Nómina: Este sistema permite desarrollar un control efectivo de los pagos a los diferentes empleados de la universidad.

Sistema de Información Integral Módulo Académico: En este sistema los estudiantes pueden acceder a la información de sus calificaciones, pases de año, entre oros.

Plataforma Educativa Virtual: La plataforma permite entrega de trabajos, así como tener información sobre los temas a ser desarrollados, es de señalar que este espacio garantiza una intercomunicación sistemática entre los estudiantes y docentes

Sistema de Investigación: A través de este sistema se logra un acceso inmediato a la información a ser utilizada por docentes y estudiantes en el desarrollo y elaboración de investigaciones.

Sistema de Talento Humano - Módulo Personal: Este sistema permite un control efectivo sobre el desempeño individual de los trabajadores de la Universidad en el ámbito laboral.

Sistema de Gestión Documental: Garantiza la utilización efectiva de la base de datos de la institución de forma inmediata y con el mínimo de errores al actualizarse la misma de forma sistemática.

Sistema de Registro de Funcionarios: Se revela como una herramienta para impartir disposiciones que redunden en el cumplimiento de los objetivos planteados por la institución a corto, mediano y largo plazo.

Con la finalidad de determinar aquellas aplicaciones críticas en el ámbito académico y financiero de la institución se procedió a crear tablas de valoración de riesgos en la que se plasme la información de forma clara y actualizada, las cuales se detallan a continuación:

Tabla 4.1. Matriz de Riesgos Sistema de Recaudaciones Sysrec

		Matriz de Riesgos		
	Proceso:	*Desarrollo*		
	Aplicación a evaluar:	***Sistema de Recaudaciones Sysrec***		
	VARIABLES FUNDAMENTALES	**A** Valor Referencial 1 (Bajo) a 5 (Alto)	**B** Ponderación 1 (Bajo) a 10 (Alto)	**C = A* B** Valor Total
1	Característica de la Actividad	3	9	27
2	Recurrencia del Servicio	4	9	36
3	Sensibilidad del manejo para la Alta Gerencia	2	9	18
4	Materialidad	3	9	27
5	Alcance de sistema, procedimiento y proceso cambiar	2	9	18
6	Complejidad	4	9	36
7	Gerencia de Proyectos	4	9	36
8	Periodo de la última revisión	3	9	27
			TOTAL	225
			PORCENTAJE (%)	56.25
	Valor Mínimo	8	8	8
	Valor Máximo	40	80	400
		PONDERACIÓN DEL RIESGO		
		Riesgo Alto	Riesgo Medio	Riesgo Bajo
		67% - 100 %	34 % - 66%	1 % - 33 %

Fuente: Autores

La información anterior destaca que las variables fundamentales como recurrencia del servicio, complejidad y gerencia de proyectos se revelan como la de mayor valor referencial, tomando en cuenta la importancia de los mismos al momento de realizar las actividades de cobro en la universidad, de ahí que de fallar los mismos el servicio tendría retrasos y perjudicaría el normal funcionamiento de la institución.

Del análisis de riesgos de la aplicación Sistema de Recaudaciones Sysrec se determinó que el porcentaje de riesgo promedio es del 56.25%, evidenciando la existencia de falencias que podrían afectar el uso de la aplicación.

Tabla 4.2. Sistema de Información Integral - Módulo Académico

		Matriz de Riesgos		
	Proceso:	*Desarrollo*		
	Aplicación a evaluar:	***Sistema de Información Integral - Módulo Académico***		
		A	**B**	**C = A* B**
	VARIABLES FUNDAMENTALES	Valor Referencial 1 (Bajo) a 5 (Alto)	Ponderación 1 (Bajo) a 10 (Alto)	Valor Total
1	Característica de la Actividad	5	9	45
2	Recurrencia del Servicio	4	9	36
3	Sensibilidad del manejo para la Alta Gerencia	4	9	36
4	Materialidad	2	9	18
5	Alcance de sistema, procedimiento y proceso cambiar	2	9	18
6	Complejidad	3	9	27
7	Gerencia de Proyectos	3	9	27
8	Periodo de la última revisión	4	9	36
			TOTAL	243
			PORCENTAJE (%)	60.75
	Valor Máximo	40	80	400
		67 % - 100 %	34 % - 66 %	1 % - 33 %

Fuente: Autores

Las características de la actividad poseen el mayor valor referencial tomando en cuenta la complejidad y características de dichas acciones, así como su importancia para el normal funcionamiento de la aplicación en cuanto a los servicios académicos ofertados, seguida de la recurrencia del servicio, sensibilidad del manejo para la alta gerencia y período de la última revisión, factores importantes para garantizar una educación de calidad a los estudiantes.

Una vez analizados los riesgos de la aplicación Sistema de Información Integral - Módulo Académico se determinó que el porcentaje de riesgo promedio del 60.75%, lo cual permite determinar que la aplicación del sistema de información integral puede ser vulnerada.

Tabla 4.3 Sistema de Talento Humano - Módulo Nómina

	Matriz de Riesgos			
	Proceso:	*Desarrollo*		
	Aplicación a evaluar:	***Sistema de Talento Humano - Módulo Nómina***		
	VARIABLES FUNDAMENTALES	**A** Valor Referencial 1 (Bajo) a 5 (Alto)	**B** Ponderación 1 (Bajo) a 10 (Alto)	**C = A* B** Valor Total
1	Característica de la Actividad	4	8	32
2	Recurrencia del Servicio	4	8	32
3	Sensibilidad del manejo para la Alta Gerencia	5	8	40
4	Materialidad	4	8	32
5	Alcance de sistema, procedimiento y proceso cambiar	4	8	32
6	Complejidad	5	8	40
7	Gerencia de Proyectos	4	8	32
8	Periodo de la última revisión	3	8	24
			TOTAL	264
			PORCENTAJE (%)	66.00
	Valor Mínimo	8	8	8
	Valor Máximo	40	80	400

PONDERACIÓN DEL RIESGO		
Riesgo Alto	Riesgo Medio	Riesgo Bajo
67 % - 100 %	34 % - 66 %	1 % - 33 %

Fuente: Autores

Se evidencia que las variables de mayor valor referencial son la sensibilidad del manejo para la alta gerencia y la complejidad, destacando la importancia de las mismas

para una correcta utilización del talento humano. Módulo de nómina, lo cual garantizará un uso efectivo de los recursos institucionales.

Estudiados los riesgos de la aplicación Sistema de Talento Humano - Módulo Nómina se determinó que el porcentaje de riesgo promedio del 66%, lo cual permite determinar que la aplicación puede ser vulnerada.

Tabla 4.4 Plataforma Educativa Virtual

Matriz de Riesgos

Proceso:	*Desarrollo*
Aplicación a evaluar:	***Plataforma Educativa Virtual***

	VARIABLES FUNDAMENTALES	A Valor Referencia 1 (Bajo) a 5 (Alto)	B Ponderación 1 (Bajo) a 10 (Alto)	C = A* B Valor Total
1	Característica de la Actividad	4	8	32
2	Recurrencia del Servicio	4	8	32
3	Sensibilidad del manejo para la Alta Gerencia	5	8	40
4	Materialidad	4	8	32
5	Alcance de sistema, procedimiento y proceso cambiar	4	8	32
6	Complejidad	5	8	40
7	Gerencia de Proyectos	4	8	32
8	Periodo de la última revisión	3	8	24
			TOTAL	264
			PORCENTAJE (%)	66.00
	Valor Mínimo	8	8	8
	Valor Máximo	40	80	400

PONDERACIÓN DEL RIESGO		
Riesgo Alto	Riesgo Medio	Riesgo Bajo
67 % - 100 %	34 % - 66 %	1 % - 33 %

Fuente: Autores

Las variables de mayor valor referencial son la sensibilidad del manejo para la alta gerencia y la complejidad, de ahí que de fallar las mismas la entrega de trabajos y otras actividades académicas se encontrarían en dificultades, lo que representaría un perjuicio para los estudiantes.

Realizado el análisis de riesgos de la aplicación Plataforma Educativa Virtual se determinó que el porcentaje de riesgo promedio del 66%, lo cual permite determinar que la aplicación puede ser vulnerada.

Tabla 4.5. Sistema de investigación

		Matriz de Riesgos		
	Proceso:	*Desarrollo*		
	Aplicación a evaluar:	***Sistema de Investigación***		
	VARIABLES FUNDAMENTALES	**A** Valor Referencial 1 (Bajo) a 5 (Alto)	**B** Ponderación 1 (Bajo) a 10 (Alto)	**C = A* B** Valor Total
1	Característica de la Actividad	4	8	32
2	Recurrencia del Servicio	4	8	32
3	Sensibilidad del manejo para la Alta Gerencia	5	8	40
4	Materialidad	4	8	32
5	Alcance de sistema, procedimiento y proceso cambiar	4	8	32
6	Complejidad	5	8	40
7	Gerencia de Proyectos	4	8	32
8	Periodo de la última revisión	3	8	24
			TOTAL	264
			PORCENTAJE (%)	66.00
	Valor Mínimo	8	8	8
	Valor Máximo	40	80	400

PONDERACIÓN DEL RIESGO		
Riesgo Alto	Riesgo Medio	Riesgo Bajo
67 % - 100 %	34 % - 66 %	1 % - 33 %

Fuente: Autores

Las variables de mayor valor referencial son la sensibilidad del manejo para la alta gerencia y la complejidad, aspectos claves para garantizar una calidad en el registro y desarrollo de investigaciones, de forma tal que se logre un nivel educativo óptimo.

Hecho el análisis de riesgos de la aplicación Sistema de Investigación se determinó que el porcentaje de riesgo promedio del 66%, lo cual permite determinar que la aplicación puede ser vulnerada.

Tabla 4.6. Sistema de Talento Humano - Módulo Personal

		Matriz de Riesgos		
Proceso:		*Desarrollo*		
Aplicación a evaluar:		***Sistema de Talento Humano - Módulo Personal***		
	VARIABLES FUNDAMENTALES	**A** Valor Referencial 1 (Bajo) a 5 (Alto)	**B** Ponderación 1 (Bajo) a 10 (Alto)	**C = A* B** Valor Total
1	Característica de la Actividad	4	8	32
2	Recurrencia del Servicio	4	8	32
3	Sensibilidad del manejo para la Alta Gerencia	5	8	40
4	Materialidad	4	8	32
5	Alcance de sistema, procedimiento y proceso cambiar	4	8	32
6	Complejidad	5	8	40
7	Gerencia de Proyectos	4	8	32
8	Periodo de la última revisión	3	8	24
			TOTAL	264
			PORCENTAJE (%)	66.00
Valor Mínimo		8	8	8
Valor Máximo		40	80	400

PONDERACIÓN DEL RIESGO		
Riesgo Alto	Riesgo Medio	Riesgo Bajo
67 % - 100 %	34 % - 66 %	1 % - 33 %

Fuente: Autores

Las variables de mayor valor referencial son la sensibilidad de alta gerencia y complejidad dado que permiten una correcta captación del talento humano detallando en sus fortalezas y debilidades y por ende su capacidad de contribuir al mejoramiento de la calidad educativa de la institución.

Del análisis de riesgos de la aplicación Sistema de Talento Humano se determinó que el porcentaje de riesgo promedio del 66%, lo cual permite determinar que la aplicación puede ser vulnerada.

Tabla 4.7. Sistema de Gestión Documental

		Matriz de Riesgos		
	Proceso:	*Desarrollo*		
	Aplicación a evaluar:	***Sistema de Gestión Documental***		
	VARIABLES FUNDAMENTALES	**A** Valor Referencial 1 (Bajo) a 5 (Alto)	**B** Ponderación 1 (Bajo) a 10 (Alto)	**C = A* B** Valor Total
1	Característica de la Actividad	4	8	32
2	Recurrencia del Servicio	4	8	32
3	Sensibilidad del manejo para la Alta Gerencia	5	8	40
4	Materialidad	4	8	32
5	Alcance de sistema, procedimiento y proceso cambiar	4	8	32
6	Complejidad	5	8	40
7	Gerencia de Proyectos	4	8	32
8	Periodo de la última revisión	3	8	24
			TOTAL	264
			PORCENTAJE (%)	66.00
	Valor Mínimo	8	8	8
	Valor Máximo	40	80	400

PONDERACIÓN DEL RIESGO		
Riesgo Alto	Riesgo Medio	Riesgo Bajo
67 % - 100 %	34 % - 66 %	1 % - 33 %

Fuente: Autores

Las variables de mayor valor referencial son la sensibilidad del manejo para la alta gerencia y complejidad, evidenciando la importancia de un manejo adecuado y oportuno de toda la información documental que permita fortalecer y desarrollar la calidad y nivel educativo de la institución.

Una vez hecho el estudio de riesgos de la aplicación Sistema de Gestión Documental se determinó que el porcentaje de riesgo promedio del 66%, lo cual permite determinar que la aplicación puede ser vulnerada.

Tabla 4.8. Sistema de Registro de Funcionarios

	Matriz de Riesgos
Proceso:	*Desarrollo*
Aplicación a evaluar:	***Sistema de Registro de Funcionarios***

	VARIABLES FUNDAMENTALES	A Valor Referencial 1 (Bajo) a 5 (Alto)	B Ponderación 1 (Bajo) a 10 (Alto)	C = A* B Valor Total
1	Característica de la Actividad	4	8	32
2	Recurrencia del Servicio	4	8	32
3	Sensibilidad del manejo para la Alta Gerencia	5	8	40
4	Materialidad	4	8	32
5	Alcance de sistema, procedimiento y proceso cambiar	4	8	32
6	Complejidad	5	8	40
7	Gerencia de Proyectos	4	8	32
8	Periodo de la última revisión	3	8	24
			TOTAL	264
			PORCENTAJE (%)	66.00

Valor Mínimo	8	8	8
Valor Máximo	40	80	400

PONDERACIÓN DEL RIESGO		
Riesgo Alto	Riesgo Medio	Riesgo Bajo
67 % - 100 %	34 % - 66 %	1 % - 33 %

Fuente: Autores

Las variables de mayor valor referencial son la sensibilidad del manejo para la alta gerencia y la complejidad evidenciando de esta forma la importancia de un control adecuado de las actividades desarrolladas por los funcionarios de la institución de forma tal que se logre una ubicación estratégica de los mismos.

Con el análisis de riesgos de la aplicación Sistema de Registro de Funcionarios se determinó que el porcentaje de riesgo promedio del 66%, lo cual permite establecer que la aplicación puede ser vulnerada.

Luego de verificado el análisis individual de cada aplicativo se procedió a realizar una matriz de análisis comparativo de riesgos (ver anexo #12), en la que se definen las aplicaciones críticas a ser evaluadas con la herramienta OWASP Zap.

Una vez auditadas las aplicaciones y viendo sus puntuaciones en riesgo se debe analizar que se analizarán las siguientes aplicaciones:

- Sistema de Recaudaciones Sysrec
- Sistema de Información Integral - Módulo Académico
- Plataforma Educativa Virtual

Sistema de Recaudaciones Sysrec

A continuación, se expone la figura de acceso interno al sistema SYSREC, en el cual se evidencia la dirección IP para realizar el ingreso correspondiente.

Figura 4.1. Acceso SYSREC interno
Fuente: Universidad Central del Ecuador

En la figura se observa que el sistema solicita nombre de usuario y contraseña, de ahí sea necesario analizar la vulnerabilidad de descifrado de la contraseña.

Figura 4.2. Interfaz de inicio de sesión SYSREC
Fuente: Universidad Central del Ecuador

Sistema de Información Integral - Módulo Académico

A continuación, se expone la forma de acceso del Sistema de Información Integral - Módulo Académico, en el cual se puede verificar que el sistema solicita nombre de usuario y contraseña haciendo necesario analizar su grado de vulnerabilidad.

Figura 4.3. Interfaz de inicio de sesión Sistema Integral de Información
Fuente: Universidad Central del Ecuador

Plataforma Educativa Virtual

La figura 23 evidencia la forma de acceso a la plataforma educativa virtual en la que se solicita el usuario y la contraseña.

Figura 4.4. Interfaz de inicio de sesión Plataforma Educativa Virtual
Fuente: Universidad Central del Ecuador

Hay varias formas de realizar un análisis de riesgo (el documento del NIST, el documento del Open Source Security Testing Methodology Manual (OSSTMM), el marco de trabajo denominado Information System Security Framework (ISAAF) y el Open Web Application Security Project (OWASP), este estudio utiliza el enfoque OWASP basado en varias metodologías, incluida la metodología de evaluación de riesgos.

Esta metodología indica que el primer paso es la definición del riesgo de seguridad que se evaluará, se debe recopilar la recopilación de información sobre los agentes que causan la amenaza, el ataque que utilizan, la vulnerabilidad y el impacto de una empresa exitosa, además, todos los sistemas basados en OWASP TOP-10 se analizan a continuación:

Tabla 4.9. Análisis de los sistemas en base al TOP 10 de OWASP

	SYSREC	Sistema de Información Integral	Plataforma Educativa Virtual
R1	Se utilizan consultas estáticas y variables parametrizadas.		
R2	Validan los datos de entrada y las peticiones HTTP para cada sesión.		

R3	Si los usuarios no cierran las sesiones, éstas caducan a los 30 minutos de inactividad.	
R4	Se definen los permisos sobre los menús o perfiles que tiene cada usuario.	
R5	Cada enlace, sesión y formulario, contiene un token de seguridad no predecible para los usuarios.	
R6	Se trabaja con un servidor web Jboss el cual mantiene subido un firewall que no permite el acceso a la consola de administración mediante su IP.	
R7	No utilizan ningún algoritmo para encriptar la información	Se encriptan datos con Advanced Encryption Standard y MD5 para encriptar las contraseñas.
R8	Se emplean mecanismos de seguridad para el acceso a las páginas, mediante la autenticación y autorización.	
R9	No se utiliza un protocolo de conexión segura como SSL	
R10	Las redirecciones y los reenvíos están validados.	

Fuente: Autores

4.2 FACTORES DE RIESGO PARA LA ESTIMACIÓN

En el caso de la aplicación Plataforma Virtual, el algoritmo de transmisión MD5 es uno de los más importantes del momento. El algoritmo se considera débil y le recomendamos que continúe reemplazándolo con un algoritmo de cifrado más seguro. En el caso de que la aplicación SYSREC y Sistema de Información Integral utilice un algoritmo de cifrado, lo que indica una vulnerabilidad significativa, ya que ocurrirá cuando se acceda a los datos en texto sin formato, el atacante tendrá más facilidad para completar la aplicación correcta.

La capa de transporte presenta un riesgo de seguridad inadecuado en aplicaciones como los protocolos criptográficos como SSL (*Safe Socket Series*) para proteger la autenticación de tráfico, además, esto no se aplica a la criptografía de canales, servicios y recursos de datos. La aplicación de este protocolo contribuye a la protección, confidencialidad y verificación de la autenticidad de la información transmitida (Areito, 2016)

Aunque las aplicaciones de análisis pueden perder la Autenticación y Gestión de Sesiones, es recomendable reducir el plazo para cerrar las sesiones. En este momento, este tiempo se establece en el CAS (Servicio de Autenticación Central) y la sesión cerrada es de 30 minutos después de la autenticación del usuario, lo cual es mucho tiempo, por lo tanto, se recomienda reducir este período a 15 minutos para que no exista la oportunidad de atacar a la aplicación.

La metodología de evaluación de riesgos se utiliza para estimar la gravedad del riesgo del Top 10 de OWASP, en este caso, la metodología se utiliza para evaluar los dos riesgos identificados en aplicaciones analíticas. Para implementar la metodología, se publica un manual en el sitio web oficial de OWASP, en particular un artículo sobre la metodología de evaluación de riesgos (Zalewski, 2012).

Después de definir del riesgo potencial, se debe tener en cuenta la probabilidad de ocurrencia. Esta es una medida aproximada de la probabilidad de que un atacante descubra una vulnerabilidad y la aproveche. En esta evaluación, no es necesario ser preciso, es suficiente para determinar si la probabilidad de ocurrencia es baja, media o alta.

Esta evaluación debe tener en cuenta una serie de factores: el primer grupo se refiere a los factores que causan una amenaza, el objetivo es ver la probabilidad de que un grupo de ataques potenciales se lance hacia un ataque exitoso.

Hay una serie de opciones relacionadas con el factor y cada opción tiene un número entre 0 y 9, lo que sugiere la probabilidad de origen. Estos valores se utilizan para determinar la probabilidad de reconocimiento global de los riesgos identificados, existe la posibilidad de tener un fenómeno:

- De 0 a < 3 la probabilidad se califica como bajo.
- De 3 a < 6 la probabilidad se califica como medio.
- De 6 a 9 la probabilidad se califica como alto.

4.2.1 FACTORES RELACIONADOS CON EL AGENTE CAUSANTE DE LA AMENAZA

El primer conjunto de factores está conectado a un intermitente que crea una amenaza, por lo tanto, el objetivo es demostrar la probabilidad de que un grupo de ataque con éxito. Cualquier persona que pueda enviar datos no confiables al sistema, incluidos usuarios externos, usuarios internos, administradores y empleados con acceso privilegiado, puede convertirse en un agente de amenazas. Incluso los usuarios del

sistema que pueden intentar robar otras cuentas de usuario pueden considerarse usuarios malintencionados (Mateu C. , 2012).

Además, observe a los empleados que desean ocultar sus acciones, así como a los usuarios con contraseñas creíbles que puede utilizar para pasar por el sistema, puede ser cualquier persona que pueda alertarte cuando solicitas el ingreso al sitio. Otros usuarios de ciertos sitios web pueden acceder a otros peligros de cualquier página web u otro canal HTML, también puede encontrar la probabilidad de que pueda capturar el tráfico de la red a sus usuarios, aquí hay algunos factores asociados con la causa que causa la amenaza.

Nivel de conocimiento: refleja el conocimiento técnico del grupo de participantes.

- Sin conocimientos
- Algunos conocimientos técnicos
- Usuario avanzado de ordenador
- Conocimientos de redes y programación
- Conocimientos de intrusiones de seguridad

Motivación: para alentar a este grupo de invasores a detectar y utilizar esta vulnerabilidad.

- Baja motivación o ninguna recompensa
- Posible recompensa
- Recompensa alta

Oportunidades: este grupo tiene la oportunidad de que los invasores identifiquen y utilicen esta vulnerabilidad.

- Ningún acceso conocido
- Acceso limitado
- Acceso total

Tamaño: Número del grupo de atacantes.

- Desarrolladores
- Administradores de sistemas
- Usuarios de la intranet
- Socios
- Usuarios autenticados
- Usuarios anónimos de Internet

4.2.2 FACTORES PARA ESTIMAR EL IMPACTO

Es importante saber que hay dos tipos de efectos: el primero es el impacto técnico de la aplicación, los datos utilizados y la funcionalidad proporcionada. El segundo es el impacto comercial, la empresa que administra la aplicación, después de todo, el impacto en el negocio es mayor. Sin embargo, puede que no sea posible acceder a toda la información necesaria para identificar las consecuencias de realizar correctamente la vulnerabilidad, en este caso, todo debe informarse en detalle sobre los riesgos técnicos que le permiten a la empresa determinar el riesgo (Beust, 2015).

El impacto técnico se puede dividir en factores correspondientes a los dominios de seguridad tradicionales: confidencialidad, integridad, disponibilidad y control de responsabilidad, el objetivo es evaluar el alcance del impacto en el sistema en el que es vulnerable.

Algunos factores pueden incluir la pérdida o corrupción de datos, falta de integridad o acceso denegado, permitiendo que los scripts ejecuten ataques de scripts en el navegador de la víctima para capturar sesiones de usuario, eliminar sitios web, códigos maliciosos, usuarios directos, etc.

Instalar código malicioso en el navegador de la víctima, los usuarios malintencionados pueden obtener acceso no autorizado a datos o funciones de la aplicación, cada uno de estos factores representa un riesgo para todo el sistema si la cuenta de un tutor está en riesgo. Esto puede revelar información de uso y puede contener muchas cuentas, aquí hay algunos factores técnicos (López & Echeverry,

2014).

Pérdida de confidencialidad: divulgación de la cantidad y sensibilidad de la información y su confidencialidad.

- Revelación mínima de datos no sensibles
- Revelación mínima de datos críticos
- Amplia revelación de datos no sensibles
- Amplia revelación de datos críticos.
- Todos los datos revelados

Pérdida de integridad: Cantidad de datos se podrían corromper y el daño que sufre.

- Mínimo, datos ligeramente corruptos
- Mínimos datos seriamente dañados
- Gran cantidad de datos ligeramente dañados
- Todos los datos totalmente corruptos

Pérdida de disponibilidad: Servicios que se pueden ver interrumpidos y su vitalidad.

- Mínimo número de servicios secundarios interrumpidos
- Mínimo número de servicios primarios interrumpidos
- Gran número de servicios secundarios interrumpidos
- Gran número de servicios primarios interrumpidos
- Todos los servicios perdidos

4.2.3 FACTORES DE IMPACTO SOBRE EL NEGOCIO

El impacto en la sociedad se deriva del impacto técnico, pero del profundo conocimiento de lo que es importante para la empresa que utiliza la aplicación, como regla general, los riesgos deben tenerse en cuenta, teniendo en cuenta el impacto en la empresa, especialmente si el público está compuesto por gerentes, el riesgo comercial se

justifica por la inversión en la solución de problemas de seguridad (Quero, García, & Peña, 2017).

Muchas empresas tienen pautas sobre clasificación de activos y/o una declaración de impacto en el negocio que definen lo que es importante para su negocio, estas normas pueden ayudarlo a enfocarse en problemas de seguridad críticos. Si no están disponibles, solicite a las personas que entienden el sector que obtengan su opinión sobre puntos importantes.

La aplicación puede estar en peligro sin saberlo, la información podría ser robada o modificada y los costos del tratamiento podrían ser altos. Información, datos o características presentadas en los canales de comunicación con respecto a sus requisitos de confidencialidad e integridad. Es muy importante tener en cuenta su impacto en la reputación de la empresa y la vulnerabilidad de su comunidad (Areito, 2016).

Los factores que se describen a continuación son comunes a muchas empresas, debido a factores asociados con amenazas, vulnerabilidades e impactos técnicos.

Daño Financiero: Daño financiero resultado de la explotación de una vulnerabilidad.

- Menor al coste de arreglar la vulnerabilidad
- Leve efecto en el beneficio anual
- Efecto significativo en el beneficio anual
- Bancarrota

Daño sobre la reputación: La explotación de una vulnerabilidad tendría por resultado un daño sobre la reputación.

- Daño mínimo
- Pérdida de las cuentas principales
- Pérdida del buen nombre
- Daño sobre la marca

No conformidad: Exposición introduce la no conformidad.

- Violación leve
- Clara violación
- Violación prominente

Violación de la privacidad: Cantidad de información que facilite la identificación personal podría ser revelada.

- Un individuo
- Cientos de personas
- Miles de personas
- Millones de personas

4.2.4 USO DE LA HERRAMIENTA OWASP

Es una herramienta poderosa para ataques intensos, llamada pentesting, utilizada para controlar aplicaciones vulnerables. Cabe señalar que esta plataforma gratuita o multijugador es una herramienta que le permite utilizarla en diferentes sistemas operativos, como ya hemos mencionado. Esta prueba ejecuta Windows 8.1. Al instalar las herramientas ZAP de OWASP, primero debe tener la configuración deseada para las vulnerabilidades que afectan a las aplicaciones de prueba de ataque (OWASP, 2017).

Debe ejecutar e ingresar la URL de la página o el servidor de la misma manera que la víctima, luego un programa de análisis para identificar las vulnerabilidades. Tenga en cuenta que esta herramienta muestra cuatro tipos de alertas, como se muestra a continuación:

1. Advertencias de alta prioridad.
2. Aviso de prioridad.
3. Alertas de baja prioridad.
4. Notas informativas

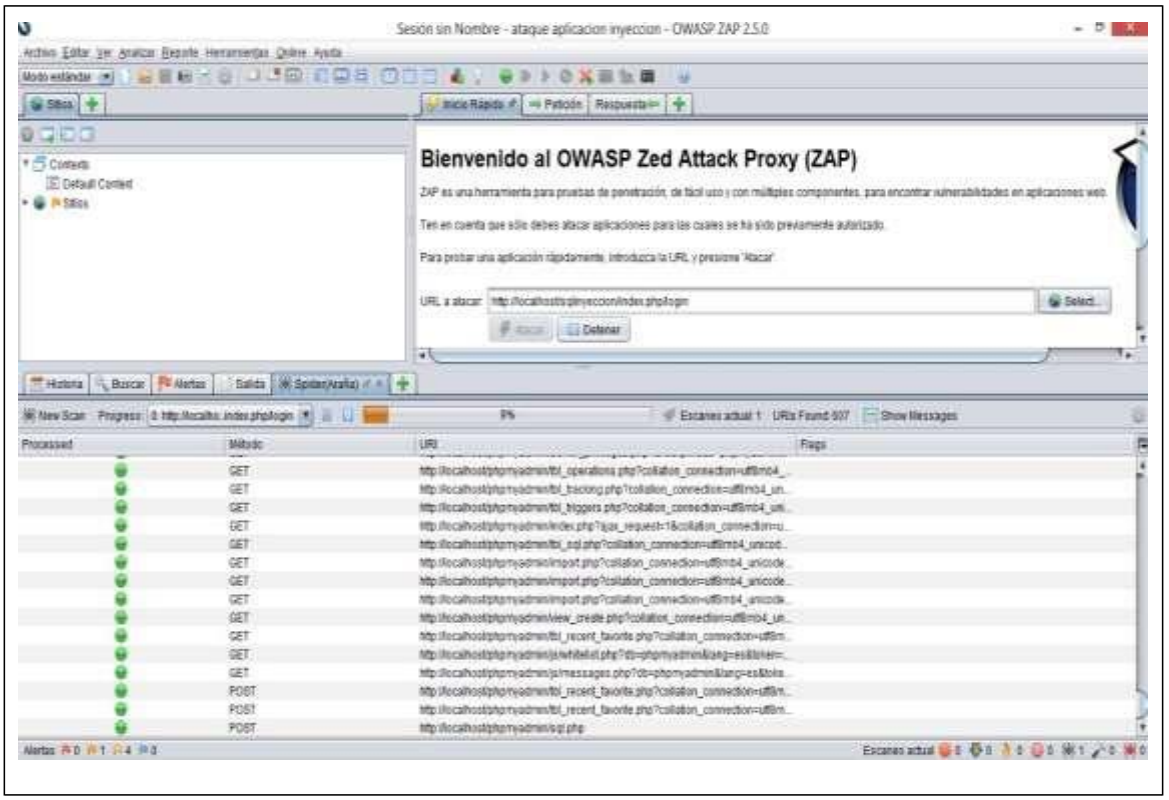
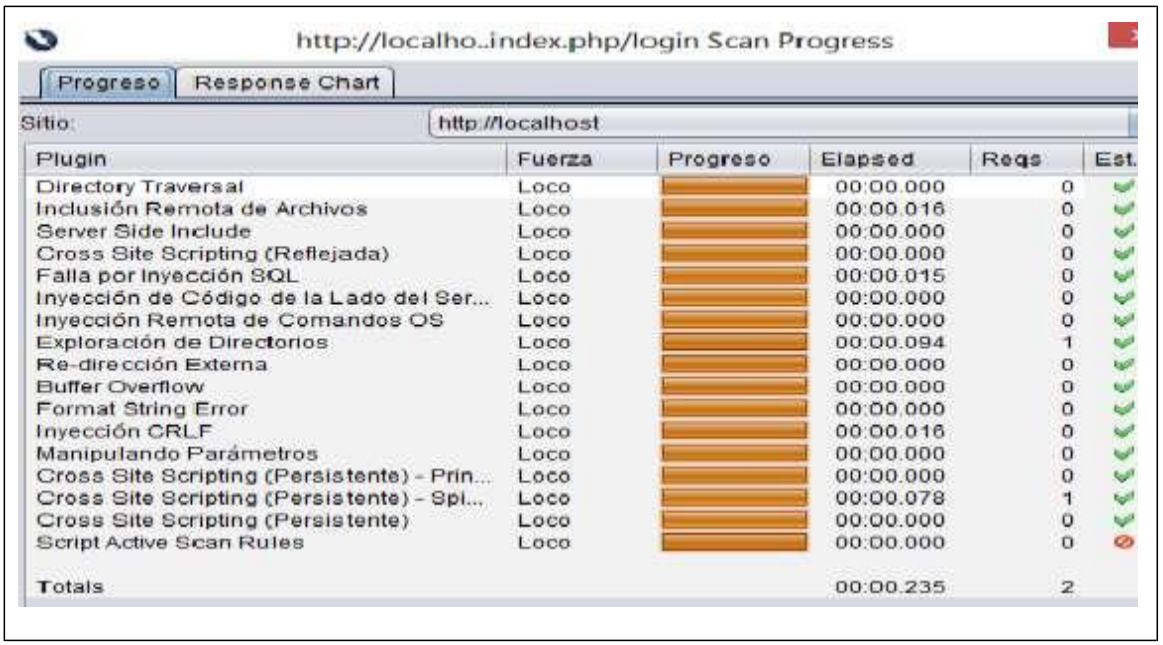


Figura 4.5. Proceso de escaneo para hallar vulnerabilidades en la aplicación
Fuente: Aplicación OWASP

La figura muestra que las aplicaciones analizan las solicitudes IAR que se envían a través del navegador para corregir errores o usan aplicaciones de seguridad directamente a la aplicación web diseñada bajo framework CodeIgniter.



Plugin	Fuerza	Progreso	Elapsed	Reqs	Est.
Directory Traversal	Loco		00:00.000	0	
Inclusión Remota de Archivos	Loco		00:00.016	0	
Server Side Include	Loco		00:00.000	0	
Cross Site Scripting (Reflejada)	Loco		00:00.000	0	
Falla por Inyección SQL	Loco		00:00.015	0	
Inyección de Código de la Lado del Ser...	Loco		00:00.000	0	
Inyección Remota de Comandos OS	Loco		00:00.000	0	
Exploración de Directorios	Loco		00:00.094	1	
Re-dirección Externa	Loco		00:00.000	0	
Buffer Overflow	Loco		00:00.000	0	
Format String Error	Loco		00:00.000	0	
Inyección CRLF	Loco		00:00.016	0	
Manipulando Parámetros	Loco		00:00.000	0	
Cross Site Scripting (Persistente) - Prin...	Loco		00:00.000	0	
Cross Site Scripting (Persistente) - Spi...	Loco		00:00.078	1	
Cross Site Scripting (Persistente)	Loco		00:00.000	0	
Script Active Scan Rules	Loco		00:00.000	0	
Totals			00:00.235	2	

Figura 4.6. Respuesta Escaneo de la Herramienta a la aplicación web
Fuente: Aplicación OWASP

Después de revisar una aplicación y cumplir con los requisitos de revisión ZAP de OWASP, se especifica un calendario en toda la aplicación, detecta errores y luego se inspecciona al 100%, puede encontrar el rango de respuestas a los tipos de amenazas y vulnerabilidades.

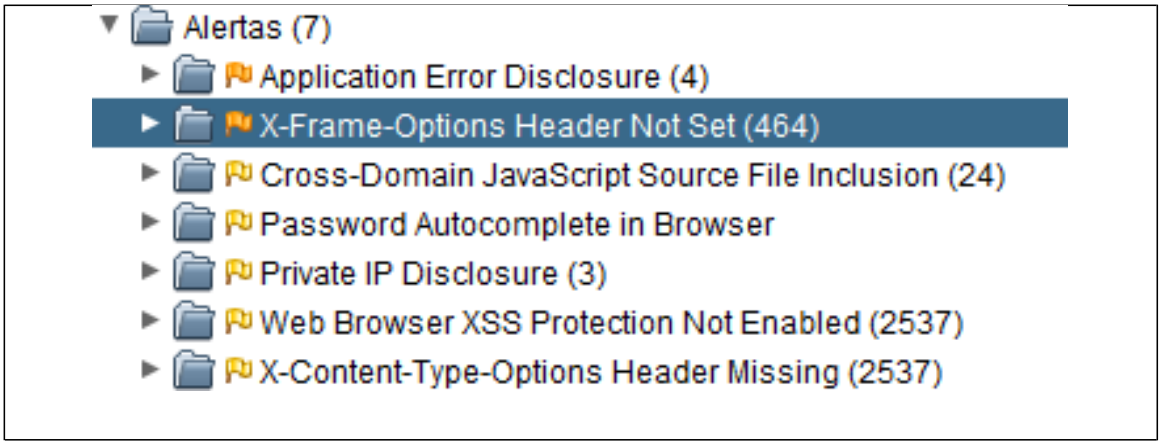


Figura 4.7. Alertas de la Herramienta al finalizar el escaneo
Fuente: Aplicación OWASP

En detalle, en el proceso de escaneo, puede verse que la aplicación incluye medidas de precaución integrales para el uso de la infraestructura y que los resultados de los ataques no utilizaron la inyección SQL, como se indica en el informe. , es posible que se usen otros tipos de ataques, pero no se enumeran específicamente para esta prueba. Las instrucciones para lanzar un ataque de inyección SQL no se encuentran en una aplicación que se va a probar. El programador puede así detectar la otra amenaza para evitar las vulnerabilidades de seguridad de los ataques, el análisis muestra los siguientes tipos de alertas:

- 2 alertas con prioridad media.
- 5 siguientes son de alerta con baja prioridad

4.2.5 DETERMINACIÓN DE LA GRAVEDAD DEL RIESGO

Para determinar la probabilidad esperada y el impacto esperado, es necesario calcular un nivel general de riesgo. En este caso, determina la probabilidad de baja, media o alta, lo que debe hacerse con la divulgación (Paredes, 2014).

Las estimaciones deben protegerse o reproducirse de modo que se pueda

considerar un procedimiento más formal para evaluar los factores y calcular el resultado. Cabe señalar que estas estimaciones están sujetas a muchas incertidumbres y que estos factores están destinados a lograr un resultado razonable. Inicialmente, se selecciona uno de los parámetros de cada factor y el número correspondiente se ingresa en la tabla, luego, toma el punto central y calcula la probabilidad de que esto suceda en el mundo.

A continuación, se presenta una prueba con valores para verificar los datos de un agente que libera los factores de amenaza y vulnerabilidad, el riesgo de almacenamiento criptográfico se indica en la aplicación SYSREC. Cada dimensión se aplica al número, lo que significa que es probable que los niveles aumenten y queden expuestos, luego agrega un grupo para compartir la probabilidad de un fenómeno global.

Tabla 4.10. Probabilidad de ocurrencia

Factores correspondientes al agente causante de amenaza	Nivel de habilidad	6
	Motivo	9
	Oportunidad	7
	Tamaño	5
	Factibilidad descubrimiento	9
Factores asociados a la vulnerabilidad	Factibilidad explotación	5
	Concienciación	9
	Detección de intrusión	8
Probabilidad de Ocurrencia Global= 7.125 (ALTA)		

Fuente: Autores

En este caso, el producto es 7.125, esta es una alta probabilidad. Además, es necesario descubrir los efectos técnicos generales y el impacto total en la empresa, ambos similares a los anteriores, en estos casos, es fácil determinar la respuesta cuando se alcanzan los valores más altos, medios o bajos, aunque la respuesta es clara, es aconsejable basar una evaluación factorial.

Inicialmente, el valor promedio de cada factor se calcula porque en el caso anterior, es menos de 3 menos, el promedio de 3 a 6 es promedio y alto de 6 a 9, para cada resultado de factor, una prueba con los valores Los números correspondientes están en la siguiente tabla, en este caso, los números se ingresan y se dividen en una serie de características evaluadas en cada uno.

La tabla proporciona datos sobre el riesgo de almacenamiento criptográfico

inestable en la aplicación SYSREC, en este caso, el efecto técnico general se estima en 7.25, por lo que se piensa que estos resultados son altos y que la empresa tiene que decidir sobre su estrategia que protegerá sus intereses.

Tabla 4.11 Impacto de ataque

Impacto Técnico	Perdida de confidencialidad	9
	Perdida de Integridad	7
	Perdida de disponibilidad	5
	Pérdida de control responsabilidad	8
Impacto Técnico Global = 7.25 (ALTO)		
Impacto sobre Negocio	Daño Financiero	9
	Daño a la Reputación	9
	No conformidad	5
	Violación de Privacidad	6
Impacto Global sobre el Negocio = 2.25 (BAJO)		

Fuente: Autores

A continuación, se muestra una prueba con valores para la verificación de datos en relación con un agente que emite la amenaza y los factores de vulnerabilidad. La siguiente tabla presenta datos sobre el riesgo de protección insuficiente del transporte en la Plataforma Educativa Virtual, el procedimiento es idéntico al del ejemplo anterior, el resultado es 6,375, lo que significa que la probabilidad de este riesgo es de uso promedio.

Tabla 4.12. Probabilidad de ocurrencia

Factores correspondientes al agente causante de la amenaza	Nivel de Conocimiento	4
	Motivación	7
	Oportunidad	8
	Tamaño	6
Factores asociados a la Vulnerabilidad	Facilidad de descubrimiento	7
	Facilidad de explotación	4
	Conocimiento	7
	Detección de Intrusión	8
Probabilidad de ocurrencia global=6.375 (MEDIA)		

Fuente: Autores

De igual manera presenta los detalles del riesgo de que el nivel de tráfico no sea suficiente en la Plataforma Educativa Virtual, en este caso, la consecuencia técnica global estimada es de 6.75 y el impacto total en la compañía es de 5.75, que es el promedio. Con estos resultados, una empresa debe determinar qué estrategia debe considerarse en función de sus intereses.

Tabla 4.13 Impacto del ataque

Impacto Técnico	Perdida de confidencialidad	8
	Perdida de Integridad	7
	Perdida de disponibilidad	4
	Pérdida de control responsabilidad	8
Impacto Técnico Global = 6.75 (MEDIO)		
Impacto sobre Negocio	Daño Financiero	7
	Daño a la Reputación	7
	No conformidad	5
	Violación de Privacidad	4
Impacto Global sobre el Negocio = 5.75 (MEDIO)		

Fuente: Autores

Después del análisis de las tablas anteriores, está claro que existe el riesgo de un almacenamiento criptográfico peligroso o presenta riesgos de protección insuficiente de la información, además, el impacto técnico general y el impacto general en el negocio son mejores.

- **IDENTIFICACIÓN DE RIESGOS EN BASE AL TOP 10 DE OWASP**

Sobre la base de la comparación y el análisis, se han identificado los siguientes riesgos:

R7: ruta criptográfica incierta, generando robo de información confidencial, pudiendo existir robo de identidad y falsificación de documentos.

R9: Protección insuficiente del tráfico, generándose el cierre de las aplicaciones de tal manera que los estudiantes no pueden cargar sus trabajos y de esta manera reprobar materias.

4.3 DISEÑO DE LA PROPUESTA DE SOLUCIÓN

La seguridad informática se encarga de diseñar, definir protocolos, horas de operación, errores, planes de contingencia y perfiles de usuario, así como el poder para garantizar un alto nivel de seguridad en las organizaciones requeridas; como resultado, se minimiza el impacto de los riesgos en la productividad de los trabajadores y las organizaciones.

La seguridad informática se desarrolló para proteger los recursos tecnológicos, como infraestructura, usuarios e información. La infraestructura es esencial para organizar, gestionar y almacenar información, la seguridad informática en esta área garantiza el funcionamiento correcto del equipo y le advierte sobre fallas. Los usuarios que utilizan una estructura tecnológica, el campo de la comunicación y la gestión de la información son usuarios, todo el sistema debe estar protegido para que su uso no comprometa la seguridad de la información. Además, debe evitar la vulnerabilidad de la información procesada o archivada, la información es el recurso principal que utiliza y reside en la infraestructura informática y es utilizado por los usuarios.

4.3.1 BUENAS PRÁCTICAS

Las buenas prácticas se refieren a los sistemas de calidad que determinan las condiciones bajo las cuales los datos recibidos se planifican, procesan, monitorean, registran y archivan para garantizar su confiabilidad, protección de prevalencia, impacto positivo, difusión de experiencias e información obtenida para que puedan comunicarse y realizarse en otros contextos (Mateu C. , 2014).

Criterios de selección

Las buenas prácticas, que se describen en detalle a continuación, tienen al menos los criterios requeridos:

- **Documentada:** sirve de referencia para otros y les ayuda a mejorar sus procesos. Esta es una comprensión importante de las mejores prácticas. Debe documentarse para que la información pueda transferirse fácilmente a otra organización para saber cómo proceder.

- **Accesible:** para usar en cualquier lugar y con cualquier persona.

- **Basado en procesos y metodologías:** en la práctica, existen metodologías cuidadosamente seleccionadas para cambiar el centro de prioridad.

- **Prueba e implementación:** Las mejores prácticas del proceso son las mejores, la evaluación o el proceso de evaluación.

- **Establecer la capacidad para establecer metas:** la mejor práctica para satisfacer una necesidad definida, después de una evaluación cuidadosa de las características específicas de un grupo de población específico que necesita ser modificado y mejorado, y que por lo tanto tiene un propósito Específico, relevante y realista.

- **Transferible:** como objetivo, la transferencia de información debe facilitarse en los métodos, herramientas y enfoques utilizados para brindar experiencia o iniciativas que tengan en cuenta las mejores prácticas.

- **Sostenibilidad:** los ingresos superan los costes. La relación costo / ingreso es mejor que una práctica similar.

- **Eficiente:** la relación entre el costo del ingreso es mejor que la de métodos similares.

- **Eficaz:** resultados esperados.

Estas características son los criterios clave para elegir las mejores prácticas.

4.3.2 BUENAS PRÁCTICAS DE SEGURIDAD PARA EL DESARROLLO WEB

Este es un conjunto de elementos o acciones implementadas para garantizar la seguridad de las aplicaciones web desde el desarrollo inicial y el mantenimiento, para implementar métodos avanzados de seguridad de red, debe considerar lo siguiente.

Un paso importante que debe estar preparado para registrar excepciones y proporcionar una respuesta de control es que los usuarios finales usen los datos correctamente, para hacer esto, debe realizar verificaciones del lado del cliente utilizando JavaScript como del lado del servidor por medio de rutinas del lenguaje de programación (Paredes, 2014).

Son muy importantes porque las comprobaciones o desactivaciones del lado del cliente pueden ignorarse, esto se hace filtrando los datos proporcionados por el usuario

del lado del servidor. Se recomienda que utilice listas blancas que se pueden generar usando expresiones regulares que impiden la asignación directa de valores obtenidos de la entrada en la variable para garantizar que los datos se verifiquen correctamente, los controles deben hacerse correctamente porque puede ingresar líneas de código malicioso para obtener información sobre la aplicación o sus usuarios, lo que puede representar un riesgo para las inyecciones de SQL, XSS y CSRF.

No se debe olvidar configurar sesiones que le permitan hacer un seguimiento de los usuarios, mantener valores variables en el sitio sin tener que usar campos ocultos en los módulos y limitar el acceso a ciertos elementos, es muy importante monitorear la sesión, iniciarla correctamente y cerrarla para evitar una violación de seguridad.

Como recomendación, debe especificar: usar sesiones cuando un usuario inicia limitado a la aplicación; la sesión siempre está activa en cualquier objeto visitante para mostrarla; de lo contrario, el usuario debe redirigir para iniciar la sesión; y cierre la sesión correctamente cuando un usuario visite el sitio. Los riesgos de uso indebido incluyen: acceso a recursos limitados, el robo de datos personales de otros usuarios y el uso inadecuado de los recursos de la aplicación (Zalewski, 2012).

La administración de datos del usuario final debe realizarse con protección adicional, lo primero que se debe evaluar es el cifrado de un canal de comunicación para el intercambio cliente-servidor. Es muy importante mantener la información proporcionada por los usuarios en un lugar seguro, al comienzo de la sesión (nombre de usuario, contraseña) y al momento de la inscripción, en los formularios (nombre, apellido, dirección, correo electrónico, teléfono). Se recomienda que instale HTTPS utilizando la certificación del servidor de aplicaciones web y configure el servidor para usarlo en la configuración principal o en cada host virtual como un riesgo, el tráfico web puede estar mediado y refleja información confidencial sobre la ruta (una en el medio).

En Internet, cuando recibe un desarrollo específico, puede personalizar los mensajes de error que los usuarios pueden necesitar para evitar información sobre su sitio, por lo tanto, es necesario incluir posibles errores en la aplicación y la información mostrada a los usuarios, ya que el nombre indica el mal funcionamiento de la seguridad,

por lo que se recomienda utilizar mensajes de error comunes según sea necesario. La exposición involuntaria a la instalación e información de configuración del sitio (versiones, software utilizado, canales del sistema) puede resultar en un riesgo de mala administración.

La información es el recurso más importante procesado por las aplicaciones web, por lo que es el más vulnerable a la seguridad informática, por lo tanto, debe ser protegido de una manera segura. Para este fin, es recomendable tomar las medidas necesarias, tales como: reducir el acceso no deseado a la información procesada en la aplicación, crear una base de datos de servicios (Beust, 2015).

Los datos simplifican la configuración y evitan que los usuarios, las contraseñas y la configuración predeterminada como riesgo de uso indebido, es posible obtener información de la base de datos (servicios y contenidos).

A veces, la aplicación debe usar características o contenido de terceros (formulario de validación, calendarios, autenticación usando auth con Twitter o Facebook) para investigar las vulnerabilidades actuales, es muy importante utilizar el rendimiento mínimo apropiado y sin instalar ningún hardware o características que no se utilizarán.

Si está instalando bibliotecas, módulos o complementos de terceros, debe instalar la última versión estable e instalar las actualizaciones de seguridad adecuadas. Los riesgos dependen del tipo de vulnerabilidad del sujeto, pero XSS, CSRF, inyección SQL, sesiones de vuelo, escalamiento de privilegios, etc.

4.3.3 ESTRATEGIA

La política de seguridad permite a los administradores de seguridad proteger la disponibilidad, integridad y confidencialidad de los datos en los sistemas de información empresarial. La estrategia debe aplicarse sistemáticamente en la práctica, como medida de precaución, e incluir planes de contingencia para hacer frente a circunstancias imprevistas.

Los gerentes deben definir el tiempo, el capital y el esfuerzo necesarios para invertir en el desarrollo de medidas y controles de seguridad adecuados.

Todas las organizaciones deben analizar sus necesidades específicas y determinar los recursos y necesidades de sus programas. Cada sistema informático, entorno y estrategia organizacional son diferentes, lo que hace que cada servicio y estrategia de seguridad sean específicos. Aquí hay algunos principios a tener en cuenta al configurar una buena estrategia de seguridad:

a. Actualización continua de herramientas y métodos de seguridad informática.

Organizaciones que ayudan a los administradores de seguridad a identificar los métodos, herramientas y métodos de ataque más probables. Este dominio de conocimiento siempre debe actualizarse para evitar ignorancia, vulnerabilidades y vulnerabilidades de seguridad.

b. Definición de estrategias proactivas e inesperadas.

Los planes de seguridad de cada organización deben incluir estrategias de prevención de ataques con una serie de pasos que reducen la vulnerabilidad de las políticas de seguridad. La evaluación continua de las debilidades ayuda a desarrollar una estrategia preventiva. Una estrategia no planificada es una estrategia que sigue a un ataque cuando el daño causado por el ataque es evaluado, corregido, documentado y resumido por la experiencia.

c. Grabar ataques en entornos de prueba.

La implementación de ataques de simulación en entornos de prueba o laboratorios proporciona una evaluación de las vulnerabilidades y los ajustes adecuados a las instrucciones y medidas de seguridad. Estas pruebas no deben realizarse en sistemas reales porque el resultado podría ser desastroso, pero es muy importante usarlos debido a los riesgos y consecuencias de los ataques.

d. Inspección de incidencias

Se recomienda crear un equipo de gestión de eventos. Este grupo debe estar involucrado en el trabajo de seguridad preventiva. Deben definir instrucciones, herramientas, encuestas y aplicar tareas de control de incidentes a los ataques del sistema.

4.3.4 GENERACIÓN DE BUENAS PRÁCTICAS EN EL DESARROLLO DE SOFTWARE

Después del análisis de las aplicaciones académicas y financieras tienen los siguientes riesgos relacionados con las características que representan y el propósito social. Todo lo que se pretende y con las características técnicas de cada uno de ellos:

- Riesgo 7: Ruta criptográfica incierta.
- Riesgo 9: Protección insuficiente en términos de tráfico.

Sobre la base de los riesgos anteriores, se describen las siguientes prácticas recomendadas, que deben tenerse en cuenta en el desarrollo y el servicio de la Universidad Central del Ecuador para utilizar aplicaciones que garanticen la navegación, privacidad e integridad de los datos y la información mostrada.

Respecto al riesgo 7: almacenamiento criptográfico no confiable Algunas aplicaciones web no ofrecen una protección adecuada de datos confidenciales, así como la autenticación a través de un mecanismo de cifrado o *sputtering*. La información o datos pueden ser protegidos para evitar el robo de identidad o falsificar datos académicos.

Mejores prácticas de riesgo 1. Un almacén criptográfico no confiable debe identificar mucha privacidad y requiere cifrado. Por ejemplo, la contraseña, los datos personales de las personas que se monitorean deben incluirse en:

Evaluar todos los riesgos que pueden afectar los datos, teniendo en cuenta los ataques internos y los usuarios externos. Proporcionar información confidencial de encriptación donde sea que esté almacenada por mucho tiempo.

- Compruebe el cifrado de las copias de seguridad almacenadas en el exterior.
- Asegúrese de que las contraseñas se administran y almacenan por separado.
- Los usuarios no autorizados permiten el acceso solo a los usuarios autorizados.
- Utilice un algoritmo estándar seguro.
- Las teclas fuertes están protegidas contra accesos no autorizados.
- Asegúrese de que los algoritmos potentes, como la transmisión, admitan claves.
- Desarrollar un plan de cambio de contraseña.

Con respecto al riesgo 7: protección insuficiente a nivel de transporte, las aplicaciones, el secreto y la integridad del tráfico a menudo no validan, cifran y protegen una red segura. Cuando esto sucede, esto se debe al uso de algoritmos débiles, la verificación expira, no es válida o simplemente es engañosa.

Mejores prácticas relacionadas con el riesgo 9: El nivel de transporte no debe tener suficiente protección para demasiada protección del transporte, lo que puede afectar el formulario de solicitud. Por lo tanto, es fácil solicitar SSL para toda la aplicación, por alguna razón, algunas aplicaciones SSL solo se utilizan para acceder a páginas privadas. Otros SSL utilizan solo páginas "críticas", pero pueden revelar identificadores de sesión y otra información confidencial. Se aplica lo siguiente:

Use SSL en las páginas más importantes y redirija las aplicaciones que no son SSL a la página donde existe.

- Configure la función segura en cada cookie de mayor riesgo.
- Configurar el servidor SSL para encontrar un potente algoritmo.
- Asegúrese de que el certificado sea válido, no haya caducado o no haya sido revocado y sea apropiado para todas las áreas utilizadas por la aplicación.
- Se deben usar sistemas anteriores y otros sistemas SSL u otras tecnologías de encriptación.

5. CONCLUSIONES

- Del análisis de vulnerabilidades de las aplicaciones web desarrolladas por la Universidad Central del Ecuador se determinó que existe una ruta criptográfica incierta e insuficiente protección del tráfico de información.

- Mediante la matriz comparativa se pudo establecer que las aplicaciones críticas son: el Sistema de Recaudaciones Sysrec, el Sistema de Información Integral - Módulo Académico y la Plataforma Educativa Virtual.

- Se procedió a evaluar los riesgos, vulnerabilidades, amenazas e impactos, respaldándose en el Top Ten de OWASP, determinando la existencia de una vulnerabilidad media alta la cual puede inclinarse a ser mayor.

- Los riesgos evidentes son almacenamiento criptográfico inseguro, así como protección insuficiente en la capa de transporte, producida porque las aplicaciones no pueden cifrar y proteger la confidencialidad e integridad del tráfico de red sensible.

- Del mismo modo se materializó una lista de buenas prácticas (anexo #10), con la finalidad de garantizar el funcionamiento de las aplicaciones lográndose de esta forma dar una corrección efectiva a los riesgos detectados o aquellos que puedan surgir durante su funcionamiento, tomando en cuenta los hallazgos de la investigación.

6. RECOMENDACIONES

- Eliminar el riesgo de almacenamiento criptográfico inseguro dado su elevado impacto negativo para la utilización efectiva de las aplicaciones académicas y financieras, mediante la comprobación del cifrado de las copias de seguridad almacenadas en el exterior, así como no permitir el acceso a usuarios no autorizados y administrar contraseñas y su almacenamiento por separado, también hacer uso del algoritmo estándar seguro, de forma tal que se garantice una utilización efectiva de la información contenida en la base de datos.

- Crear una guía estandarizada de la información a ser recopilada de forma tal que se pueda brindar una información ordenada y oportuna y que la misma pueda ser analizada de forma eficiente según lo planteado en la OWASP, a través del desarrollo de planes de cambios de contraseña, protección de las teclas fuertes contra accesos no autorizados y garantizar que los algoritmos potentes tales como la transmisión admitan claves.

- Automatizar a futuro el proceso de estudio de vulnerabilidades de las aplicaciones académicas y financieras tomando en cuenta las especificaciones derivadas del uso de la guía estandarizada en la recolección de la información con la utilización de sistemas anteriores y otros sistemas SSL.

- Desarrollar un análisis sistemático de los aspectos a ser tomados en cuenta tales como la configuración de la función segura en cada cookie de mayor riesgo, del mismo modo se configurará el servidor SSL con la finalidad de encontrar un potente algoritmo en la utilización futura de las aplicaciones académicas y financieras en plena concordancia con los parámetros contenidos en las actualizaciones OWASP 2013.

- Solicitar SSL para las aplicaciones de forma tal que su utilización no se limite a páginas privadas o críticas de forma tal que se garantice identificadores de sesión, así como el correcto uso de la información confidencial.

7. REFERENCIAS BIBLIOGRÁFICAS

Areito, J. (2016). *Seguridad de la información. Redes, Informática y sistemas de información.* Madrid: Cengage Learning Paraninfo S.A.

Beust, C. (2015). *Programación Java Server con J2EE.* Barcelona: Anaya Multimedia.

Cabré, T. (2015). *Terminología y buenas prácticas.* Barcelona: Publifarum.

Cardador, A. L. (2014). *Implantación de Aplicaciones Web en entornos Internet, Intranet y Extranet.* Málaga: ic editorial.

Hernández, E. (2017). Comaparación de los modelos OSI y TCP/IP. Huejutla, Huejutla, Mexico.

Latorre, M. (2018). *Historia de las Web.* Perú: Universidad Marcelino Champagnat.

López, M., & Echeverry, C. (2014). *Servicios de gestión de conocimiento utilizando la computación en Nube.* Manizales: Universidad nacional de Colombia.

Marini, E. (2012). El modelo cliente/servidor. 11.

Mateu, C. (2012). *Desarrollo de Aplicaciones Web*. Cataluña: Eureca Media, SL.

Mateu, C. (2014). *Seguridad de las aplicaciones web.* Tarragona: Eureca Media SL.

Montoya, C. E., Uribe, C. A., & Rodríguez, L. E. (2013). Seguridad en la configuración del servidor web Apache. *INGE CUC*, 31-38.

OWASP. (2017). *Los díez riesgos más criticos en aplicaciones web*. Obtenido de owasp.org

OWASP. (2017). *The OWASP™ Foundation*. Obtenido de The OWASP™ Foundation: The OWASP™ Foundation

Paredes, B. (2014). *Especificaciones técnicas para medir vulnerabilidades informáticas.* México D.F.: Trillas.

Quero, E., García, A., & Peña, J. (2017). *Mantenimiento de Portales de Información: explotación de sistemas informáticos.* Madrid: P.S.A. International Thomson Editores.

Rodríguez, M. (2017). *Scrum desde cero.* Madrid: Mc. Graw-Hill.

Zalewski, M. (2012). *La web enredada: guía para la seguridad de aplicaciones web modernas.* Madrid: Anaya.

8. ANEXOS

Anexo #1

OWASP Top 10 Application Security Risks - 2017

T10 OWASP Top 10 Application Security Risks – 2017

A1 – Injection	Injection flaws, such as SQL, OS, XXE, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
A2 – Broken Authentication and Session Management	Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities (temporarily or permanently).
A3 – Cross-Site Scripting (XSS)	XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user supplied data using a browser API that can create JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
A4 – Broken Access Control	Restrictions on what authenticated users are allowed to do are not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.
A5 – Security Misconfiguration	Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, platform, etc. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date.
A6 – Sensitive Data Exposure	Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.
A7 – Insufficient Attack Protection	The majority of applications and APIs lack the basic ability to detect, prevent, and respond to both manual and automated attacks. Attack protection goes far beyond basic input validation and involves automatically detecting, logging, responding, and even blocking exploit attempts. Application owners also need to be able to deploy patches quickly to protect against attacks.
A8 – Cross-Site Request Forgery (CSRF)	A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. Such an attack allows the attacker to force a victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim.
A9 – Using Components with Known Vulnerabilities	Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.
A10 – Underprotected APIs	Modern applications often involve rich client applications and APIs, such as JavaScript in the browser and mobile apps, that connect to an API of some kind (SOAP/XML, REST/JSON, RPC, GWT, etc.). These APIs are often unprotected and contain numerous vulnerabilities.

Anexo #2
Glosario

Glosario de términos básicos

Control de acceso: una forma de restringir el acceso a archivos, funciones de referencias, URLs y datos basados en la identidad de los usuarios o grupos a que pertenecen.

Address Space Layout Randomization (ASLR): una técnica para ayudar a proteger contra ataques de desbordamiento de búfer.

Aplicaciones de seguridad: La seguridad a nivel de aplicación se centra en el análisis de los componentes que conforman la capa de aplicación del -Modelo de Referencia de Interconexión de sistema abierto (modelo OSI), en lugar de centrarse en por ejemplo el sistema operativo subyacente o redes conectadas.

Verificación de seguridad en aplicaciones: la evaluación técnica de una aplicación contra el ASVS.

Informe de verificación de seguridad de aplicación: un informe que documenta los resultados generales y análisis de apoyo producido por el verificador para una aplicación particular.

Autenticación: verificación de la identidad reivindicada de usuario de una aplicación.

Verificación automatizada: el uso de herramientas automatizadas (herramientas de análisis dinámico, las herramientas de análisis estático o ambos) que utilizan firmas de vulnerabilidad para encontrar problemas.

Puertas traseras: un tipo de código malicioso que permite el acceso no autorizado a una aplicación.

Lista negra: una lista de datos u operaciones que no se permiten, por ejemplo, una lista de caracteres que no se permite como entrada.

Hojas de Estilos en Cascada (CSS): un lenguaje de hoja de estilo utilizado para describir la semántica de la presentación del documento escrito en un lenguaje de marcado, como HTML.

Autoridad de certificación (CA): una entidad que emite los certificados digitales.

Seguridad de las comunicaciones: la protección de datos de aplicaciones cuando se transmite entre los componentes de aplicación, entre clientes y servidores y entre sistemas externos y la aplicación.

Componente: una unidad independiente de código, con interfaces de red y disco asociadas que se comunica con otros componentes.

Cross-Site Scripting (XSS): una vulnerabilidad de seguridad se encuentra típicamente en aplicaciones que permiten la inyección de secuencias de comandos de cliente en contenido web.

Módulo criptográfico: Hardware, software o firmware que implementa algoritmos criptográficos o genera claves criptográficas.

Ataques de denegación de servicio (DoS): la inundación de una aplicación con más peticiones que puede manejar.

Verificación del diseño: la evaluación técnica de la arquitectura de seguridad de una aplicación.

Verificación dinámica: el uso de herramientas automatizadas que utilizan firmas de vulnerabilidad para encontrar problemas durante la ejecución de una aplicación.

Sistemas externos: una aplicación de servidor o servicio que no es parte de la aplicación.

FIPS 140-2: un estándar/norma que puede utilizarse como base para la verificación del diseño y aplicación de módulos criptográficos

Identificador único global (GUID): un número de referencia único utilizado como un identificador de software.

Lenguaje de marcado de hipertexto (HTML): el lenguaje de marcado principal para la creación de páginas web y otra información mostrada en el navegador web.

Hyper Text Transfer protocolo (HTTP): un protocolo de aplicación para sistemas de información distribuido, colaborativo hipermedia. Es la base de datos de comunicación de la World Wide Web.

Validación de entrada: la canonización y la validación de entrada de usuario no es de confianza.

Protocolo ligero de acceso a directorios (LDAP): un protocolo de aplicación para el acceso y mantenimiento de servicios de información de directorio distribuida sobre una red.

Código malicioso: código introducido en una aplicación durante su desarrollo desconocido al dueño de la aplicación, que elude la política de seguridad de la aplicación.

Malware: código ejecutable que se introduce en una aplicación en tiempo de ejecución sin el conocimiento del usuario de la aplicación o el administrador.

Proyecto Abierto de Seguridad en aplicación Web (OWASP): es una comunidad libre y abierta en todo el mundo enfocada en mejorar la seguridad de software en aplicaciones. Nuestra misión es hacer «visible», la seguridad de aplicaciones para que personas y organizaciones pueden tomar decisiones informadas sobre los riesgos de seguridad de la aplicación.

Codificación de salida: la canonización y la validación de solicitud de salida para los navegadores Web y sistemas externos.

Información de identificación personal (IPI): es información que puede utilizarse por sí solo o con otra información para identificar, contactar o localizar a una sola persona, o para identificar a un individuo en contexto.

Arquitectura de seguridad: una abstracción del diseño de una aplicación que identifica y describe los controles de seguridad sobre dónde y cómo se utilizan, identifica y describe la ubicación y la sensibilidad de los datos de usuario y la aplicación.

Configuración de seguridad: la configuración de tiempo de ejecución de una aplicación que afecta a cómo se utilizan los controles de seguridad.

Control de seguridad: una función o componente que realiza una comprobación de seguridad (por ejemplo, una verificación de control de acceso) o cuando resultados llamados resultan en efecto de seguridad (por ejemplo, generando un registro de auditoría).

SQL Injection (SQLi): una técnica de inyección de código utilizada para atacar aplicaciones de datos, en que se insertan sentencias SQL maliciosas en un punto de entrada.

Verificación estática: el uso de herramientas automatizadas que utilizan firmas de vulnerabilidad para encontrar problemas en el código fuente de la aplicación.

Objetivo de la verificación (TOV): si usted está realizando una verificación de seguridad en la aplicación según los requisitos del ASVS, la verificación será de un uso particular. Esta aplicación se llama "El objetivo de la verificación" o simplemente el TOV.

Modelado de Amenazas: una técnica que consiste en desarrollar cada vez más arquitecturas refinadas de seguridad para identificar agentes de amenaza, las zonas de seguridad, controles de seguridad y recursos técnicos y de negocios importantes.

Seguridad de capa de transporte: protocolos criptográficos que proporcionan la seguridad de las comunicaciones por Internet

Fragmentos de URL/URI/URL: un identificador uniforme de recursos es una cadena de caracteres utilizado para identificar un nombre o un recurso web. Un localizador uniforme de recursos a menudo se utiliza como una referencia a un recurso.

Aceptación la prueba del usuario (UAT): tradicionalmente un entorno de prueba que se comporta como el entorno de producción donde se realizan todas las pruebas de software antes de desplegar la aplicación en vivo.

Verificador: la persona o equipo que se está revisando una aplicación contra los requisitos del ASVS.

Lista blanca: una lista de datos permitidos u operaciones, por ejemplo, una lista de caracteres permitidos para realizar la validación de entrada.

XML: un lenguaje de marcado que define un conjunto de normas de codificación de documentos.

Anexo #3

Acta de Constitución Sistema de Legislación Universitaria

Información del Documento

TÍTULO:	Acta de constitución
SUBTÍTULO:	Sistema de Legislación Universitaria
VERSIÓN:	1
ARCHIVO:	ActaDeConstitucionVs1.docx
AUTOR:	Fátima Tobar, Fernando Santamaría
ESTADO:	Final

Lista de Cambios

VERSIÓN	FECHA	AUTOR	DESCRIPCIÓN
1.0.0	30/03/2015	Fátima Tobar, Fernando Santamaría	Emisión inicial

Cualquier otro nombre o nombres de productos usados en este documento son marcas registradas o marcas comerciales de sus respectivos propietarios.

1 Información del proyecto

1.1 Datos del proyecto

Dependencia	Secretaria General
Responsable de la dependencia	Dr. Silvio Toscano
Responsable principal del proceso	Jeffrey Jara
Fecha de preparación	30-03-2015

1.2 Patrocinadores del proyecto (responsables del proceso)

NOMBRE	CARGO	DEPENDENCIA
Jeffrey Jara		Secretaria General
Silvio Toscano	Secretario General	Secretaria General

Anexo #4

Sistema Integral de Información Universitaria

Sistema Integral de Información Universitaria

Sistema Integral de Información Universitaria pretende cubrir las todas las necesidades institucionales y externas, convirtiéndose en una herramienta sólida y robusta que permita el ingreso de información, análisis y toma de decisiones. Este Sistema integrará los siguientes módulos:

Módulo de gestión académica incluirá el módulo de planificación académica que a su vez se integrará con el sistema de titulación. Así mismo permitirá realizar la evaluación al desempeño académico como también la integración con la Plataforma Educativa Virtual y el seguimiento al silabo.

Módulo de investigación: registro de participantes del proyecto, número de horas involucradas en el proyecto, fecha inicio y fecha fin

Módulo de vinculación con la sociedad: registro de proyectos de vinculación con la sociedad en los que participan docentes y estudiantes de cada una de las carreras de la institución número de horas involucradas en el proyecto, fecha inicio y fecha fin.

Módulo de gestión de talento humano: gestión y administración del historial de los servidores de la institución.

Módulo de integración con el sistema de recaudaciones: automatización de la comunicación entre el sistema de recaudaciones con la entidad financiera correspondiente.

Módulo de Posgrado: comprende las fases de registro de postulante, postulación, declaratoria de idoneidad, evaluación de méritos, carga de calificaciones de la etapa de oposición y presentación de resultados.

Plataforma Educativa Virtual de la Universidad Central del Ecuador, la misma que está basada en Moodle y está orientada para apoyar los procesos de enseñanza-aprendizaje a través del entorno virtual, la comunidad universitaria deberá utilizar exclusivamente ésta plataforma, pues se utilizará como apoyo en las siguientes áreas:

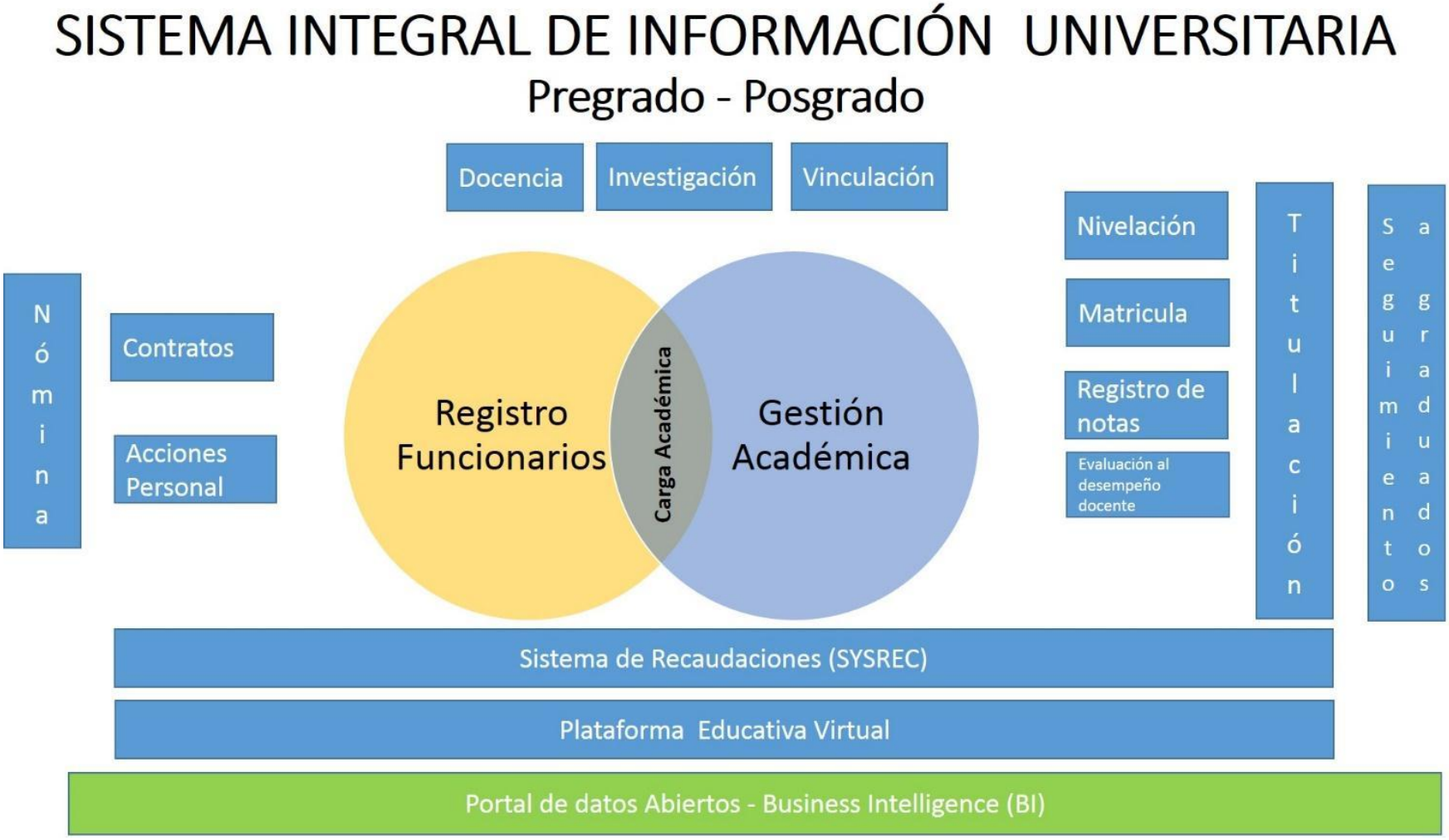
Docencia en la modalidad presencial sea este de Grado o Posgrado, para apoyo a las actividades que se desarrollan en clase presencial, fomentando el aprendizaje colaborativo, manejo de portafolio académico para el docente y estudiante.

Docencia en la modalidad a Distancia, semipresencial o virtual sea este de Grado o Posgrado, como herramienta fundamental para el desarrollo del proceso de enseñanza – aprendizaje, manejo de portafolio académico para el docente y estudiante.

Formación docente a cargo del Instituto de Capacitación Pedagógica, en donde el docente podrá participar en cursos para mejorar sus competencias profesionales y de docencia.

En UCE- Virtual el docente podrá utilizar todos los recursos y actividades que la plataforma ofrece para realizar el acompañamiento virtual de la asignatura que imparte y de los cursos de capacitación respectivamente. El ingreso se realizará a través de la dirección: uvirtual.uce.edu.ec

1.1. Descripción gráfica del proyecto:



Anexo #5
OWASP Risk Calculation

OWASP Risk Calculation

Each risk is calculated using generic vulnerability facts, based on the OWASP Risk Rating Methodology [1]...

Threat Agents	Attack Vectors	Weakness Prevalence	Weakness Detectability	Technical Impacts	Business Impacts
App Specific	Easy	Widespread	Easy	Severe	App / Business Specific
	Average	Common	Average	Moderate	
	Difficult	Uncommon	Difficult	Minor	

...but impact is environment and business specific!

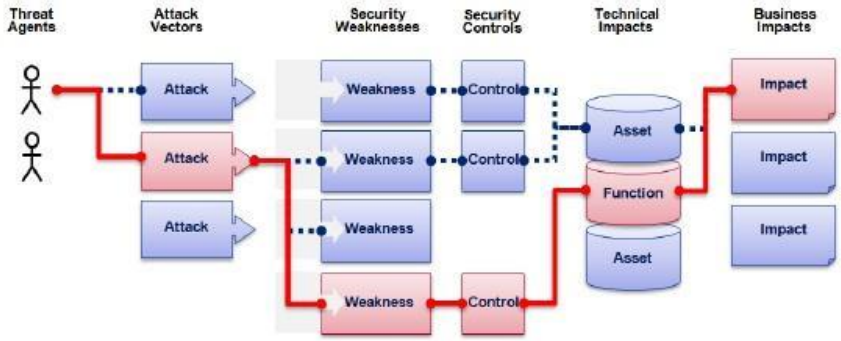
Image Source: OWASP Top Ten 2017 rc1

1. https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

ATTAIN

Anexo #6
Top 10 OWASP

OWASP Top 10 Risk Rating Methodology



Threat Agent	Attack Vector	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact
?	1 Easy	Widespread	Easy	Severe	?
	2 Average	Common	Average	Moderate	
	3 Difficult	Uncommon	Difficult	Minor	
	1	2	2	1	

Injection Example

1.66 * 1

1.66 weighted risk rating

Anexo #7
Detaikls about risk factors

+F Details About Risk Factors

Top 10 Risk Factor Summary

The following table presents a summary of the 2017 Top 10 Application Security Risks, and the risk factors we have assigned to each risk. These factors were determined based on the available statistics and the experience of the OWASP Top 10 team. To understand these risks for a particular application or organization, you must consider your own specific threat agents and business impacts. Even egregious software weaknesses may not present a serious risk if there are no threat agents in a position to perform the necessary attack or the business impact is negligible for the assets involved.

RISK	Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
		Exploitability	Prevalence	Detectability	Impact	
A1-Injection	App Specific	EASY	COMMON	AVERAGE	SEVERE	App Specific
A2-Authentication	App Specific	AVERAGE	COMMON	AVERAGE	SEVERE	App Specific
A3-XSS	App Specific	AVERAGE	VERY WIDESPREAD	AVERAGE	MODERATE	App Specific
A4-Access Ctrl	App Specific	EASY	WIDESPREAD	EASY	MODERATE	App Specific
A5-Misconfig	App Specific	EASY	COMMON	EASY	MODERATE	App Specific
A6-Sens. Data	App Specific	DIFFICULT	UNCOMMON	AVERAGE	SEVERE	App Specific
A7-Attack Prot.	App Specific	EASY	COMMON	AVERAGE	MODERATE	App Specific
A8-CSRF	App Specific	AVERAGE	UNCOMMON	EASY	MODERATE	App Specific
A9-Components	App Specific	AVERAGE	COMMON	AVERAGE	MODERATE	App Specific
A10-API Prot.	App Specific	AVERAGE	COMMON	DIFFICULT	MODERATE	App Specific

Additional Risks to Consider

The Top 10 covers a lot of ground, but there are many other risks you should consider and evaluate in your organization. Some of these have appeared in previous versions of the Top 10, and others have not, including new attack techniques that are being identified all the time. Other important application security risks (in alphabetical order) that you should also consider include:

- Clickjacking (CAPEC-103)
- Denial of Service (CWE-400) (Was 2004 Top 10 – Entry 2004-A9)
- Deserialization of Untrusted Data (CWE-502) For defenses, see: OWASP Deserialization Cheat Sheet
- Expression Language Injection (CWE-917)
- Information Leakage (CWE-209) and Improper Error Handling (CWE-388) (Was part of 2007 Top 10 – Entry 2007-A6)
- Hotlinking Third Party Content (CWE-829)
- Malicious File Execution (CWE-434) (Was 2007 Top 10 – Entry 2007-A3)
- Mass Assignment (CWE-915)
- Server-Side Request Forgery (SSRF) (CWE-918)
- Unvalidated Redirects and Forwards (CWE-601) (Was 2013 Top 10 – Entry 2013-A10)
- User Privacy (CWE-359)

Anexo #8
A7: Insufficient Attack Protection

A7 Insufficient Attack Protection

Application Specific	Exploitability EASY	Prevalence COMMON	Detectability AVERAGE	Impact MODERATE	Application / Business Specific
Consider anyone with network access can send your application a request. Does your application detect and respond to both manual and automated attacks?	Attackers, known users or anonymous, send in attacks. Does the application or API detect the attack? How does it respond? Can it thwart attacks against known vulnerabilities?	Applications and APIs are attacked all the time. Most applications and APIs detect invalid input, but simply reject it, letting the attacker attack again and again. Such attacks indicate a malicious or compromised user probing or exploiting vulnerabilities. Detecting and blocking both manual and automated attacks, is one of the most effective ways to increase security. How quickly can you patch a critical vulnerability you just discovered?		Most successful attacks start with vulnerability probing. Allowing such probes to continue can raise the likelihood of successful exploit to 100%. Not quickly deploying patches aids attackers.	Consider the impact of insufficient attack protection on the business. Successful attacks may not be prevented, go undiscovered for long periods of time, and expand far beyond their initial footprint.

Anexo #9
Entrevista

Entrevista para el levantamiento de información acerca de los aplicativos WEB en la Universidad Central del Ecuador

Fecha: 15-11-2018

Entrevistados: Área de Desarrollo UCE

- María Esther Moyano

Entrevistadores:

- Andrade María José
- Zambrano Grace

Desarrollo:

1. ¿Qué actividades, funciones y/o procesos se realizan en esta área?

En esta área se realiza el desarrollo, mantenimiento y soporte de todas las aplicaciones web que tiene la universidad Central.

2. ¿Qué procedimientos están previamente establecidos para desarrollar dichos aplicativos?.

Claro toda el área de Desarrollo cuenta con procesos establecidos para el desarrollo de los aplicativos. Como por ejemplo, tenemos pre definido como lenguaje de programación JAVA con Netbeans basándonos en metodologías águiles.

3. ¿Cuáles son los aplicativos que mantienen al momento?

- Sistema de Recaudaciones Sysrec.
- Sistema de Talento Humano
- Sistema de Información Integral
- Plataforma Educativa Virtual
- Sistema de Investigación
- Sistema de Talento Humano
- Sistema de Gestión Documental
- Sistema de Registro de Funcionarios

5. ¿Cuáles son los procesos que aplican para volver estas aplicaciones seguras?

- Encriptación de contraseñea

- Validación de las peticiones HTTP
- Cierre de sesión cada cierto tiempo
- Se tiene un token de seguridad para cada enlace.

6. ¿Se puede tener una información más detallada de cada aplicativo?

Claro, con gusto se les enviará los digitales de los procesos y descripción de los aplicativos que consideren en su análisis los más vulnerables.

7. ¿Anteriormente, ya han realizado una auditoria o un análisis de la vulnerabilidad de sus aplicativos?

No, en realidad no hemos tenido una auditoría o un estudio parecido al que ustedes proponen. Esta sería la primera vez. Aunque anualmente tenemos auditorías de la Contraloría del Estado pero de manera más general no a nivel de aplicativo.

8. ¿En alguna ocasión han tenido un ataque en sus aplicativos? En caso de ser afirmativa la respuesta, que tan grave fue el ataque?

Si los hemos tenido, la mayoría de los mismos estudiantes de la Facultad de Sistemas; como queriendo probar los conocimientos adquiridos. Al decir verdad no han sido graves.

Anexo #10
Informe de buenas Prácticas UCE

VULNERABILIDADES INFORMÁTICAS EN LAS APLICACIONES WEB DE LA UNIVERSIDAD CENTRAL DEL ECUADOR

Informe de Resultados

1 de enero de 2019

Autor: María José Andrade Rodríguez Y Grace Marcela Zambrano Vélez

VULNERABILIDADES INFORMÁTICAS EN LAS APLICACIONES WEB DE LA UNIVERSIDAD CENTRAL DEL ECUADOR

Informe de Resultados

1. Problema de Investigación

Con el paso del tiempo el uso del Internet se ha incrementado, generando una demanda de aplicativos Web cada vez mayor. Todo se maneja desde una terminal (laptop, pc, celular) conectada al Internet facilitando el logro de una actividad en específico al usuario. Durante el tiempo de funcionamiento, la Universidad Central llevaba sus procesos y registros de manera manual aumentando tiempo de respuestas y generando malestar en sus usuarios.

Con estos antecedentes, la UCE ha desarrollado varios aplicativos que le permiten generar tareas específicas a sus usuarios finales que van desde personal administrativo hasta los estudiantes; con el fin de optimizar tiempos y recursos. Estas aplicaciones han logrado sistematizar los procesos críticos y con ello obtener mejores resultados, pero al mismo tiempo abrir una brecha a los riesgos y vulnerabilidades externos que puedan presentar. Es por todo esto que resulta relevante realizar el análisis propuesto en el presente trabajo de investigación para identificar dichas brechas en la seguridad de los aplicativos más críticos dentro de su catálogo de plataformas Web de la Universidad.

2. OBJETIVOS

La presente investigación es de gran importancia para el correcto funcionamiento de la Universidad Central del Ecuador, de ahí que se plantearon los siguientes objetivos:

2.1. OBJETIVO GENERAL

Diagnosticar las vulnerabilidades de las aplicaciones web desarrolladas en la Universidad Central del Ecuador.

2.2. OBJETIVOS ESPECÍFICOS

- Determinar las aplicaciones web críticas a través de una matriz de riesgos.
- Analizar cada una de las vulnerabilidades que presenten las aplicaciones seleccionadas.
- Generar recomendaciones de seguridad para las vulnerabilidades identificadas.

3. Fundamentos básicos

3.1. Las Aplicaciones Web

Es un conjunto de herramientas orientadas al usuario con el fin de que este pueda acceder a un servidor mediante el uso de un navegador que se conecta a Internet o bien a una intranet. Las aplicaciones web son muy exitosas debido a su independencia del sistema operativo que tenga instalado el usuario y porque pueden encontrarse de cualquier tipo: web-mails, tiendas on-line, gestión bancaria, blogs, foros. Basan su éxito en el concepto de interactividad que mantienen las aplicaciones web con el usuario. Un ejemplo es el uso de formularios o gestionar bases de datos. Las ventajas que se encuentran a la hora de diseñar aplicaciones Web son varias, entre las principales se pueden considerar las siguientes (Cardador, 2014):

- No es necesario instalar nada de parte del cliente.
- No es necesario que el cliente actualice nada.
- No hay problema de actualización de versiones. Todos usan la misma versión
- Centralización de la información
- No se requiere un sistema operativo determinado, ni software ni hardware determinado.
- Se puede trabajar donde se quiera siempre que se disponga de un equipo y conexión de red.
- Al momento de utilizar aplicaciones Web se pueden presentar algunas desventajas, entre las que se puede mencionar:
- Requieren de una conexión de red.
- Su desarrollo es complejo, dado que hay que garantizar la compatibilidad con los sistemas operativos. Software y hardware de los clientes.

- Su tiempo de respuesta suele ser algo más lento, aunque hoy en día la capacidad de respuesta no tiene nada que envidiar a las aplicaciones de escritorio.

3.2. Seguridad en las aplicaciones web

Todas las organizaciones que exponen sus servicios de información deben tener acceso a las redes para no escatimar esfuerzos para garantizar la protección de la información y los recursos. Internet es un factor de comunicación importante, así como un claro riesgo potencial de acceso y mal uso de los servicios e información disponibles. Por supuesto, los sistemas más importantes están catalogados contra otros cuya seguridad debe ser muy importante, pero en general, todas las aplicaciones web deben estar protegidas y protegidas contra ataques fundamentales (Rodríguez, 2017).

En la aplicación web, la seguridad se comparte en:

- **Accesibilidad:** la propiedad o característica de un activo compuesto por personas autorizadas o procesos con acceso a la solicitud.
- **Autenticación:** la característica es que la entidad es la que llama o proporciona la fuente para la cual se recibieron los datos.
- **Complementariedad:** característica o característica de esta información no aplicada.
- **Confidencialidad:** propiedad o propiedad que no reemplaza ni divulga información a personas, organizaciones o procesos no autorizados.
- **Trazabilidad:** propiedad o característica que las actividades de la organización pueden atribuirse exclusivamente a esta organización.

3.3. Seguridad de la información

La seguridad de la información tiene como prioridad las medidas de prevención y respuesta para las organizaciones y los sistemas tecnológicos que protegen y protegen la información, al tiempo que buscan preservar la confidencialidad, la disponibilidad y la integridad de los datos y los datos (Mateu C. , 2014).

El concepto de seguridad de la información no debe confundirse con la seguridad de la información, ya que solo se refiere a la seguridad en un entorno de información, pero la información se puede encontrar en diferentes entornos o módulos, no solo en los entornos informáticos. La seguridad de la información tiene un impacto significativo en su privacidad y puede determinar los diferentes elementos que dependen de la cultura.

El campo de la seguridad de la información se ha expandido considerablemente desde la Segunda Guerra Mundial y es una carrera reconocida en todo el mundo. Esta área ofrece una amplia gama de áreas de experiencia, incluida la revisión de sistemas de información, la planificación de la continuidad del negocio, la administración forense digital y la seguridad administrativa, entre otras (Cardador, 2014).

3.3.1. Seguridad informática

La seguridad informática es definida como un proceso de prevención y detección de uso no autorizado de un sistema informático, incluye un proceso para eliminar a los intrusos de nuestros recursos informáticos con fines malintencionados o beneficios, o incluso para acceder a ellos accidentalmente para protegerlos (Mateu, 2012).

La seguridad informática es en realidad un término más general, con seguridad de la información, aunque los dos términos se usan a menudo en la práctica, incluye un intervalo de seguridad así como las medidas de seguridad de la computadora tales como programas antivirus, firewalls y otras medidas, que dependen del usuario, como la activación de la desactivación de ciertas funciones del software, como Java Script, ActiveX, el uso adecuado de una computadora, recursos web o en Internet.

Evite el robo de datos, como números de cuentas bancarias, información de tarjetas de crédito, contraseñas, documentos de trabajo, hojas de cálculo, etc., que son necesarios para la comunicación moderna, muchas de las actividades diarias dependen de la seguridad de los datos y como uno de los puntos de partida en la ruta, los datos en la computadora no están autorizados (Mateu C. , 2014).

Una amenaza puede alterar y modificar el código fuente del programa y usted puede usar su propia foto o crear cuentas de correo electrónico maliciosas, como imágenes pornográficas o cuentas sociales incorrectas. Un delincuente cibernético que intenta acceder a computadoras con propósitos

maliciosos, como ataques informáticos, sitios web o cualquier otra red, pero también crea caos (Rodríguez, 2017).

Los hackers pueden bloquear un sistema informático para mitigar la pérdida de datos pueden realizar ataques para garantizar que no se puede acceder a las páginas web cuando el servidor también falla, todos estos factores han subrayado la necesidad de mantener los datos seguros y confidenciales, y la necesidad, por lo tanto, de la protección del equipo, lo que significa que es necesario e importante para todo lo relacionado con la seguridad informática.

3.3.2. Seguridad en las aplicaciones informáticas

En la actualidad, Internet tiene un impacto directo en la seguridad de la información procesada diariamente, los sitios web, servicios, bancos e incluso redes sociales contienen información secreta que es muy importante en la mayoría de los casos (Latorre, 2018). Se puede decir que son uno de los problemas de seguridad de Internet más importantes que afectan directamente a los usuarios, en este caso los servidores web, a menudo se escuchan errores en los sistemas de seguridad de los servidores más utilizados, como Apache, NGINX, IIS, etc., o en los lenguajes de programación en los que se ejecutan las aplicaciones. Sin embargo, ninguna de estas partes constituye la mayoría de los problemas encontrados en los servicios en línea, lo que lleva a prácticas de programación deficientes.

Se debe entender que las aplicaciones de los programas no son fáciles de programar porque los programadores no solo deben lograr el objetivo principal del funcionamiento de la aplicación, sino también una comprensión general de los riesgos de divulgación de la información procesada con el sistema.

3.4. Riesgos y vulnerabilidades

En el área de la informática mencionar la existencia de un riesgo, puede implicar la probabilidad de que una amenaza se produzca, conllevando a un ataque al equipo o a un servidor; no siendo nada más que la posibilidad de que ocurra el ataque por parte de la amenaza. Al realizar un análisis del riesgo existente se puede tomar decisiones para asegurar mejor al sistema (Marini, 2012).

Las vulnerabilidades no son más que puntos débiles en el software que se identifican permitiendo que un atacante pueda llegar a comprometer la integridad, disponibilidad o confidencialidad de un Sistema o Aplicativo. Algunas de las vulnerabilidades más fuertes permiten la ejecución de una serie de códigos por parte del atacante, convirtiéndose en vulnerabilidades de seguridad.

Riesgos de seguridad para aplicaciones

Para las Instituciones que manejan información crítica este es uno de los temas más sensibles de manejar, ya que, nombres, direcciones, números de tarjetas de crédito o cualquier otro tipo de información valiosa podría ser utilizada de forma incorrecta y con esto perjudicar a los usuarios (Mateu, 2012).

Al contar con aplicaciones poco seguras o vulnerables las Instituciones podrían enfrentar muchos problemas, la mayoría de estos se dan por el desconocimiento de las empresas acerca de cuáles son los riesgos y los principales problemas de seguridad que enfrentan sus aplicaciones hoy en día; además de una deficiente validación de la información que se manipula. Los atacantes pueden, potencialmente, utilizar diferentes rutas a través de su aplicación para perjudicar su negocio u organización. Cada uno de estos caminos representa un riesgo que puede o no ser suficientemente grave como para merecer atención (OWASP, 2017). Lo cual se ilustra en la figura.

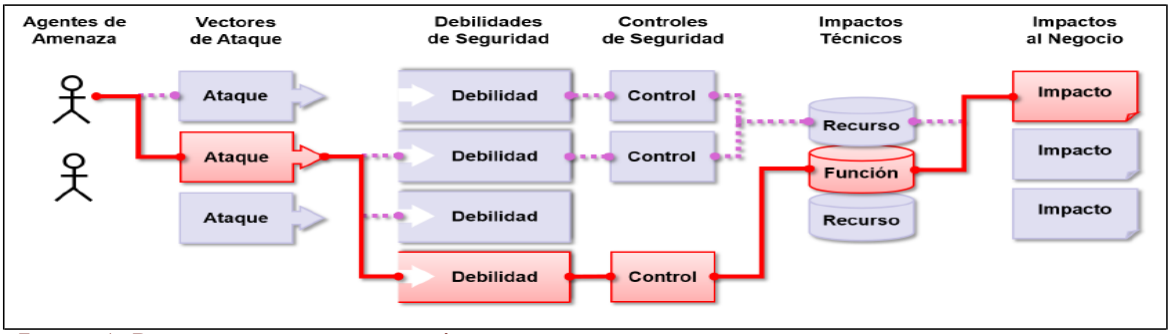


FIGURA 1. **RIESGOS DE SEGURIDAD DE APLICACIONES.**
Fuente: OWASP Top Ten (2017)

3.4.1. Vulnerabilidades en aplicaciones

Las aplicaciones web pueden presentar diversas vulnerabilidades, las cuales ocurren de acuerdo a los servicios que prestan. Según OWASP (Acrónimo de Open Web Application Security Project en inglés,

Proyecto de seguridad de aplicaciones web abiertas"), las vulnerabilidades que prevalecen sobre el tiempo son:

- Inyección
- Pérdida de Autenticación
- Exposición de datos sensibles
- Entidades Externas XML (XXE)
- Pérdida de control de acceso
- Configuración de Seguridad Incorrecta
- Secuencia de Comandos en Sitios Cruzados (XSS)
- Deserialización Insegura
- Componentes con vulnerabilidades conocidas
- Registro y Monitoreo Insuficientes

3.5. OWASP Top 10 – 2017

El Proyecto Abierto de Seguridad en Aplicaciones Web (OWASP por sus siglas en inglés) es una comunidad abierta dedicada a permitir que las organizaciones desarrollen, adquieran y mantengan aplicaciones y APIs en las que se pueda confiar.

Inyección A1:2017

Las falencias realizadas por inyección, como SQL, NoSQL, OS o LDAP se presentan cuando se envían datos no confiables a un intérprete, como parte de un comando o consulta. Los datos dañinos del atacante pueden engañar al intérprete para que ejecute comandos involuntarios o acceda a los datos sin la debida autorización, como se observa en la figura 5.

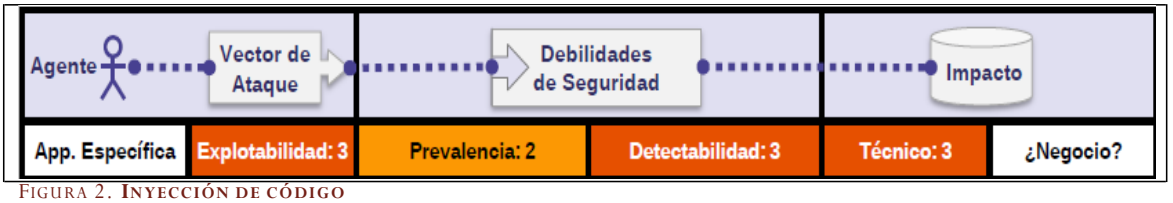


FIGURA 2. INYECCIÓN DE CÓDIGO
Fuente: OWASP Top 10 2017 Los diez riesgos más críticos en Aplicaciones Web

Pérdida de Autenticación A2:2017

Las funciones de la aplicación relacionadas a autenticación y gestión de sesiones son implementadas incorrectamente, permitiendo a los atacantes comprometer usuarios y contraseñas, token de sesiones, o explotar otras fallas de implementación para asumir la identidad de otros usuarios (temporal o permanentemente), lo cual se verifica en la figura 6.

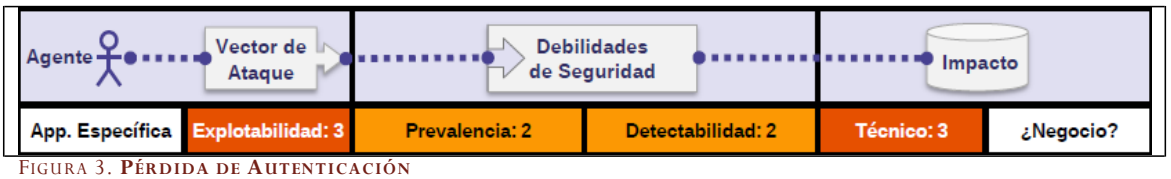


FIGURA 3. PÉRDIDA DE AUTENTICACIÓN
Fuente: OWASP Top 10 2017 Los diez riesgos más críticos en Aplicaciones Web

Exposición de datos sensibles A3:2017

Muchas aplicaciones web y APIs no protegen adecuadamente datos sensibles, tales como información financiera, de salud o Información Personalmente Identificable (PII). Los atacantes pueden robar o modificar estos datos protegidos inadecuadamente para llevar a cabo fraudes con tarjetas de crédito, robos de identidad u otros delitos. Los datos sensibles requieren métodos de protección adicionales, como el cifrado en almacenamiento y tránsito, representado en la figura.

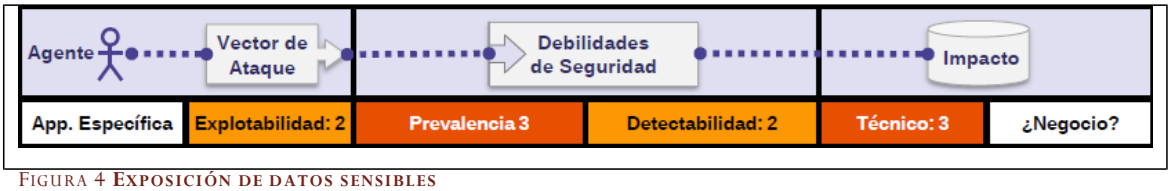


FIGURA 4 EXPOSICIÓN DE DATOS SENSIBLES
Fuente: OWASP Top 10 2017 Los diez riesgos más críticos en Aplicaciones Web

Entidades Externas XML (XXE) A4:2017

Muchos procesadores XML antiguos o mal configurados evalúan referencias a entidades externas en documentos XML. Las entidades externas pueden utilizarse para revelar archivos internos mediante la URI o archivos internos en servidores no actualizados, escanear puertos de la LAN, ejecutar código de forma remota y realizar ataques de denegación de servicio (DoS), evidenciando en la figura 8.

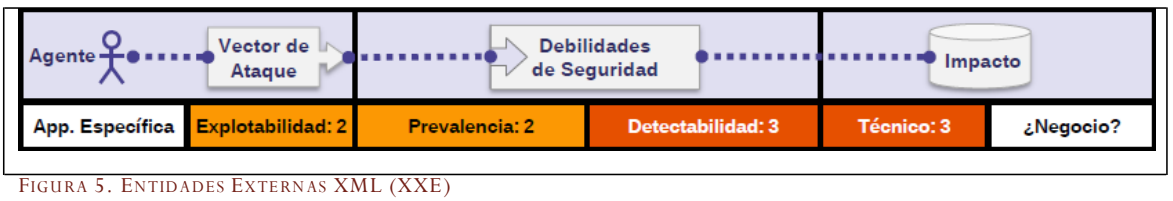


FIGURA 5. ENTIDADES EXTERNAS XML (XXE)
Fuente: OWASP Top 10 2017 Los diez riesgos más críticos en Aplicaciones Web

Pérdida de control de acceso A5:2017

Las restricciones sobre lo que los usuarios autenticados pueden hacer no se aplican correctamente. Los atacantes pueden explotar estos defectos para acceder, de forma no autorizada, a funcionalidades y/o datos, cuentas de otros usuarios, ver archivos sensibles, modificar datos, cambiar derechos de acceso y permisos, etc, expuesto en la figura 9.

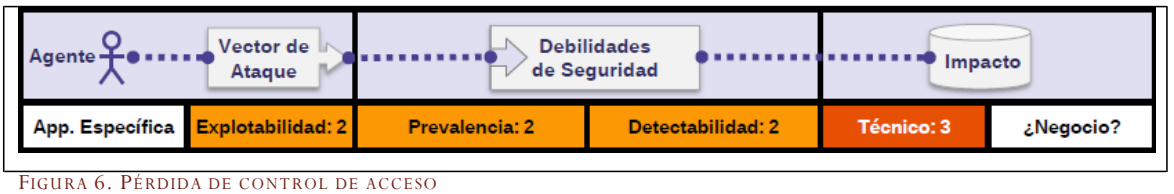


FIGURA 6. PÉRDIDA DE CONTROL DE ACCESO
Fuente: OWASP Top 10 2017 Los diez riesgos más críticos en Aplicaciones Web

Configuración de Seguridad Incorrecta A6:2017

La configuración de seguridad incorrecta es un problema muy común y se debe en parte a establecer la configuración de forma manual, ad hoc o por omisión (o directamente por la falta de configuración). Son ejemplos: S3 buckets abiertos, cabeceras HTTP mal configuradas, mensajes de error con contenido sensible, falta de parches y actualizaciones, frameworks, dependencias y componentes desactualizados, etc, demostrado en la figura.

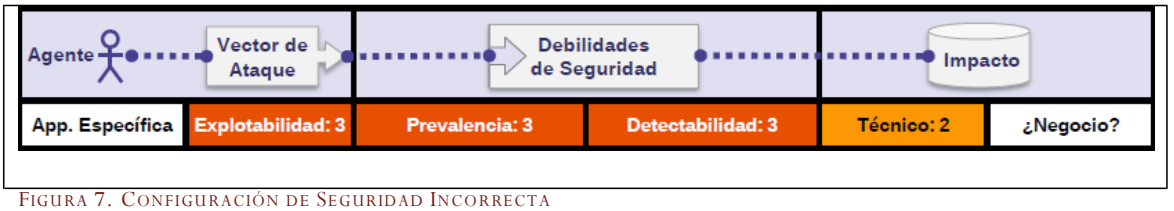


FIGURA 7. CONFIGURACIÓN DE SEGURIDAD INCORRECTA
Fuente: OWASP Top 10 2017 Los diez riesgos más críticos en Aplicaciones Web

Secuencia de Comandos en Sitios Cruzados (XSS) A7:2017

Los XSS ocurren cuando una aplicación toma datos no confiables y los envía al navegador web sin una validación y codificación apropiada; o actualiza una página web existente con datos suministrados por el usuario utilizando una API que ejecuta JavaScript en el navegador. Permiten ejecutar comandos en el navegador de la víctima y el atacante puede secuestrar una sesión, modificar (defacement) los sitios web, o redireccionar al usuario hacia un sitio malicioso, expuesta en la figura 11.

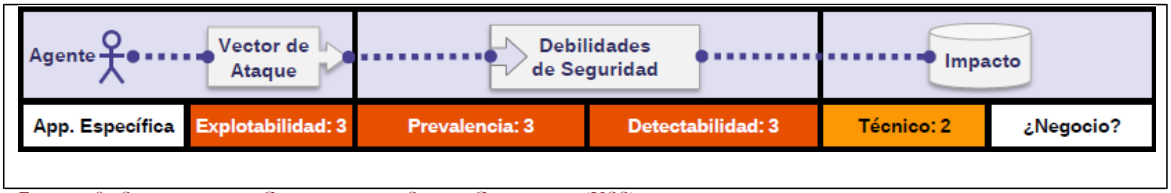


FIGURA 8. SECUENCIA DE COMANDOS EN SITIOS CRUZADOS (XSS)
Fuente: OWASP Top 10 2017 Los diez riesgos más críticos en Aplicaciones Web

Deserialización Insegura A8:2017

Estos defectos ocurren cuando una aplicación recibe objetos serializados dañinos y estos objetos pueden ser manipulados o borrados por el atacante para realizar ataques de repetición, inyecciones o elevar sus privilegios de ejecución. En el peor de los casos, la deserialización insegura puede conducir a la ejecución remota de código en el servidor, señalado en la figura.

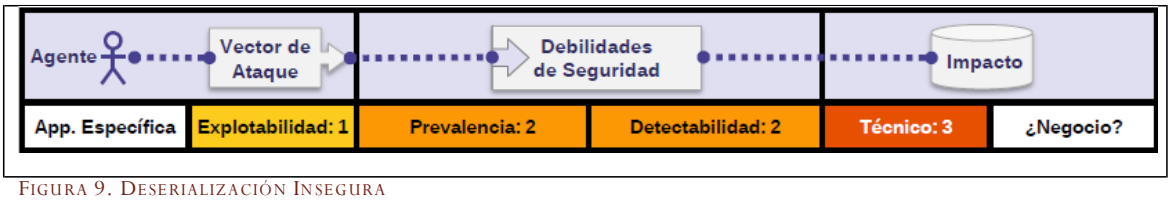


FIGURA 9. DESERIALIZACIÓN INSEGURA
Fuente: OWASP Top 10 2017 Los diez riesgos más críticos en Aplicaciones Web

Componentes con vulnerabilidades conocidas A9:2017

Los componentes como bibliotecas, frameworks y otros módulos se ejecutan con los mismos privilegios que la aplicación. Si se explota un componente vulnerable, el ataque puede provocar una pérdida de datos o tomar el control del servidor. Las aplicaciones y API que utilizan componentes con vulnerabilidades conocidas pueden debilitar las defensas de las aplicaciones y permitir diversos ataques e impactos, explicada en la figura.

FIGURA 10. COMPONENTES CON VULNERABILIDADES CONOCIDAS
Fuente: OWASP Top 10 2017 Los diez riesgos más críticos en Aplicaciones Web

Registro y Monitoreo Insuficientes A10:2017

El registro y monitoreo insuficiente, junto a la falta de respuesta ante incidentes permiten a los atacantes mantener el ataque en el tiempo, pivotear a otros sistemas y manipular, extraer o destruir

datos. Los estudios muestran que el tiempo de detección de una brecha de seguridad es mayor a 200 días, siendo típicamente detectado por terceros en lugar de por procesos internos, indicada en la figura.

FIGURA 11. REGISTRO Y MONITOREO INSUFICIENTES
Fuente: OWASP Top 10 2017 Los diez riesgos más críticos en Aplicaciones Web

3.6. DIAGNÓSTICO DE LA SITUACIÓN ACTUAL

La Universidad Central del Ecuador dedicada al campo de la enseñanza y catalogada como una de las principales y más representativas del Ecuador, con un aproximado de 66000 (http://datosabiertos.uce.edu.ec/Indicadores) estudiantes en total en las diferentes facultades y un total de docentes de 2200 aproximadamente.

Dentro de la oferta académica tienen diferentes carreras como Administración de Empresas, Administración Pública, Arquitectura, Ciencias del Lenguaje y Literatura, Ciencias Policiales y Seguridad Ciudadana, Contabilidad y Auditoría; entre otras. Siendo las ciencias Administrativas y Médicas las de mayor demanda, como muestra la figura 18.

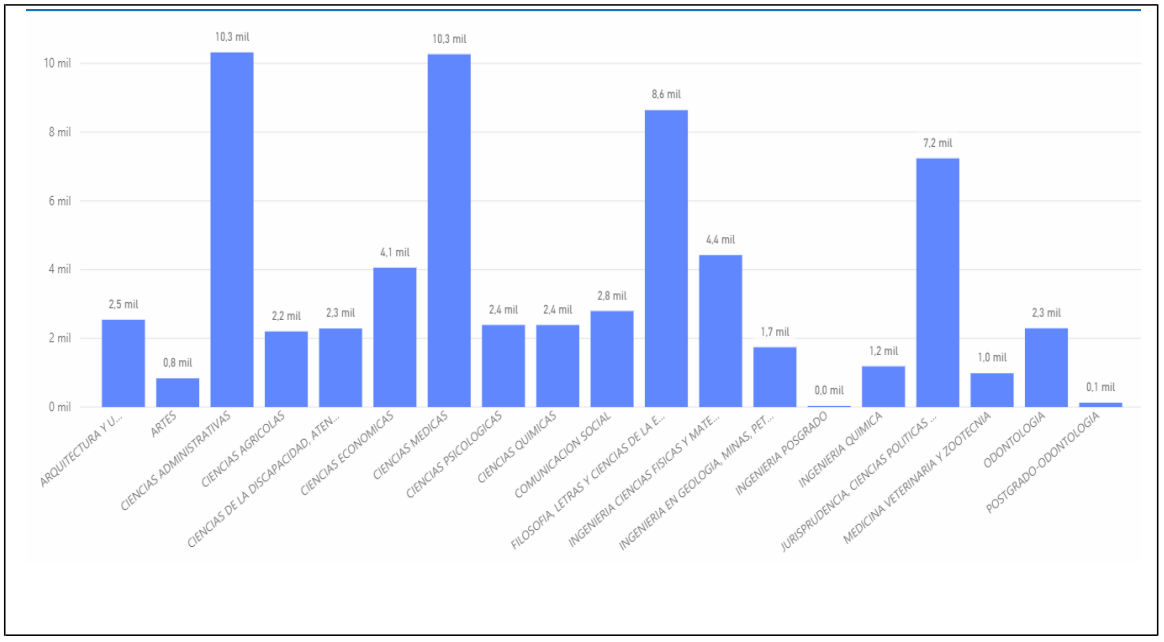


FIGURA 12. TOTAL, ESTUDIANTES POR FACULTAD
Fuente: http://datosabiertos.uce.edu.ec/Indicadores

Su parte organizacional y de administración se da por Rector, Vicerrector Académico y de Investigación y; vicerrector Administrativo y Financiero. (Colocar lo del consejo universitario). Todos los campus se encuentran comunicados y conectados a través de redes tanto LAN como WAN; de la misma manera, la Universidad junto con su equipo tecnológico ha desarrollado cada uno de los aplicativos según se ha ido presentado la necesidad de automatizar o mejorar sus procesos tanto internos como externos.

El Área de Desarrollo tiene definidas buenas prácticas y procedimientos que deben ser aplicados y respetados como parte del proceso de lanzar un nuevo sistema o brindar soporte a cualquiera de ellos. En gran mayoría los sistemas que se manejan son orientados a la Web. Su parte organizacional y de administración se da por Rector, Vicerrector Académico y de Investigación y; vicerrector Administrativo y Financiero. (Colocar lo del consejo universitario)

Se encuentra ubicada en la avenida América, el predio abarca varios edificios donde se ubican las diferentes facultades y personal administrativo. Ciertas facultades se encuentran fuera de este campus como es el caso de las Ciencias Agrícolas que está ubicada al nor-oriente de la ciudad de Quito. Todos los campus se encuentran comunicados y conectados a través de redes tanto LAN como WAN; De la misma manera, la Universidad junto con su equipo tecnológico ha desarrollado cada uno de los aplicativos según se ha ido presentado la necesidad de automatizar o mejorar sus procesos tanto internos como externos. El Área de Desarrollo tiene definidas buenas prácticas y procedimientos que deben ser aplicados y respetados como parte del proceso de lanzar un nuevo sistema o brindar soporte a cualquiera de ellos. En gran mayoría los sistemas que se manejan son orientados a la Web.

3.7. Aplicaciones web de la Universidad Central del Ecuador

Las aplicaciones web que actualmente posee la Universidad Central del Ecuador son:

- **Sistema de Recaudaciones Sysrec:** Utilizado para la recaudación y facturación electrónica fue implementado para dar respuesta al cambio del sistema operativo XP a Windows 10 y como respuesta al incremento de los volúmenes de recaudación.
- **Sistema de Talento Humano - Módulo Nómina**: Este sistema permite desarrollar un control efectivo de los pagos a los diferentes empleados de la universidad.

- **Sistema de Información Integral Módulo Académico**: En este sistema los estudiantes pueden acceder a la información de sus calificaciones, pases de año, entre oros.
- **Plataforma Educativa Virtual**: La plataforma permite entrega de trabajos, así como tener información sobre los temas a ser desarrollados, es de señalar que este espacio garantiza una intercomunicación sistemática entre los estudiantes y docentes
- **Sistema de Investigación**: A través de este sistema se logra un acceso inmediato a la información a ser utilizada por docentes y estudiantes en el desarrollo y elaboración de investigaciones.
- **Sistema de Talento Humano - Módulo Personal**: Este sistema permite un control efectivo sobre el desempeño individual de los trabajadores de la Universidad en el ámbito laboral.
- **Sistema de Gestión Documental**: Garantiza la utilización efectiva de la base de datos de la institución de forma inmediata y con el mínimo de errores al actualizarse la misma de forma sistemática.
- **Sistema de Registro de Funcionarios**: Se revela como una herramienta para impartir disposiciones que redunden en el cumplimiento de los objetivos planteados por la institución a corto, mediano y largo plazo.

Con la finalidad de determinar aquellas aplicaciones críticas en el ámbito académico y financiero de la institución se procedió a crear tablas de valoración de riesgos en la que se plasme la información de forma clara y actualizada, las cuales se detallan a continuación:

MATRIZ DE RIESGOS

DEFINICIÓN DE APLICACIONES CRÍTICAS DESARROLLADAS EN LA UNIVERSIDAD CENTRAL DEL ECUADOR

APLICACIONES AUDITABLES	FACTORES DE RIESGO DE NEGOCIO							
	AUDIT RISK RANKING	Financiero	Estratégico	Operativo	Legal-Cumplimiento	FACTORES DE RIESGO EMPRESARIAL CLASIFICACIÓN	CLASIFICACIÓN DE RIESGOS TOTALES	Porcentaje (%)
	Ponderación de Riesgo	5*	4*	3*	2*			
Sistema de Recaudaciones Sysrec	270	1	1	1	0	12	3240	57.86
Sistema de Información Integral - Módulo Académico	243	1	0	1	1	10	2430	43.39
Sistema de Talento Humano - Módulo Nómina	243	1	0	1	1	10	2430	43.39
Plataforma Educativa Virtual	264	1	0	1	0	8	2112	37.71
Sistema de Investigación	232	0	1	1	1	9	2088	37.29
Sistema de Talento Humano - Módulo Personal	144	1	1	1	1	14	2016	36.00
Sistema de Gestión Documental	225	0	1	1	0	7	1575	28.13
Sistema de Registro de Funcionarios	120	1	0	0	1	7	840	15.00
							TOTAL	16731

Mínimo:	0
Máximo:	5600

PONDERACIÓN DEL RIESGO	
Riesgo Alto:	67 % - 100 %
Riesgo Medio:	34 % - 66 %
Riesgo Bajo:	1 % - 33 %

Una vez auditadas las aplicaciones y viendo sus puntuaciones en riesgo se debe analizar que se analizarán las siguientes aplicaciones:

- Sistema de Recaudaciones Sysrec
- Sistema de Información Integral - Módulo Académico
- Plataforma Educativa Virtual

3.8. Factores de Riesgo para la estimación

En el caso de la aplicación Plataforma Virtual, el algoritmo de transmisión MD5 es uno de los más importantes del momento. El algoritmo se considera débil y le recomendamos que continúe reemplazándolo con un algoritmo de cifrado más seguro. En el caso de que la aplicación SYSREC y Sistema de Información Integral utilice un algoritmo de cifrado, lo que indica una vulnerabilidad significativa, ya que ocurrirá cuando se acceda a los datos en texto sin formato, el atacante tendrá más facilidad para completar la aplicación correcta.

La capa de transporte presenta un riesgo de seguridad inadecuado en aplicaciones como los protocolos criptográficos como SSL (Safe Socket Series) para proteger la autenticación de tráfico, además, esto no se aplica a la criptografía de canales, servicios y recursos de datos. La aplicación de este protocolo contribuye a la protección, confidencialidad y verificación de la autenticidad de la información transmitida (Areito, 2016)

Aunque las aplicaciones de análisis pueden perder la Autenticación y Gestión de Sesiones, es recomendable reducir el plazo para cerrar las sesiones. En este momento, este tiempo se establece en el CAS (Servicio de Autenticación Central) y la sesión cerrada es de 30 minutos después de la autenticación del usuario, lo cual es mucho tiempo, por lo tanto, se recomienda reducir este período a 15 minutos para que no exista la oportunidad de atacar a la aplicación.

La metodología de evaluación de riesgos se utiliza para estimar la gravedad del riesgo del Top 10 de OWASP, en este caso, la metodología se utiliza para evaluar los dos riesgos identificados en aplicaciones analíticas. Para implementar la metodología, se publica un manual en el sitio web oficial de OWASP, en particular un artículo sobre la metodología de evaluación de riesgos (Zalewski, 2012).

Después de definir del riesgo potencial, se debe tener en cuenta la probabilidad de ocurrencia. Esta es una medida aproximada de la probabilidad de que un atacante descubra una vulnerabilidad y la aproveche. En esta evaluación, no es necesario ser preciso, es suficiente para determinar si la probabilidad de ocurrencia es baja, media o alta.

Esta evaluación debe tener en cuenta una serie de factores: el primer grupo se refiere a los factores que causan una amenaza, el objetivo es ver la probabilidad de que un grupo de ataques potenciales se lance hacia un ataque exitoso. Hay una serie de opciones relacionadas con el factor y cada opción tiene un número entre 0 y 9, lo que sugiere la probabilidad de origen. Estos valores se utilizan para determinar la probabilidad de reconocimiento global de los riesgos identificados, existe la posibilidad de tener un fenómeno:

- De 0 a < 3 la probabilidad se califica como bajo.
- De 3 a < 6 la probabilidad se califica como medio.
- De 6 a 9 la probabilidad se califica como alto.

3.8.1. Factores relacionados con el agente causante de la amenaza

El primer conjunto de factores está conectado a un intermitente que crea una amenaza, por lo tanto, el objetivo es demostrar la probabilidad de que un grupo de ataque con éxito. Cualquier persona que pueda enviar datos no confiables al sistema, incluidos usuarios externos, usuarios internos, administradores y empleados con acceso privilegiado, puede convertirse en un agente de amenazas. Incluso los usuarios del sistema que pueden intentar robar otras cuentas de usuario pueden considerarse usuarios malintencionados (Mateu C. , 2012).

Además, observe a los empleados que desean ocultar sus acciones, así como a los usuarios con contraseñas creíbles que puede utilizar para pasar por el sistema, puede ser cualquier persona que pueda alertarte cuando solicitas el ingreso al sitio. Otros usuarios de ciertos sitios web pueden acceder a otros peligros de cualquier página web u otro canal HTML, también puede encontrar la probabilidad de que pueda capturar el tráfico de la red a sus usuarios, aquí hay algunos factores asociados con la causa que causa la amenaza.

Nivel de conocimiento: refleja el conocimiento técnico del grupo de participantes.

- Sin conocimientos
- Algunos conocimientos técnicos
- Usuario avanzado de ordenador
- Conocimientos de redes y programación
- Conocimientos de intrusiones de seguridad

Motivación: para alentar a este grupo de invasores a detectar y utilizar esta vulnerabilidad.

- Baja motivación o ninguna recompensa
- Posible recompensa
- Recompensa alta

Oportunidades: este grupo tiene la oportunidad de que los invasores identifiquen y utilicen esta vulnerabilidad.

- Ningún acceso conocido
- Acceso limitado
- Acceso total

Tamaño: Número del grupo de atacantes.

- Desarrolladores
- Administradores de sistemas
- Usuarios de la intranet
- Socios
- Usuarios autenticados
- Usuarios anónimos de Internet

3.8.2. Factores para estimar el impacto

Es importante saber que hay dos tipos de efectos: el primero es el impacto técnico de la aplicación, los datos utilizados y la funcionalidad proporcionada. El segundo es el impacto comercial, la empresa que administra la aplicación, después de todo, el impacto en el negocio es mayor. Sin embargo, puede que no sea posible acceder a toda la información necesaria para identificar las consecuencias de

realizar correctamente la vulnerabilidad, en este caso, todo debe informarse en detalle sobre los riesgos técnicos que le permiten a la empresa determinar el riesgo (Beust, 2015).

El impacto técnico se puede dividir en factores correspondientes a los dominios de seguridad tradicionales: confidencialidad, integridad, disponibilidad y control de responsabilidad, el objetivo es evaluar el alcance del impacto en el sistema en el que es vulnerable. Algunos factores pueden incluir la pérdida o corrupción de datos, falta de integridad o acceso denegado, permitiendo que los scripts ejecuten ataques de scripts en el navegador de la víctima para capturar sesiones de usuario, eliminar sitios web, códigos maliciosos, usuarios directos, etc.

Instalar código malicioso en el navegador de la víctima, los usuarios malintencionados pueden obtener acceso no autorizado a datos o funciones de la aplicación, cada uno de estos factores representa un riesgo para todo el sistema si la cuenta de un tutor está en riesgo. Esto puede revelar información de uso y puede contener muchas cuentas, aquí hay algunos factores técnicos (López & Echeverry, 2014).

Pérdida de confidencialidad: divulgación de la cantidad y sensibilidad de la información y su confidencialidad.

- Revelación mínima de datos no sensibles
- Revelación mínima de datos críticos
- Amplia revelación de datos no sensibles
- Amplia revelación de datos críticos.
- Todos los datos revelados

Pérdida de integridad: Cantidad de datos se podrían corromper y el daño que sufre.

- Mínimo, datos ligeramente corruptos
- Mínimos datos seriamente dañados
- Gran cantidad de datos ligeramente dañados
- Todos los datos totalmente corruptos

Pérdida de disponibilidad: Servicios que se pueden ver interrumpidos y su vitalidad.

- Mínimo número de servicios secundarios interrumpidos
- Mínimo número de servicios primarios interrumpidos
- Gran número de servicios secundarios interrumpidos
- Gran número de servicios primarios interrumpidos
- Todos los servicios perdidos

3.8.3. Factores de impacto sobre el negocio

El impacto en la sociedad se deriva del impacto técnico, pero del profundo conocimiento de lo que es importante para la empresa que utiliza la aplicación, como regla general, los riesgos deben tenerse en cuenta, teniendo en cuenta el impacto en la empresa, especialmente si el público está compuesto por gerentes, el riesgo comercial se justifica por la inversión en la solución de problemas de seguridad (Quero, García, & Peña, 2017). Muchas empresas tienen pautas sobre clasificación de activos y/o una declaración de impacto en el negocio que definen lo que es importante para su negocio, estas normas pueden ayudarlo a enfocarse en problemas de seguridad críticos. Si no están disponibles, solicite a las personas que entienden el sector que obtengan su opinión sobre puntos importantes.

La aplicación puede estar en peligro sin saberlo, la información podría ser robada o modificada y los costos del tratamiento podrían ser altos. Información, datos o características presentadas en los canales de comunicación con respecto a sus requisitos de confidencialidad e integridad. Es muy importante tener en cuenta su impacto en la reputación de la empresa y la vulnerabilidad de su comunidad (Areito, 2016). Los factores que se describen a continuación son comunes a muchas empresas, debido a factores asociados con amenazas, vulnerabilidades e impactos técnicos.

Daño Financiero: Daño financiero resultado de la explotación de una vulnerabilidad.

- Menor al coste de arreglar la vulnerabilidad
- Leve efecto en el beneficio anual
- Efecto significativo en el beneficio anual
- Bancarrota

Daño sobre la reputación: La explotación de una vulnerabilidad tendría por resultado un daño sobre la reputación.

- Daño mínimo
- Pérdida de las cuentas principales
- Pérdida del buen nombre
- Daño sobre la marca

No conformidad: Exposición introduce la no conformidad.

- Violación leve
- Clara violación
- Violación prominente

Violación de la privacidad: Cantidad de información que facilite la identificación personal podría ser revelada.

- Un individuo
- Cientos de personas
- Miles de personas
- Millones de personas

4. Uso de la herramienta OWASP

Es una herramienta poderosa para ataques intensos, llamada pentesting, utilizada para controlar aplicaciones vulnerables. Cabe señalar que esta plataforma gratuita o multijugador es una herramienta que le permite utilizarla en diferentes sistemas operativos, como ya hemos mencionado. Esta prueba ejecuta Windows 8.1. Al instalar las herramientas ZAP de OWASP, primero debe tener la configuración deseada para las vulnerabilidades que afectan a las aplicaciones de prueba de ataque (OWASP, 2017).

Debe ejecutar e ingresar la URL de la página o el servidor de la misma manera que la víctima, luego un programa de análisis para identificar las vulnerabilidades. Tenga en cuenta que esta herramienta muestra cuatro tipos de alertas, como se muestra a continuación:

1. Advertencias de alta prioridad.

2. Aviso de prioridad.
3. Alertas de baja prioridad.
4. Notas informativas

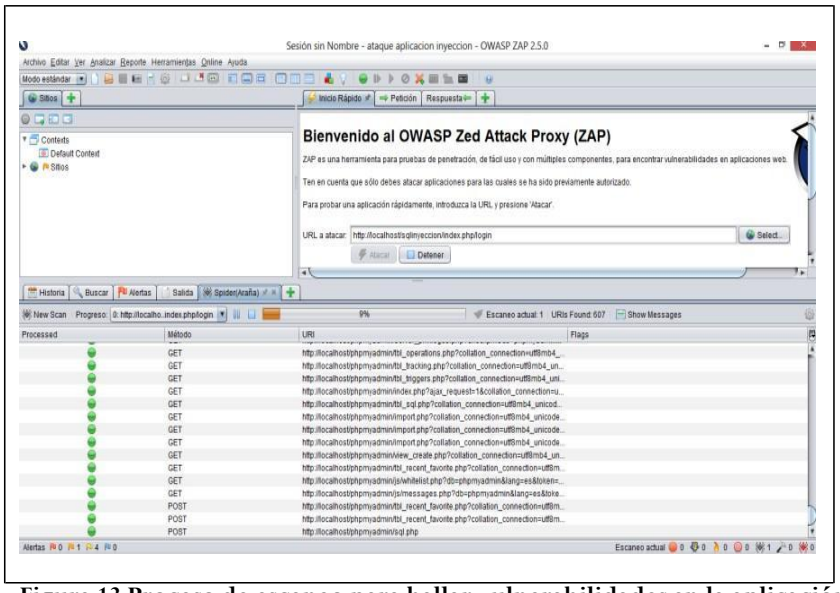


Figura 13 Proceso de escaneo para hallar vulnerabilidades en la aplicación

La figura muestra que las aplicaciones analizan las solicitudes IAR que se envían a través del navegador para corregir errores o usan aplicaciones de seguridad directamente a la aplicación web diseñada bajo framework CodeIgniter.

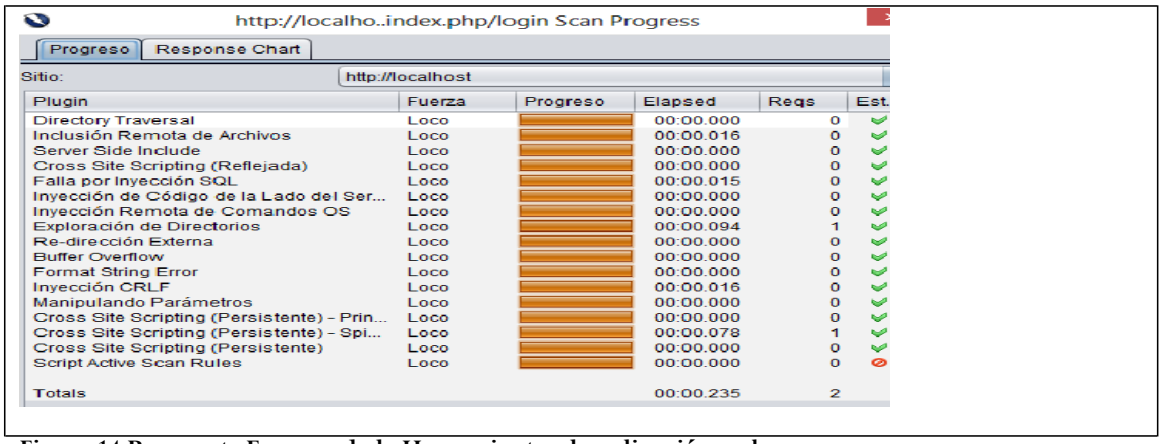


Figura 14 Respuesta Escaneo de la Herramienta a la aplicación web

Después de revisar una aplicación y cumplir con los requisitos de revisión ZAP de OWASP, se especifica un calendario en toda la aplicación, detecta errores y luego se inspecciona al 100%, puede encontrar el rango de respuestas a los tipos de amenazas y vulnerabilidades.

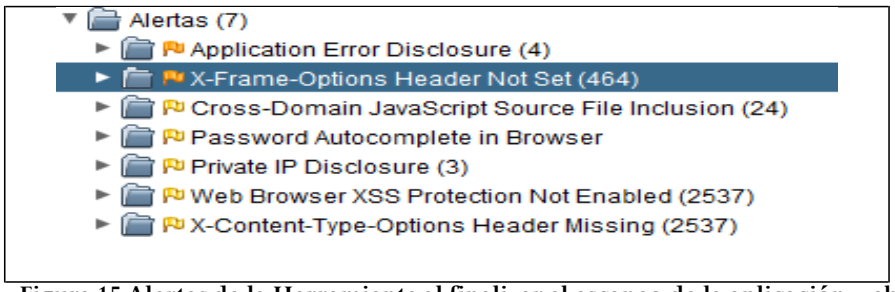


Figura 15 Alertas de la Herramienta al finalizar el escaneo de la aplicación web

En detalle, en el proceso de escaneo, puede verse que la aplicación incluye medidas de precaución integrales para el uso de la infraestructura y que los resultados de los ataques no utilizaron la inyección SQL, como se indica en el informe. , es posible que se usen otros tipos de ataques, pero no se enumeran específicamente para esta prueba. Las instrucciones para lanzar un ataque de inyección SQL no se encuentran en una aplicación que se va a probar. El programador puede así detectar la otra amenaza para evitar las vulnerabilidades de seguridad de los ataques, el análisis muestra los siguientes tipos de alertas:

- 2 alertas con prioridad media.
- 5 siguientes son de alerta con baja prioridad

4.1. Determinación de la gravedad del riesgo

Para determinar la probabilidad esperada y el impacto esperado, es necesario calcular un nivel general de riesgo. En este caso, determina la probabilidad de baja, media o alta, lo que debe hacerse con la divulgación (Paredes, 2014). Las estimaciones deben protegerse o reproducirse de modo que se pueda considerar un procedimiento más formal para evaluar los factores y calcular el resultado. Cabe señalar que estas estimaciones están sujetas a muchas incertidumbres y que estos factores están destinados a lograr un resultado razonable. Inicialmente, se selecciona uno de los parámetros de cada factor y el número correspondiente se ingresa en la tabla, luego, toma el punto central y calcula la probabilidad de que esto suceda en el mundo.

A continuación se presenta una prueba con valores para verificar los datos de un agente que libera los factores de amenaza y vulnerabilidad, el riesgo de almacenamiento criptográfico se indica en la aplicación SYSREC. Cada dimensión se aplica al número, lo que significa que es probable que los niveles aumenten y queden expuestos, luego agrega un grupo para compartir la probabilidad de un fenómeno global.

TABLA 1 PROBABILIDAD DE OCURRENCIA

Factores correspondientes al agente causante de amenaza	Nivel de habilidad	6
	Motivo	9
	Oportunidad	7
	Tamaño	5
	Factibilidad descubrimiento	9
Factores asociados a la vulnerabilidad	Factibilidad explotación	5
	Concienciación	9
	Detección de intrusión	8
Probabilidad de Ocurrencia Global= 7.125 (ALTA)		

En este caso, el producto es 7.125, esta es una alta probabilidad. Además, es necesario descubrir los efectos técnicos generales y el impacto total en la empresa, ambos similares a los anteriores, en estos casos, es fácil determinar la respuesta cuando se alcanzan los valores más altos, medios o bajos, aunque la respuesta es clara, es aconsejable basar una evaluación factorial.

Inicialmente, el valor promedio de cada factor se calcula porque en el caso anterior, es menos de 3 menos, el promedio de 3 a 6 es promedio y alto de 6 a 9, para cada resultado de factor, una prueba con los valores Los números correspondientes están en la siguiente tabla, en este caso, los números se ingresan y se dividen en una serie de características evaluadas en cada uno. La tabla proporciona datos sobre el riesgo de almacenamiento criptográfico inestable en la aplicación SYSREC, en este caso, el efecto técnico general se estima en 7.25, por lo que se piensa que estos resultados son altos y que la empresa tiene que decidir sobre su estrategia que protegerá sus intereses.

TABLA 2 IMPACTO DE ATAQUE

Impacto Técnico	Perdida de confidencialidad	9
	Perdida de Integridad	7
	Perdida de disponibilidad	5
	Pérdida de control responsabilidad	8
Impacto Técnico Global = 7.25 (ALTO)		
Impacto sobre Negocio	Daño Financiero	9
	Daño a la Reputación	9
	No conformidad	5
	Violación de Privacidad	6
Impacto Global sobre el Negocio = 2.25 (BAJO)		

A continuación se muestra una prueba con valores para la verificación de datos en relación con un agente que emite la amenaza y los factores de vulnerabilidad. La siguiente tabla presenta datos sobre el riesgo de protección insuficiente del transporte en la Plataforma Educativa Virtual, el procedimiento es idéntico al del ejemplo anterior, el resultado es 6,375, lo que significa que la probabilidad de este riesgo es de uso promedio.

TABLA 3 PROBABILIDAD DE OCURRENCIA

Factores correspondientes al agente causante de la amenaza	Nivel de Conocimiento	4
	Motivación	7
	Oportunidad	8
	Tamaño	6
Factores asociados a la Vulnerabilidad	Facilidad de descubrimiento	7
	Facilidad de explotación	4
	Conocimiento	7
	Detección de Intrusión	8
Probabilidad de ocurrencia global=6.375 (MEDIA)		

De igual manera presenta los detalles del riesgo de que el nivel de tráfico no sea suficiente en la Plataforma Educativa Virtual, en este caso, la consecuencia técnica global estimada es de 6.75 y el impacto total en la compañía es de 5.75, que es el promedio. Con estos resultados, una empresa debe determinar qué estrategia debe considerarse en función de sus intereses.

TABLA 4 IMPACTO DEL ATAQUE

Impacto Técnico	Perdida de confidencialidad	8
	Perdida de Integridad	7
	Perdida de disponibilidad	4
	Pérdida de control responsabilidad	8
Impacto Técnico Global = 6.75 (MEDIO)		
Impacto sobre Negocio	Daño Financiero	7
	Daño a la Reputación	7
	No conformidad	5
	Violación de Privacidad	4
Impacto Global sobre el Negocio = 5.75 (MEDIO)		

Después del análisis de las tablas anteriores, está claro que existe el riesgo de un almacenamiento criptográfico peligroso o presenta riesgos de protección insuficiente de la información, además, el impacto técnico general y el impacto general en el negocio son mejores.

4.2. Identificación de riesgos en base al Top 10 de OWASP

Sobre la base de la comparación y el análisis, se han identificado los siguientes riesgos:

R7: ruta criptográfica incierta, generando robo de información confidencial, pudiendo existir robo de identidad y falsificación de documentos.

R9: Protección insuficiente del tráfico, generándose el cierre de las aplicaciones de tal manera que los estudiantes no pueden cargar sus trabajos y de esta manera reprobar materias.

5. Propuesta de Buenas Prácticas

Las buenas prácticas se refieren a los sistemas de calidad que determinan las condiciones bajo las cuales los datos recibidos se planifican, procesan, monitorean, registran y archivan para garantizar su confiabilidad, protección de prevalencia, impacto positivo, difusión de experiencias e información obtenida para que puedan comunicarse y realizarse en otros contextos (Mateu C. , 2014).

Criterios de selección

Las buenas prácticas, que se describen en detalle a continuación, tienen al menos los criterios requeridos:

- **Documentada:** sirve de referencia para otros y les ayuda a mejorar sus procesos. Esta es una comprensión importante de las mejores prácticas. Debe documentarse para que la información pueda transferirse fácilmente a otra organización para saber cómo proceder.
- **Accesible:** para usar en cualquier lugar y con cualquier persona.
- **Basado en procesos y metodologías:** en la práctica, existen metodologías cuidadosamente seleccionadas para cambiar el centro de prioridad.
- **Prueba e implementación:** Las mejores prácticas del proceso son las mejores, la evaluación o el proceso de evaluación.
- **Establecer la capacidad para establecer metas:** la mejor práctica para satisfacer una necesidad definida, después de una evaluación cuidadosa de las características específicas de un grupo de población específico que necesita ser modificado y mejorado, y que por lo tanto tiene un propósito Específico, relevante y realista.
- **Transferible:** como objetivo, la transferencia de información debe facilitarse en los métodos, herramientas y enfoques utilizados para brindar experiencia o iniciativas que tengan en cuenta las mejores prácticas.
- **Sostenibilidad:** los ingresos superan los costes. La relación costo / ingreso es mejor que una práctica similar.
- **Eficiente:** la relación entre el costo del ingreso es mejor que la de métodos similares.

- **Eficaz:** resultados esperados.

Estas características son los criterios clave para elegir las mejores prácticas.

5.1. Buenas prácticas de seguridad para el desarrollo web

Este es un conjunto de elementos o acciones implementadas para garantizar la seguridad de las aplicaciones web desde el desarrollo inicial y el mantenimiento, para implementar métodos avanzados de seguridad de red, debe considerar lo siguiente. Un paso importante que debe estar preparado para registrar excepciones y proporcionar una respuesta de control es que los usuarios finales usen los datos correctamente, para hacer esto, debe realizar verificaciones del lado del cliente utilizando JavaScript como del lado del servidor por medio de rutinas del lenguaje de programación (Paredes, 2014).

Son muy importantes porque las comprobaciones o desactivaciones del lado del cliente pueden ignorarse, esto se hace filtrando los datos proporcionados por el usuario del lado del servidor. Se recomienda que utilice listas blancas que se pueden generar usando expresiones regulares que impiden la asignación directa de valores obtenidos de la entrada en la variable para garantizar que los datos se verifiquen correctamente, los controles deben hacerse correctamente porque puede ingresar líneas de código malicioso para obtener información sobre la aplicación o sus usuarios, lo que puede representar un riesgo para las inyecciones de SQL, XSS y CSRF.

No se debe olvidar configurar sesiones que le permitan hacer un seguimiento de los usuarios, mantener valores variables en el sitio sin tener que usar campos ocultos en los módulos y limitar el acceso a ciertos elementos, es muy importante monitorear la sesión, iniciarla correctamente y cerrarla para evitar una violación de seguridad.

Como recomendación, debe especificar: usar sesiones cuando un usuario inicia limitado a la aplicación; la sesión siempre está activa en cualquier objeto visitante para mostrarla; de lo contrario, el usuario debe redirigir para iniciar la sesión; y cierre la sesión correctamente cuando un usuario visite el sitio. Los riesgos de uso indebido incluyen: acceso a recursos limitados, el robo de datos personales de otros usuarios y el uso inadecuado de los recursos de la aplicación (Zalewski, 2012).

La administración de datos del usuario final debe realizarse con protección adicional, lo primero que se debe evaluar es el cifrado de un canal de comunicación para el intercambio cliente-servidor. Es muy importante mantener la información proporcionada por los usuarios en un lugar seguro, al comienzo de la sesión (nombre de usuario, contraseña) y al momento de la inscripción, en los formularios (nombre, apellido, dirección, correo electrónico, teléfono). Se recomienda que instale HTTPS utilizando la certificación del servidor de aplicaciones web y configure el servidor para usarlo en la configuración principal o en cada host virtual como un riesgo, el tráfico web puede estar mediado y refleja información confidencial sobre la ruta (una en el medio).

En Internet, cuando recibe un desarrollo específico, puede personalizar los mensajes de error que los usuarios pueden necesitar para evitar información sobre su sitio, por lo tanto, es necesario incluir posibles errores en la aplicación y la información mostrada a los usuarios, ya que el nombre indica el mal funcionamiento de la seguridad, por lo que se recomienda utilizar mensajes de error comunes según sea necesario. La exposición involuntaria a la instalación e información de configuración del sitio (versiones, software utilizado, canales del sistema) puede resultar en un riesgo de mala administración.

La información es el recurso más importante procesado por las aplicaciones web, por lo que es el más vulnerable a la seguridad informática, por lo tanto, debe ser protegido de una manera segura. Para este fin, es recomendable tomar las medidas necesarias, tales como: reducir el acceso no deseado a la información procesada en la aplicación, crear una base de datos de servicios (Beust, 2015).

Los datos simplifican la configuración y evitan que los usuarios, las contraseñas y la configuración predeterminada como riesgo de uso indebido, es posible obtener información de la base de datos (servicios y contenidos). A veces, la aplicación debe usar características o contenido de terceros (formulario de validación, calendarios, autenticación usando oauth con Twitter o Facebook) para investigar las vulnerabilidades actuales, es muy importante utilizar el rendimiento mínimo apropiado y sin instalar ningún hardware o características que no se utilizarán.

Si está instalando bibliotecas, módulos o complementos de terceros, debe instalar la última versión estable e instalar las actualizaciones de seguridad adecuadas. Los riesgos dependen del tipo de vulnerabilidad del sujeto, pero XSS, CSRF, inyección SQL, sesiones de vuelo, escalamiento de privilegios, etc.

5.2. Estrategia

La política de seguridad permite a los administradores de seguridad proteger la disponibilidad, integridad y confidencialidad de los datos en los sistemas de información empresarial. La estrategia debe aplicarse sistemáticamente en la práctica, como medida de precaución, e incluir planes de contingencia para hacer frente a circunstancias imprevistas.

Los gerentes deben definir el tiempo, el capital y el esfuerzo necesarios para invertir en el desarrollo de medidas y controles de seguridad adecuados. Todas las organizaciones deben analizar sus necesidades específicas y determinar los recursos y necesidades de sus programas. Cada sistema informático, entorno y estrategia organizacional son diferentes, lo que hace que cada servicio y estrategia de seguridad sean específicos. Aquí hay algunos principios a tener en cuenta al configurar una buena estrategia de seguridad:

a. Actualización continúa de herramientas y métodos de seguridad informática.

Organizaciones que ayudan a los administradores de seguridad a identificar los métodos, herramientas y métodos de ataque más probables. Este dominio de conocimiento siempre debe actualizarse para evitar ignorancia, vulnerabilidades y vulnerabilidades de seguridad.

b. Definición de estrategias proactivas e inesperadas.

Los planes de seguridad de cada organización deben incluir estrategias de prevención de ataques con una serie de pasos que reducen la vulnerabilidad de las políticas de seguridad. La evaluación continua de las debilidades ayuda a desarrollar una estrategia preventiva. Una estrategia no planificada es una estrategia que sigue a un ataque cuando el daño causado por el ataque es evaluado, corregido, documentado y resumido por la experiencia.

c. Grabar ataques en entornos de prueba.

La implementación de ataques de simulación en entornos de prueba o laboratorios proporciona una evaluación de las vulnerabilidades y los ajustes adecuados a las instrucciones y medidas de seguridad.

Estas pruebas no deben realizarse en sistemas reales porque el resultado podría ser desastroso, pero es muy importante usarlos debido a los riesgos y consecuencias de los ataques.

d. Inspección de incidencias

Se recomienda crear un equipo de gestión de eventos. Este grupo debe estar involucrado en el trabajo de seguridad preventiva. Deben definir instrucciones, herramientas, encuestas y aplicar tareas de control de incidentes a los ataques del sistema.

5.3. Generación de buenas prácticas en el desarrollo de software

Después del análisis de las aplicaciones académicas y financieras tienen los siguientes riesgos relacionados con las características que representan y el propósito social. Todo lo que se pretende y con las características técnicas de cada uno de ellos:

- Riesgo 7: Ruta criptográfica incierta.
- Riesgo 9: Protección insuficiente en términos de tráfico.

Sobre la base de los riesgos anteriores, se describen las siguientes prácticas recomendadas, que deben tenerse en cuenta en el desarrollo y el servicio de la Universidad Central del Ecuador para utilizar aplicaciones que garanticen la navegación, privacidad e integridad de los datos y la información mostrada.

Respecto al riesgo 7: almacenamiento criptográfico no confiable Algunas aplicaciones web no ofrecen una protección adecuada de datos confidenciales, así como la autenticación a través de un mecanismo de cifrado o sputtering. La información o datos pueden ser protegidos para evitar el robo de identidad o falsificar datos académicos.

Mejores prácticas de riesgo 1. Un almacén criptográfico no confiable debe identificar mucha privacidad y requiere cifrado. Por ejemplo, la contraseña, los datos personales de las personas que se monitorean deben incluirse en:

Evaluar todos los riesgos que pueden afectar los datos, teniendo en cuenta los ataques internos y los usuarios externos. Proporcionar información confidencial de encriptación donde sea que esté almacenada por mucho tiempo.

- Compruebe el cifrado de las copias de seguridad almacenadas en el exterior.
- Asegúrese de que las contraseñas se administran y almacenan por separado.
- Los usuarios no autorizados permiten el acceso solo a los usuarios autorizados.
- Utilice un algoritmo estándar seguro.
- Las teclas fuertes están protegidas contra accesos no autorizados.
- Asegúrese de que los algoritmos potentes, como la transmisión, admitan claves.
- Desarrollar un plan de cambio de contraseña.

Con respecto al riesgo 7: protección insuficiente a nivel de transporte, las aplicaciones, el secreto y la integridad del tráfico a menudo no validan, cifran y protegen una red segura. Cuando esto sucede, esto se debe al uso de algoritmos débiles, la verificación expira, no es válida o simplemente es engañosa.

Mejores prácticas relacionadas con el riesgo 9: El nivel de transporte no debe tener suficiente protección para demasiada protección del transporte, lo que puede afectar el formulario de solicitud. Por lo tanto, es fácil solicitar SSL para toda la aplicación, por alguna razón, algunas aplicaciones SSL solo se utilizan para acceder a páginas privadas. Otros SSL utilizan solo páginas "críticas", pero pueden revelar identificadores de sesión y otra información confidencial. Se aplica lo siguiente:

Use SSL en las páginas más importantes y redirija las aplicaciones que no son SSL a la página donde existe.

- Configure la función segura en cada cookie de mayor riesgo.
- Configurar el servidor SSL para encontrar un potente algoritmo.
- Asegúrese de que el certificado sea válido, no haya caducado o no haya sido revocado y sea apropiado para todas las áreas utilizadas por la aplicación.
- Se deben usar sistemas anteriores y otros sistemas SSL u otras tecnologías de encriptación.

6. CONCLUSIONES

- Del análisis de vulnerabilidades de las aplicaciones web desarrolladas por la Universidad Central del Ecuador se determinó que existe una ruta criptográfica incierta e insuficiente protección del tráfico de información.

- Mediante la matriz comparativa se pudo establecer que las aplicaciones críticas son: el Sistema de Recaudaciones Sysrec, el Sistema de Información Integral - Módulo Académico y la Plataforma Educativa Virtual.
- Se procedió a evaluar los riesgos, vulnerabilidades, amenazas e impactos, respaldándose en el Top Ten de OWASP, determinando la existencia de una vulnerabilidad media alta la cual puede inclinarse a ser mayor.
- Los riesgos evidentes son almacenamiento criptográfico inseguro, así como protección insuficiente en la capa de transporte.
- Del mismo modo se materializó una lista de buenas prácticas (anexo #10), con la finalidad de garantizar el funcionamiento de las aplicaciones lográndose de esta forma dar una corrección efectiva a los riesgos detectados o aquellos que puedan surgir durante su funcionamiento, tomando en cuenta los hallazgos de la investigación.

7. RECOMENDACIONES

- Eliminar el riesgo de almacenamiento criptográfico inseguro dado su elevado impacto negativo para la utilización efectiva de las aplicaciones académicas y financieras, mediante la comprobación del cifrado de las copias de seguridad almacenadas en el exterior, así como no permitir el acceso a usuarios no autorizados y administrar contraseñas y su almacenamiento por separado, también hacer uso del algoritmo estándar seguro, de forma tal que se garantice una utilización efectiva de la información contenida en la base de datos.
- Crear una guía estandarizada de la información a ser recopilada de forma tal que se pueda brindar una información ordenada y oportuna y que la misma pueda ser analizada de forma eficiente según lo planteado en la OWASP, a través del desarrollo de planes de cambios de contraseña, protección de las teclas fuertes contra accesos no autorizados y garantizar que los algoritmos potentes tales como la transmisión admitan claves.
- Automatizar a futuro el proceso de estudio de vulnerabilidades de las aplicaciones académicas y financieras tomando en cuenta las especificaciones derivadas del uso de la guía estandarizada en la recolección de la información con la utilización de sistemas anteriores y otros sistemas SSL.

- Desarrollar un análisis sistemático de los aspectos a ser tomados en cuenta tales como la configuración de la función segura en cada cookie de mayor riesgo, del mismo modo se configurará el servidor SSL con la finalidad de encontrar un potente algoritmo en la utilización futura de las aplicaciones académicas y financieras en plena concordancia con los parámetros contenidos en las actualizaciones OWASP 2013.
- Solicitar SSL para las aplicaciones de forma tal que su utilización no se limite a páginas privadas o críticas de forma tal que se garantice identificadores de sesión, así como el correcto uso de la información confidencial.

8. REFERENCIAS BIBLIOGRÁFICAS

Areito, J. (2016). *Seguridad de la información. Redes, Informática y sistemas de información.* Madrid: Cengage Learning Paraninfo S.A.

Beust, C. (2015). *Programación Java Server con J2EE.* Barcelona: Anaya Multimedia.

Cabré, T. (2015). *Terminología y buenas prácticas.* Barcelona: Publifarum.

Cardador, A. L. (2014). *Implantación de Aplicaciones Web en entornos Internet, Intranet y Extranet.* Málaga: ic editorial.

Latorre, M. (2018). *Historia de las Web.* Perú: Universidad Marcelino Champagnat.

López, M., & Echeverry, C. (2014). *Servicios de gestión de conocimiento utilizando la computación en Nube.* Manizales: Universidad nacional de Colombia.

Marini, E. (2012). El modelo cliente/servidor. 11.

Mateu, C. (2012). *Desarrollo de Aplicaciones Web.* Cataluña: Eureca Media, SL.

Mateu, C. (2014). *Seguridad de las aplicaciones web.* Tarragona: Eureca Media SL.

Montoya, C. E., Uribe, C. A., & Rodríguez, L. E. (2013). Seguridad en la configuración del servidor web Apache. *INGE CUC*, 31-38.

OWASP. (2017). *Los díez riesgos más criticos en aplicaciones web*. Obtenido de owasp.org

Paredes, B. (2014). *Especificaciones técnicas para medir vulnerabilidades informáticas.* México D.F.: Trillas.

Quero, E., García, A., & Peña, J. (2017). *Mantenimiento de Portales de Información: explotación de sistemas informáticos.* Madrid: P.S.A. International Thomson Editores.

Rodríguez, M. (2017). *Scrum desde cero.* Madrid: Mc. Graw-Hill.

Zalewski, M. (2012). *La web enredada: guía para la seguridad de aplicaciones web modernas.* Madrid: Anaya.

Anexo #11

Cuadro comparativo de Investigaciones anteriores

Cuadro comparativo de Investigaciones anteriores

CUADRO COMPARATIVO DE TRABAJOS DE INVESTIGACIÓN ACERCA DE LA MISMA TEMÁTICA			
PARÁMETRO / **TEMA**	DIAGNÓSTICO DE LAS VULNERABILIDADES INFORMÁTICAS EN LAS APLICACIONES WEB DE LA UNIVERSIDAD CENTRAL DEL ECUADOR	ANÁLISIS DE LAS APLICACIONES WEB DE LA SUPERINTENDENCIA DE BANCOS Y SEGUROS, UTILIZANDO LAS RECOMENDACIONES TOP TEN DE OWASP PARA DETERMINAR LOS RIESGOS MÁS CRÍTICOS DE SEGURIDAD E IMPLEMENTAR BUENAS PRÁCTICAS DE SEGURIDAD PARA EL DESARROLLO DE SUS APLICATIVOS	ANÁLISIS DE VULNERABILIDADES DE SOFTWARE PARA MEJORAR LA SEGURIDAD EN LOS SISTEMAS INFORMÁTICOS.
Resumen	Las aplicaciones se desarrollan de acuerdo con los requisitos del campo de garantía de calidad; los requisitos que surgen de cada dependencia de una institución, tanto académica como administrativa, si se verifican la	En la actualidad las aplicaciones web se han vuelto indispensables para el manejo de la información en una organización, convirtiéndose en una herramienta que permite al usuario acceder y utilizar un sistema informático	Este proyecto consiste en el desarrollo de un sistema seguro para el Cementerio Municipal de Riobamba, mediante el estudio de tres vulnerabilidades más comunes que afectan las aplicaciones web: Inyección

	viabilidad y la rentabilidad, se establecen procesos generales y específicos, reflejados en documentos con requisitos funcionales transferidos al desarrollar un dominio para el análisis y diseño de una base de datos y, finalmente, para el desarrollo de un sistema, siendo el objetivo de la investigación analizar las vulnerabilidades de las aplicaciones web desarrolladas en la Universidad Central del Ecuador, aplicando una investigación contrastiva y aplicada, utilizando como base el Top 10 de OWASP – 2017, concluyendo que se revelan como de vital importancia además que el manejo de información es elevado dado que son sistemas que se actualizan periódicamente significando los mismos la posibilidad de brindar un funcionamiento óptimo para dicha institución.	a través de internet mediante un navegador web, permitiendo el acceso a la información desde cualquier parte del mundo. La Superintendencia de Bancos y Seguros al ser una institución Pública se ha visto obligada a la adopción de estándares abiertos y software libre para automatizar sus procesos, y ha desarrollado aplicaciones web utilizando la plataforma Java Enterprise Edition (JEE) sin embargo no se ha aplicado ningún tipo de estándar o buenas prácticas en el aseguramiento del aplicativo. El presente proyecto tiene como objetivo el análisis de riesgos de las aplicaciones web utilizando las recomendaciones OWASP Top 10 – 2010 para descubrir las vulnerabilidades que se presenta durante el desarrollo de un software y estimar el riesgo asociado para el negocio. A partir de los resultados obtenidos donde se identificaron la ocurrencia de almacenamiento criptográfico inseguro y	SQL, Secuencia de comandos cruzados (XSS) y la falsificación de sitios cruzados (CSRF). En primer lugar, se ha realizado el análisis de diez vulnerabilidades de software que nos presentó la organización OWASP (Te Open Web Aplicación Security Project) sobre el análisis y la seguridad de las aplicaciones web. El Cementerio Municipal de la ciudad de Riobamba maneja toda la información de catastro de: bóvedas particulares, bóvedas institucionales, nichos, mantenimiento de bóvedas y nichos de forma manual, la cual provoca una gran pérdida de tiempo al momento de registrar, buscar y modificar la información de alguna persona fallecidas, demás dicha búsqueda no siempre es exitosa. De igual forma conlleva a la confusión o pérdida de información al momento de trascribir los todos datos a una hoja de Excel.

		protección insuficiente en la capa de transporte se realizó una propuesta de buenas prácticas para asegurar las aplicaciones, corregir los riesgos detectados y asegurar el proceso de desarrollo de nuevas funcionalidades y existentes.	Se estudian las vulnerabilidades según las características más comunes y peligrosas en el mundo para las cuales se implementó mecanismo de protección para disminuir el impacto en el sistema para el Cementerio Municipal de Riobamba.
Metodología	OWASP Top 10 – 2017	OWASP Top 10 – 2010	OWASP Top 10 – 2013
Institución	Universidad Central del Ecuador	Superintendencia de Bancos y Seguros	Cementerio Municipal de Riobamba
Autores	Andrade Rodríguez María José Zambrano Vélez Grace Marcela	Salgado Yánez Angel Lenin	Gavidia Villacrés Marco Vinicio Valle Padilla Jessica Janneth

Anexo #12
Matriz de riesgos

Matriz de riesgos

MATRIZ DE RIESGOS

DEFINICIÓN DE APLICACIONES CRÍTICAS DESARROLLADAS EN LA UNIVERSIDAD CENTRAL DEL ECUADOR

APLICACIONES AUDITABLES	A	FACTORES DE RIESGO DE NEGOCIO				B	C = A * B	
	AUDIT RISK RANKING	Financiero	Estratégico	Operativo	Legal-Cumplimiento	FACTORES DE RIESGO EMPRESARIAL CLASIFICACIÓN	CLASIFICACIÓN DE RIESGOS TOTALES	Porcentaje (%)
	Ponderación de Riesgo	5*	4*	3*	2*			
Sistema de Recaudaciones Sysrec	270	1	1	1	0	12	3240	57.86
Sistema de Información Integral - Módulo Académico	243	1	0	1	1	10	2430	43.39
Sistema de Talento Humano - Módulo Nómina	243	1	0	1	1	10	2430	43.39
Plataforma Educativa Virtual	264	1	0	1	0	8	2112	37.71
Sistema de Investigación	232	0	1	1	1	9	2088	37.29
Sistema de Talento Humano - Módulo Personal	144	1	1	1	1	14	2016	36.00
Sistema de Gestión Documental	225	0	1	1	0	7	1575	28.13
Sistema de Registro de Funcionarios	120	1	0	0	1	7	840	15.00
							TOTAL	16731

Mínimo:	0
Máximo:	5600
PONDERACIÓN DEL RIESGO	
Riesgo Alto:	67 % - 100 %
Riesgo Medio:	34 % - 66 %
Riesgo Bajo:	1 % - 33 %

Fuente: Autores