
# UNIVERSIDAD ESTATAL
# PENÍNSULA DE SANTA ELENA

**FACULTAD DE SISTEMAS Y TELECOMUNICACIONES**

DISEÑO E IMPLEMENTACIÓN DE UNA AUDITORÍA DE SEGURIDAD A LA INFORMACIÓN DE LOS DATOS SENSIBLES DE UN CENTRO DE EDUCACION SUPERIOR.

## TESIS DE GRADO

Previa a la obtención del Título de:

**INGENIERA EN SISTEMAS**

**AUTORA:** BRENDA BONILLA TUMBACO

**TUTOR:** ING. CARLOS SÁNCHEZ LEÓN

**LA LIBERTAD – ECUADOR**

**2015**

# UNIVERSIDAD ESTATAL
# PENÍNSULA DE SANTA ELENA

## FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

DISEÑO E IMPLEMENTACIÓN DE UNA AUDITORÍA DE SEGURIDAD A LA INFORMACIÓN DE LOS DATOS SENSIBLES DE UN CENTRO DE EDUCACION SUPERIOR.

## TESIS DE GRADO

Previa a la obtención del Título de:

## INGENIERA EN SISTEMAS

**AUTORA:** BRENDA BONILLA TUMBACO

**TUTOR:** ING. CARLOS SÁNCHEZ LEÓN

**LA LIBERTAD – ECUADOR**

**2015**

La Libertad, 2 de Marzo del 2015

## APROBACIÓN DEL TUTOR

En mi calidad de tutor del trabajo de investigación, “DISEÑO E IMPLEMENTACIÓN DE UNA AUDITORÍA DE SEGURIDAD A LA INFORMACIÓN DE LOS DATOS SENSIBLES DE UN CENTRO DE EDUCACION SUPERIOR”, elaborado por la Srta. Brenda Bonilla Tumbaco, egresada de la Carrera de Informática, Escuela de Informática, Facultad de Sistemas y Telecomunicaciones del centro de educación superior, previo a la obtención del Título de Ingeniera en Sistemas, me permito declarar que luego de haber orientado, estudiado y revisado, la apruebo en todas sus partes.

Atentamente

……

**Ing. Carlos Sánchez León**

**DOCENTE TUTOR**

## DEDICATORIA

A Dios por derramar grandes y poderosas bendiciones permitiéndome culminar con éxitos este proyecto.

Con mucho amor a mis adorados padres Marlene Tumbaco y Ángel Bonilla, siendo ellos mi orgullo, por ser mis pilares fundamentales brindándome siempre su apoyo y guiado en el camino para lograr mis objetivos a lo largo de mi vida y más en mi formación como profesional.

***Brenda***

## AGRADECIMIENTO

Agradezco a mis amados padres Marlene y Ángel por su motivación constante que me permitió hacer frente nuevos retos haciéndome crecer como persona y profesional. A José M. por su apoyo incondicional.

Al Departamento de Unidad de Producción de la Escuela de Informática por permitirme desarrollar mi trabajo de tesis y brindarme su confianza y a todos aquellos que de alguna manera me ayudaron con la culminación de mi trabajo, especialmente a Camilo G. Dédalo.

***Brenda***

## TRIBUNAL DE GRADO

| | |
|---|---|
| _____ | _____ |
| Ing. Fredy Villao Santos, MSc.<br>Decano de la Facultad de<br>Sistemas y Telecomunicaciones | Ing. Walter Orozco Iguasnia, MSc.<br>Director de Escuela de<br>Informática |
| _____ | _____ |
| Ing. Carlos Sánchez León MSc.<br>Profesor - Tutor | Ing. José Sánchez Aquino<br>Profesor Área |

_____

Ab. Joe Espinoza Ayala

Secretario General

**UNIVERSIDAD ESTATAL "PENÍNSULA DE SANTA ELENA"**
**FACULTAD DE SISTEMAS Y TELECOMUNICACIONES**
**ESCUELA DE INFORMÁTICA**
**"DESEÑO E IMPLEMENTACIÓN DE UNA AUDITORÍA DE SEGURIDAD A LA INFORMACIÓN A LOS DATOS SENSIBLES DE UN CENTRO DE EDUCACION SUPERIOR"**

**Autora:** BRENDA ESTEFANIA BONILLA TUMBACO

**Tutor:** CARLOS SANCHEZ LEÓN

## RESUMEN

Los Centros de Educación Superior aportan al desarrollo tecnológico y científico en la Educación Superior, además, se caracteriza de brindar a la comunidad universitaria acceso a las aplicaciones de Internet y sistemas de información, a través del sitio Web oficial del centro de educación superior; así como avanza y se utilizan las tecnologías en las Instituciones, al mismo tiempo aumentan las amenazas de ataques informáticos; por este motivo es considerable conocer las fortalezas y debilidades a las que pudieran estar sometidos los datos privados que se encuentran en custodia por el centro de educación superior, mediante la implementación de una auditoría de seguridad a la plataforma informática WEB, utilizando herramientas de software libre con el objetivo de sugerir estrategias que minimicen la ocurrencia de estas amenazas y explotación de vulnerabilidades, el resultado esperado en la ejecución de esta auditoría es la optimización de seguridad de la información que reposa en las bases de datos, la cual sirve de complemento para los administradores de sistemas de información en la toma de decisiones, así mismo al correcto control de seguridad informática, ya que se brindarán medidas específicas de corrección y recomendaciones preventivas de seguridad para resolver los posibles problemas, buscando mantener la confidencialidad, la disponibilidad e integridad.

## Contenido

# ÍNDICE DE TABLAS

# ÍNDICE DE FIGURAS

# INTRODUCCIÓN

En la actualidad estamos inmersos en un mundo donde la tecnología es un recurso primordial para optimizar, agilizar y perfeccionar las actividades; motivo por el cual se han desarrollado diferentes sistemas informáticos que brindan servicios, los mismos que están expuestos a ataques, por ello se ha visto la necesidad de que se realicen auditorías informáticas para garantizar la seguridad e integridad de los datos.

El centro de Educación Superior contiene información primordial; entre estos tipos de información podemos mencionar datos académicos, administrativos y de investigación los mismos que están expuestos en sistemas informáticos, por este motivo surge la necesidad de realizar un estudio técnico para identificar las diversas amenazas y vulnerabilidades que puedan presentarse, obtenido estos resultados se elabora un informe brindando medidas preventivas que permitan resolver los posibles problemas de seguridad.

En el **Primer Capítulo** se plantea la problemática, la justificación y los objetivos que se desea cumplir en el presente trabajo; continuando con el **Segundo Capítulo**, el cual contiene las bases teóricas de los diferentes temas que se señalarán en el proyecto. El contenido del **Tercer Capítulo** detalla las metodologías de investigación utilizadas para el levantamiento de información; así mismo el análisis técnico, económico y operativo del proyecto junto al análisis e interpretación de resultados de las encuestas y entrevistas desarrolladas. En el **Cuarto Capítulo** se observa el diseño de la auditoría a implementar, especificando las fases para desarrollar la auditoría de seguridad en el capítulo posterior. El **Quinto Capítulo** refleja las evidencias recolectadas durante la implementación y ejecución de las diferentes fases de la auditoría de seguridad, los cuales proveen la base para el reporte final.

# CAPÍTULO I

# MARCO REFERENCIAL

## 1 MARCO REFERENCIAL

En este capítulo se describen los objetivos que se desean cumplir, además se detalla el problema actual en que están expuestos los datos referentes a su seguridad; así mismo se justifica la realización de una auditoría en seguridad a la información de datos sensibles que manejan las plataformas web del centro de educación superior.

## 1.1 Identificación del Problema

Los sistemas informáticos surgieron con la necesidad de facilitar el trabajo y administración de información de los usuarios, estos datos pueden ser de carácter confidencial o públicos, sin embargo la seguridad era un factor ausente al no presentarse situaciones de riesgos, intrusiones o manipulaciones en sistemas informáticos, este aspecto se omitía debido a que la existencia de ataques era mínima.

En la actualidad las instituciones se han hecho dependientes de sistemas y redes informáticas, esto incita a quienes se dedican realizar intrusiones con fines maliciosos para obtener información y usarla a su conveniencia, así mismo la presencia de herramientas que facilitan el trabajo de un atacante al detectar vulnerabilidades, y valerse de estas para explotarlas con la finalidad de tener acceso a datos confidenciales sin respetar las Leyes y normativas de cada organización.

Las Instituciones se han visto en la necesidad de buscar herramientas de seguridad informática e implementarlas; con el objetivo de optimizar los controles de seguridad de sus sistemas informáticos, salvaguardando información que se encuentran en los repositorios de datos evitando perdidas, ediciones, hurto y eliminación de datos que afecten a su integridad, disponibilidad y confidencialidad. Además efectuar o adquirir auditorías internas y externas en los sistemas informáticos es de suma importancia para obtener un análisis global con la evaluación de los riesgos a los cuales pueden estar sometidos los datos que se encuentran en custodia por la institución; al realizar auditorías se estaría cumpliendo con las normativas y estándares de calidad de seguridad a la información, entre los patrones existentes tenemos: ISO 27001 e ISO 27002, los mismos que tienen como objetivo “Garantizar la seguridad de los sistemas”.

## 1.2 Situación actual del Problema

El centro de educación superior con el uso de plataformas Web registran, modifican, almacenan y consultan gran cantidad de datos, convirtiendo éstos en información valiosa que deben ser tratados cuidadosamente. Este Centro de Educación Superior cuenta con la Unidad de Producción de la Escuela de Informática, la misma que ha ido implementando constantes actualizaciones en sus plataformas sistemáticas, brindando servicios en línea que permiten agilizar los procesos de flujo de información creando un banco de datos que requieren un control de seguridad en las aplicaciones.

Hace mucho tiempo la página web oficial del centro de educación superior fue intercedida y modificada por terceras personas. En las aplicaciones que se encuentran ubicadas en el sitio Web del centro de educación superior (WEB), se procesa y maneja información incluyendo datos sensibles, considerándose un factor de riesgo que incita a un atacante ocasionar perjuicios e intrusiones dentro de los sistemas de información al no contar con un debido control de seguridad.

El personal administrativo del departamento informático afirmó que nunca se ha realizado un test de intrusión para garantizar la seguridad de los sistemas; por lo tanto surge la necesidad de realizar una auditoría de seguridad a la información en las aplicaciones Web utilizando varios tipos de herramientas y técnicas de Hacking Ético con el fin de encontrar posibles vulnerabilidades en la WEB y conocer el nivel de seguridad de los sistemas. Es importante saber que día a día se generan nuevas vulnerabilidades en los sistemas, y con la existencia de la web es fácil adquirir herramientas que logren explotar estos fallos; una persona puede hacer uso de estos recursos sin tener conocimientos previos.

## 1.3 Justificación del Problema

La comunidad universitaria hace uso de las tecnologías de información, entre ellas; las aplicaciones Web, siendo un punto de ataque para los delincuentes informáticos con el fin de alterar o robar los datos privados que maneja el centro de educación superior.

Existe la necesidad de combatir las vulnerabilidades que inducen a que los sistemas de información sean inseguros, por tal motivo el centro de educación superior requiere de una evaluación para optimizar la seguridad de los datos, debido a que no se ha realizado antes una auditoría de seguridad externa para conocer el nivel de seguridad de la información; por esta razón es considerable que se realice un test de intrusión para hallar vulnerabilidades con la finalidad de mejorar la calidad en el control de seguridad; más no con finalidades maliciosas que perjudiquen la confidencialidad de la información del centro de educación superior.

La implementación de una auditoría de seguridad a la información del centro de educación superior permitirá conocer el nivel de protección, manteniendo la integridad de los datos, evaluando la eficiencia y eficacia de las aplicaciones web con el propósito de seguir ofreciendo calidad en sus servicios, y así brindar a los usuarios confianza para almacenar información privada con alta seguridad y protección de los mismos.

Después de realizar la auditoría y obtener las debilidades en los sistemas, se brindará un informe detallando las soluciones a las vulnerabilidades con sus respectivas recomendaciones; contribuyendo para la toma de decisiones en el control de seguridad de los sistemas a cargo del departamento de Unidad de Producción de la Escuela de Informática del centro de educación superior e inmediatamente dicho informe puede ser implementado por el personal a cargo de los sistemas en caso de que así lo desee.

## 1.4 OBJETIVOS

### 1.4.1 Objetivo General

Implementar una auditoría de seguridad a la plataforma informática WEB del centro de educación superior, mediante el uso de herramientas Open Source para identificación de amenazas y optimización en la protección de datos expuestos en la red universitaria.

### 1.4.2 Objetivos Específicos

- ✓ Analizar metodologías de Testeo de Seguridad para el estudio de vulnerabilidades, prevención y protección contra fallos encontrados en las aplicaciones Web.

- ✓ Seleccionar las diferentes herramientas que provee Linux para el pentest de las aplicaciones, basado en las metodologías de hacking ético.

- ✓ Ejecutar ataques controlados y técnicas de penetración al sistema para la identificación de vulnerabilidades.

- ✓ Evaluar los resultados obtenidos en la realización de las pruebas de penetración y determinar soluciones para los fallos encontrados.

## 1.5 Hipótesis

La implementación de una auditoría de seguridad a la plataforma informática WEB del centro de educación superior, permitirá identificar las amenazas y optimizar la protección de datos expuestos en la red universitaria.

## 1.6 Resultados esperados

- El análisis de las metodologías de testeo de seguridad ayudará con la determinación de las etapas del diseño de auditoría.

- Al realizar un análisis de metodologías de hacking ético se determinarán las técnicas a utilizar para el proceso de auditoría.

- En el proceso de auditoría se realizará la identificación de vulnerabilidades en la plataforma WEB del centro de educación superior.

- Después de la identificación de vulnerabilidades se analizarán las posibles soluciones.

- Informe con estrategias, recomendaciones y soluciones posibles que servirán para fortalecer los niveles de seguridad en las aplicaciones que contiene el WEB del centro de educación superior.

# CAPÍTULO II

# MARCO TEÓRICO

## 2 MARCO TEÓRICO

Brinda las bases necesarias de conceptualización de los temas que va a contener el presente trabajo a lo largo de su desarrollo. El objetivo de este capítulo es tener conocimiento de términos que son utilizados en auditorías de seguridad a la información.

## 2.1 Antecedentes

### 2.1.1 Históricos

La seguridad de la información ha evolucionado considerablemente desde la utilización de la maquina enigma en la Segunda Guerra Mundial cuya función era de cifrar y descifrar mensajes, con la finalidad de proteger los datos; tiempo después Alan Turing descifró el código secreto de la maquina enigma, esto es una referencia que la seguridad absoluta no es posible, de forma que el elemento de riesgo está siempre presente.

Con la aparición de la informática, las redes de datos y el Internet, su masiva utilidad ha producido un número creciente de problemas de seguridad, debido al flujo de datos privados que son enviados a través de la red que pueden ser interceptados por hackers. Existen distintos grupos de comunidades de individuos que intentan encontrar vulnerabilidades en sistemas informáticos; estos grupos se identifican por el color de sombrero que utilizan cuando realizan sus investigaciones de seguridad, este tono indica cuáles son sus propósitos. Los hackers de sombrero blanco realizan test de pruebas en redes y sistemas para examinar el rendimiento, determinando que tan vulnerables son ante una intrusión; estos hackers trabajan éticamente con sistemas propios o de un cliente con propósitos de auditorías de seguridad. Los hackers de sombrero negro son aquellos que buscan vulnerabilidades en sistemas con fines maliciosos; especializados para explotarlas, descubrir información privada o confidencial los cuales son para beneficio personal o para producir anomalías a un sistema o red.

No existe un sistema 100% seguro independientemente de las medidas de seguridad tomadas; sin embargo existen hackers que no importa cuál sea su intención, lo primordial es conocer las vulnerabilidades de los sistemas y evitar que estas sean explotadas.

### 2.1.2 Legales

Algunas de las Leyes y normas que regulan la protección de datos en Ecuador son:

La Ley del Sistema Nacional de Registro de Datos Públicos indica en:

> El artículo 66, numerales 19 y 28 garantizan los derechos a la identidad colectiva y personal y a la protección de datos de carácter personal, el cual incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. (Ley N° 162 Sistema Nacional de Registro de Datos Públicos, 2010)

Ley de Comercio Electrónico, Firmas y Mensajes de Datos en su Art. 9 establece:

> Protección de datos.- Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros. (Ley No. 2002-67 Ley de Comercio Electrónico, Firmas y Mensajes de Datos, 2002)

Ley Organica de Transparencia y Acceso a la Información Pública considera Información Confidencial:

> Se considera información confidencial aquella información pública personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales, especialmente aquellos señalados en los artículos 23 y 24 de la Constitución Política de la República.

> El uso ilegal que se haga de la información personal o su divulgación, dará lugar a las acciones legales pertinentes. (Ley Organica de Transparencia y Acceso a la Información Pública, 2004)

Existen Leyes penales contra los delitos informáticos. Los siguientes artículos del Código Orgánico Integral Penal juzgan:

Art. 202.-

> El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica. (El Código Orgánico Integral Penal, 2014)

Art. 262.-

> Serán reprimidos con tres a seis años de reclusión menor, todo empleado público y toda persona encargada de un servicio público, que hubiere maliciosa y fraudulentamente, destruido o suprimido documentos, títulos, programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, de que fueren depositarios, en su calidad de tales, o que les hubieren sido encomendados sin razón de su cargo. (El Código Orgánico Integral Penal, 2014)

Art. 415.-

> Daños informáticos.- El que dolosamente, de cualquier modo o utilizando cualquier método, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, será reprimido con prisión de seis meses a tres años y multa de sesenta a ciento cincuenta dólares de los Estados Unidos de Norteamérica. (El Código Orgánico Integral Penal, 2014)

Entre los estándares de seguridad de la información tenemos:

Entre otros estándares existen: “Las normas publicadas bajo la serie ISO 27000 son estándares alineados con el conjunto de normas publicadas por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission) actuales o futuras y que son desarrolladas mediante comités técnicos específicos” (Normas ISO 27000, 2009).

La norma ISO 27001: “Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización” (NORMAS ISO 27001, 2005).

De la familia de normas ISO 27000 existe otro estándar para la seguridad de la información. ISO 27002 que:

> Proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.

> La seguridad de la información se define en el estándar como "la preservación de la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (asegurando que la información y sus métodos de proceso son exactos y completos) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran). (NORMAS ISO 27002, 2007).

Buscar metodologías para poder controlar los sistemas informáticos en la actualidad es complejo por tal motivo existen leyes y estándares para mantener la seguridad de los datos en conjunto con el uso de auditorías de seguridad informática.

## 2.2 Bases Teóricas

### 2.2.1 Seguridad Informática

Se necesita distinguir entre seguridad informática y seguridad de la información, comúnmente se piensa que es lo mismo cuando en realidad son dos cosas distintas.

La Seguridad Informática en sí es un conjunto de estándares, políticas, métodos y protocolos encargados de resguardar la infraestructura tanto Hardware como Software incluyendo la información administrada y almacenada por los mismos, garantizando su disponibilidad, integridad y confidencialidad. (Piattini Velthuis & Del Peso Navarro, 2001)

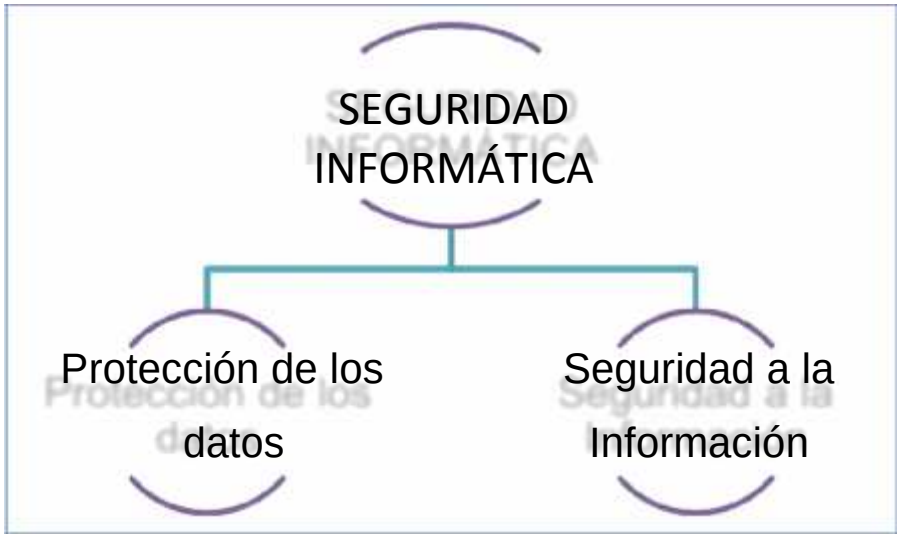


**Figura 1 Seguridad Informática.**

Fuente: https://protejete.wordpress.com/gdr_principal/seguridad_informacion

### 2.2.2 Seguridad a la Información

"La seguridad de la información consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización" (NORMAS ISO 27001).


**Figura 2 Seguridad a la Información**

Fuente: https://protejete.wordpress.com/gdr_principal/seguridad_informacion

> La protección de datos es una disciplina jurídica de reciente creación que tiene por objeto proteger la intimidad y demás derechos fundamentales de las personas físicas frente al riesgo que para ellos supone la recopilación y el uso indiscriminado de sus datos personales. (Portal Formativo sobre protección de datos, 2008)

La protección de datos es un derecho que todos merecemos, salvaguardar los datos personales se sitúa dentro del campo de derecho informático; se refiere a su garantía en la protección de la información manejada por un Hardware y Software evitando el uso indiscriminado, divulgación, supresión, modificación o con cualquier fin que perjudique a una persona. La Ley establece un tratamiento especial a los datos privados.

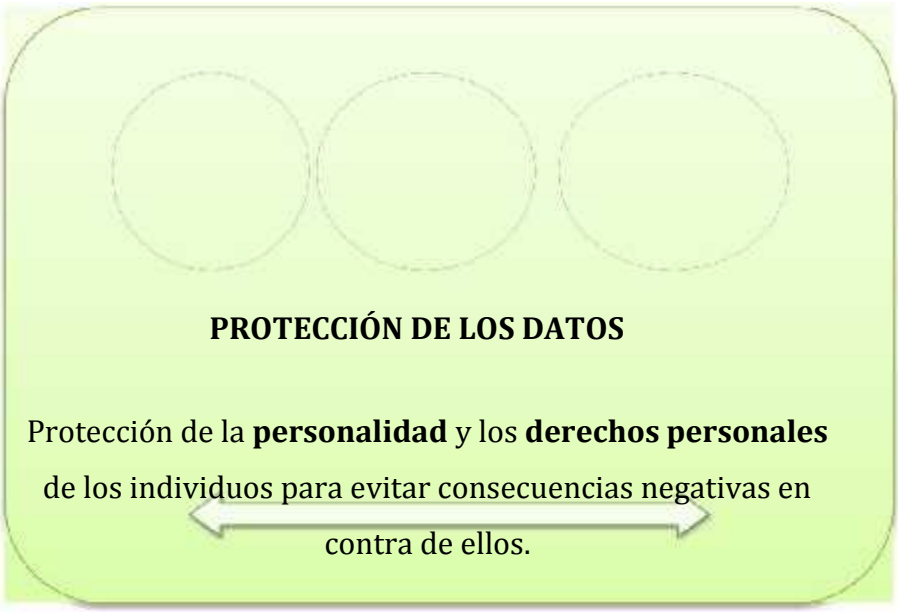


**Figura 3 Protección de los Datos**

Fuente: https://protejete.wordpress.com/gdr_principal/seguridad_informacion

### 2.2.3 Objetivos de la Seguridad a la Información

La Seguridad a la Información tiene la función y principal objetivo de conservar las siguientes características:

**Integridad**: Garantizar que la información no sufra cambios sin ser autorizados, la perdida de integridad puede causar decisiones erróneas o fraudes.

**Confidencialidad**: Certificar que sólo el personal autorizado tenga acceso a los datos.

**Disponibilidad:** Garantizar el acceso a los sistemas de información por personas autorizadas en el momento que lo requieran.

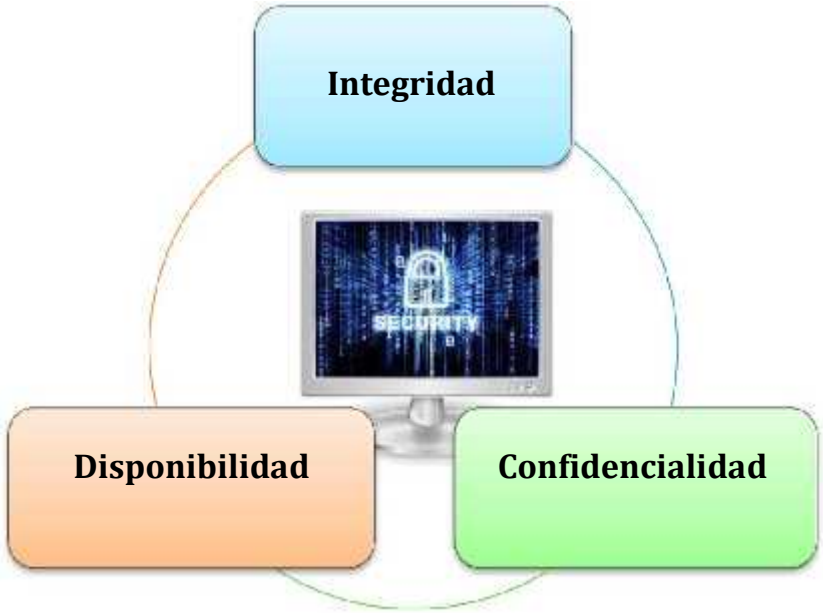


**Figura 4 Características de Seguridad a la Información**

Fuente: http://telematicanet.ucol.mx/moodle/course/info.php?id=2

### 2.2.4 Amenazas

Toda acción capaz de provocar un delito o daño contra los sistemas de información y su seguridad en los datos. Las amenazas se clasifican: Según el Origen:

> **Externo:** Se ocasionan en forma remota, fuera de las instalaciones de la organización, un atacante al no tener información del sistema informático debe realizar varios pasos para conocer qué es lo que hay en ella y buscar la manera de atacar.

**Interno:** Se originan dentro de la organización, son consideradas más serias que las externas, los usuarios tienen conocimiento del funcionamiento del sistema informático.

Según el área de consecuencia:

**Humana:** Vulneran las seguridades utilizando como medio a las personas.

**Física:** Afecta a los componentes físicos de la organización.

**Lógica:** Vulnera a todo lo relacionado con el Software (activos de naturaleza digital).

Según el efecto que provocan:

**Interrupción:** Dificulta la continuidad de los servicios, provocando que queden no disponibles.

**Interceptación:** Acceso a los datos por personas no autorizadas.

**Modificación:** Alteración de los datos por parte de una persona no autorizada.

**Fabricación:** Una persona no autorizada crea un objeto similar al atacado para ser insertado y suplantado.

### 2.2.5 Hacking Ético

El Hacking Ético es una forma de representar la acción de una persona que usa sus conocimientos y habilidades de seguridad informática realizando pruebas en las redes de datos y demás sistemas informáticos de una organización para encontrar vulnerabilidades, estas se reportan con el objetivo de corregirlas antes que ocurra alguna sustracción de información.

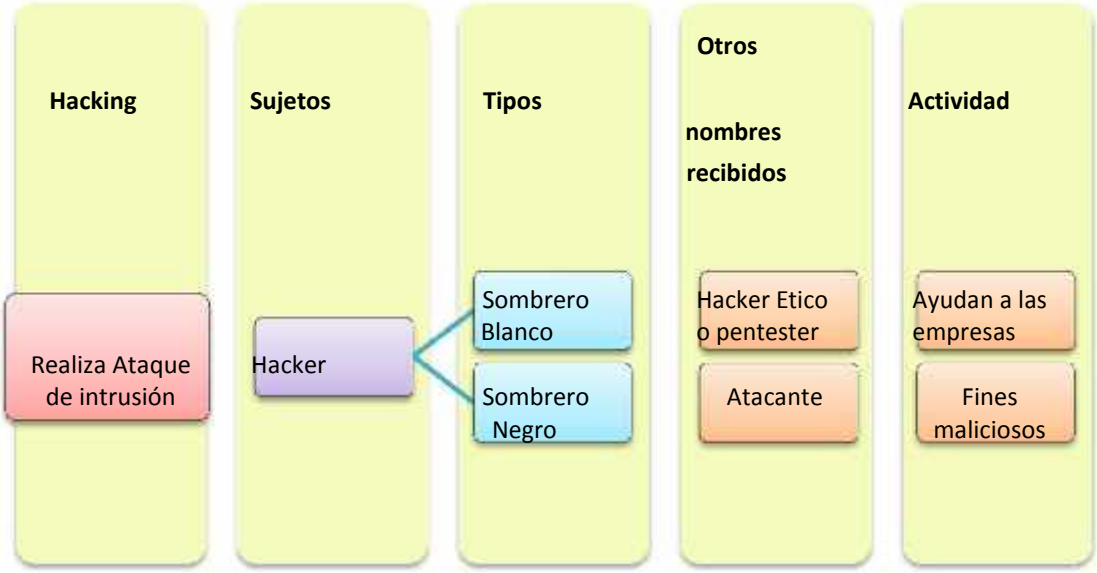


**Figura 5 Hacking Ético**

Fuente: http://www.gitsinformatica.com/hackers.html

Existen dos términos que se relacionan con la expresión Hacking Ético:

**Los hackers de sombrero blanco** son quienes examinan sistemas o redes para conocer sus capacidades y determinar qué tan vulnerables son ante una intrusión con el propósito de controlar su seguridad.

**Los hackers sombrero negro** es sinónimo de atacante, estos intentan provocar un daño explotando las vulnerabilidades existentes dejando al descubierto información valiosa de un determinado sistema o red.

**Un hacker ético** tiene la necesidad de mantenerse dentro de la Ley y siempre actuar de manera profesional.

### 2.2.6 Metodologías de Hacking Ético

Para realizar un test de penetración sea con o sin objetivos, interna o externamente existen tres tipos de accesos a la red objetivo.

**Test de caja negra:** El testeador o auditor no dispone de información previa sobre los elementos a auditar. Simula un ataque real.

**Test de caja blanca:** Se tiene información previa permitiéndonos omitir la fase inicial de recolección de información.

**Test de caja gris:** Al igual que la caja negra se simulan ataques reales pero conociendo gran parte de la información técnica al igual que la caja blanca.

Un pentest o test de penetración está compuesta por 4 fases, dichas fases se modifican en cuanto el contenido y orden dependiendo del método utilizado. Las fases básicas para realizar un pentest son:

1. Recopilación de información.
2. Generación de informes y/o parcheo de los sistemas.
3. Búsqueda de vulnerabilidades.
4. Explotación de vulnerabilidades.

### 2.2.7 Auditoría de seguridad a la información

Una auditoría de seguridad a la información es un estudio que se enfoca en la gestión y análisis de sistemas de información efectuado por profesionales informáticos para identificar, enumerar y describir las diferentes vulnerabilidades que puedan existir en una revisión en las redes de datos y aplicaciones.

Con los resultados obtenidos en el proceso de la auditoría se procede a su identificación, luego se registran y reportan al personal responsable por los sistemas informáticos. Se deberán establecer medidas preventivas de refuerzo y/o corrección que permitan a los administradores perfeccionar la seguridad de sus sistemas.

La realización de una auditoría de seguridad a la información nos permitirá conocer la situación exacta en que se encuentran sus activos de información en cuanto a protección, control y medidas de seguridad en el momento que se la realiza la auditoría. (José Antonio Echenique García, 2001).

### 2.2.8 Kali Linux

“Kali Linux es una distribución basada en Debian GNU/Linux diseñada principalmente para la auditoría y seguridad informática en general” (Wikipedia.org, 2015) .

### 2.2.9 Manual de metodología abiertade testeo de seguridad, OSSTMM

OSSTMM (Open Source Security Testing Methodology Manual), es un estándar internacional que indica los métodos para la realización de Auditorías basadas precisamente para la seguridad de la información, seguridad de los procesos, seguridad física, seguridad inalámbrica, seguridad en las comunicaciones y en la seguridad en las tecnologías de internet. La metodología OSSTMM (Manual de metodología abierta de testeo de seguridad), es una de las más relevantes a nivel internacional es de licencia abierta, orientada para cualquier tipo de organización.


**Figura 6 Elementos Metodología de análisis de riesgo**

**Fuente:** http://tesis-toth.com.ar/fai/wp-content/uploads/2014/05/Tesis-Toth.pdf

### 2.2.10 Proyecto abierto de seguridad de aplicaciones Web, OWASP

OWASP (Open Web Application Security Project), es un proyecto que contiene una lista de pruebas a realizar exclusivamente en seguridad de aplicaciones Web. Su objetivo es ayudar a las empresas para comprobar la fiabilidad y seguridad de sus aplicaciones.

El proyecto OWASP ha definido una lista de diez vulnerabilidades más críticas, esta lista se conoce como OWASP Top 10; pero estas no son las únicas, pues existen mucho más riesgos y vulnerabilidades que pueden suceder en las aplicaciones.

| OWASP Top 10 – 2013 (Nuevo) |
| --- |
| A1 – Inyección |
| A2 – Pérdida de Autenticación y Gestión de Sesiones |
| A3 – Secuencia de Comandos en Sitios Cruzados (XSS) |
| A4 – Referencia Directa Insegura a Objetos |
| A5 – Configuración de Seguridad Incorrecta |
| A6 – Exposición de Datos Sensibles |
| A7 – Ausencia de Control de Acceso a las Funciones |
| A8 – Falsificación de Peticiones en Sitios Cruzados (CSRF) |
| A9 – Uso de Componentes con Vulnerabilidades Conocidas |
| A10 – Redirecciones y reenvíos no validados |

**Figura 7 Top 10 OWASP**

Fuente: www.owasp.org/images/5/5f/OWASP_Top_10_-_2013_Final_-_Espa%C3%B1ol.pdf

## 2.3 VARIABLES

### Hipótesis

La implementación de una auditoría de seguridad a la plataforma informática (WEB) del centro de educación superior, permitirá identificar las amenazas y optimizar la protección de datos expuestos en la red universitaria.

### 2.3.1 Variable Independiente

Auditoría de seguridad a la plataforma informática.

### 2.3.2 Variable Dependiente

Identificación de amenazas y optimización en la protección de datos expuestos en la red universitaria.

### 2.3.3 Operacionalización de Variables

Se define las dimensiones e indicadores de la variable independiente y la dependiente seguido de las técnicas a emplear para la recolección de datos.

| HIPÓTESIS | VARIABLES | DEFINICIÓN | DIMENSIONES | INDICADORES | INSTRUMENTOS |
|---|---|---|---|---|---|
| La implementación de una auditoría de seguridad a la plataforma informática (WEB) del Centro de Educación Superior, permitirá identificar las amenazas y optimizar la protección de datos expuestos en la red universitaria. | **Variable Independiente** Auditoría de seguridad a la información en las aplicaciones Web | Aplicar auditoría de seguridad contribuirá en el mejoramiento de la protección de los datos | Aplicaciones Web | ✓ Herramientas de intrusión.<br>✓ Nivel de seguridad de datos | ✓ Observación<br>✓ Entrevistas<br>✓ Encuestas<br>✓ Software |
| | **Variable Dependiente** Identificación de amenazas y optimización en la protección de datos expuestos en la red Universitaria. | Optimizará riesgos donde se comprometa la información privada de los usuarios del Centro de Educación Superior | Seguridad de la información | ✓ Vulnerabilidades encontradas.<br>✓ Estrategias de seguridad | ✓ Observación<br>✓ Entrevistas<br>✓ Encuestas |

**Tabla 1 Matriz Operacionalización de variable.**

**Fuente:** http://es.slideshare.net/melissasanchezromero5/operaconalizacin-de-variables

## 2.4 Métodos e instrumentos de investigación

Existen variedad de métodos para recopilar datos, cada uno tiene ventajas y desventajas por eso es necesario utilizar dos o más para complementar el trabajo.

Para el proceso de recolección de datos e investigación del presente proyecto surge la necesidad de usar métodos e instrumentos de investigación:

**Método Analítico – Sintético**: Se utilizó un estudio de aceptación que contribuye en el desarrollo de una auditoría en seguridad a la información en la comunidad universitaria. El método Analítico se refiere al análisis del objeto, descomponerlo o estudiarlo minuciosamente, aplicando la síntesis sobre los resultados obtenidos previamente del análisis.

**Método Inductivo-Deductivo**: A partir de la observación de casos particulares sobre los peligros que están expuestos los datos en la Web se plantea el problema de requerir una auditoría en seguridades.

A través de un proceso de inducción, este problema se remite a la inseguridad de los datos. A partir del planteamiento del problema se formula una hipótesis mediante un razonamiento Deductivo, que posteriormente se intentará validar.

**Método de Investigación de Campo:** El presente trabajo está inmerso en un estudio de campo de carácter evaluativo, ya que los datos estarán tomados acorde a la realidad.

| ETAPA DE INVESTIGACIÓN | MÉTODOS DE INVESTIGACIÓN | TÉCNICAS E INSTRUMENTOS | RESULTADO |
|---|---|---|---|
| **Fundamentación Teórica** | Analítico-Sintético Inductivo-Deductivo | Revisión Bibliográfica y por Internet | Bases teóricas de la investigación |
| **Diagnóstico** | Recolección de Información | Observaciones Entrevistas Encuestas | Diagnóstico del estado actual del problema |
| **Propuesta** | Método Investigación de campo | Analizar Resultados | Propuesta |

**Tabla 2 Etapas de la Investigación.**

**Fuente:** http://www.gestiopolis.com/economia/metodos-y-tecnicas-de-investigacion.htm

## Técnicas e instrumentos de investigación

A partir de los instrumentos de observación, entrevistas y encuestas a la comunidad se obtiene la recolección de datos primarios para la investigación.

La ***Entrevista,*** es una técnica que ayuda a conocer más el ambiente o campo de investigación, la misma sirve para la comprobación a la factibilidad del proyecto. “La entrevista, es la comunicación interpersonal establecida entre el investigador y el sujeto de estudio a fin de obtener respuestas verbales a los interrogantes planteados sobre el problema propuesto. Se considera que este método es más eficaz que el cuestionario, ya que permite obtener una información más completa”

(Manuel Galán Amador, 2009). Mediante la entrevista se obtendrá información sobre lo que se auditará.

Las ***Encuestas*** en este trabajo de investigación serán realizadas a los Docentes y Personal Administrativo, quienes son los que frecuentemente utilizan las aplicaciones Web del centro de educación superior y proveen a las diferentes bases de datos de información sensible, que deben ser tratadas con mucha seguridad.

Con la realización de la encuesta se obtendrá información útil. “La encuesta es una técnica de recogida de datos mediante la aplicación de un cuestionario a una muestra de individuos” (Centro de Investigaciones Sociológicas, 2013).

La ***Observación*** es una técnica de investigación primordial y de utilidad en el presente trabajo el cual: “Consiste en observar atentamente el fenómeno, hecho o caso, tomar información y registrarla para su posterior análisis” (Puente, 2013).

La ***Población*** “Es el conjunto total de individuos, objetos o medidas que poseen algunas características comunes observables en un lugar y en un momento determinado” (Wigodski, 2010).

La ***Muestra*** “Es un subconjunto fielmente representativo de la población”

(Wigodski, 2010). Se determinó la utilización de un muestreo probabilístico estratificado el cual nos ayuda a resaltar un subgrupo específico dentro de la población.

## 2.5 Términos Básicos

Es necesario definir algunos términos básicos que serán de uso frecuente en los siguientes capítulos.

**Ataque Informático**

Acción que realiza un individuo mediante una herramienta informática con el objetivo de aprovechar una falla o vulnerabilidad de un sistema informático intentando tomar el control, dañarlo y desestabilizarlo.

**Firewall**

Un cortafuegos, puede ser Software o Hardware configurados para bloquear accesos no autorizados a la red, permitiendo solo comunicaciones autorizadas. (Caballar Falcon, 2006)

**Vulnerabilidades**

Son fallos, errores o debilidades en un sistema informático que puede ser explotado por un ataque, comprometiendo la seguridad de los sistemas informáticos.

**Riesgos**

Un riesgo se define como la probabilidad de que ocurra una amenaza y se convierta en un desastre. Es importante conocer y gestionar los riesgos permitiendo la toma de decisiones con el fin de mejorar la protección a los sistemas.

**Pentest**

Test de Penetración, es la forma de denominar a un conjunto de técnicas utilizadas para analizar y evaluar la seguridad de los sistemas, redes, y aplicaciones involucradas en los mismos.

**Escaneo de puertos**

Una de las técnicas que un atacante recurre principalmente para descubrir un punto de entrada al servidor es un escáner de puertos, el mismo que consiste en buscar puertos abiertos (servicios en ejecución dentro del servidor) y fijarse en los que puedan ser receptivos o de utilidad. (ACISSI, 2013)

**Explotación de errores**

Suceden en el momento que se encuentran agujeros, debilidades o vulnerabilidades de seguridad en los sistemas operativos, protocolos de red o aplicaciones.

**WAF (Web Application Firewall)**

Firewall de aplicación Web, es un elemento sea Software o Hardware el cual analiza, y a la vez filtra el tráfico de datos entre un cliente y un servidor Web.

WAF, trabaja en la capa de aplicación dentro del modelo TCP/IP. Se utiliza para defender y detectar Inyección SQL, Local File Inclusion (LFI) o Cross Site Scripting (XSS)

**Bypass**

“Básicamente una inyección de código significa hacer consultas malformadas a la base de datos, la cual, si no está bien estructurada para identificarlas, validarlas y/o bloquearlas, nos va a arrojar información sensible” (0xdeadlock.org, 2014).

**Live HTTP Header**

Es un complemento del navegador Firefox, el cual permite observar la información que contiene la cabecera HTTP que son enviadas al servidor Web o las que recibimos como respuesta del servidor.

# CAPÍTULO 3

# ANÁLISIS

## 3 ANÁLISIS

En este segmento contiene diagramas el diagrama de procesos, identificación de requerimientos. Además en este capítulo se observa el análisis del proyecto en conjunto con la interpretación de resultados de las encuestas y entrevistas desarrolladas, con la finalidad de conocer la factibilidad para la implementación de una auditoría

### 3.1 Diagrama de procesos

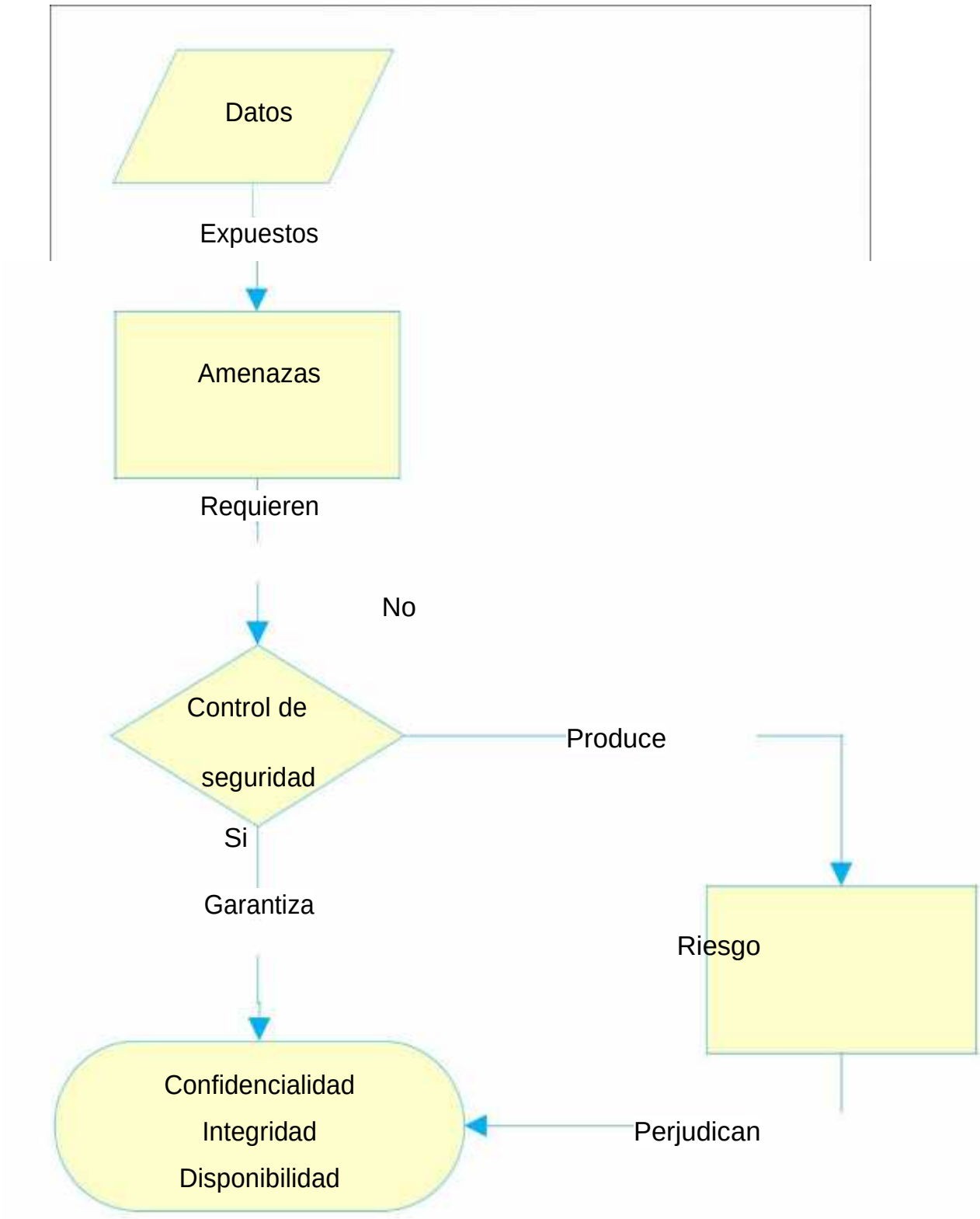


**Figura 8 Diagrama de seguridad a la información**

**Autor:** Bonilla Tumbaco Brenda

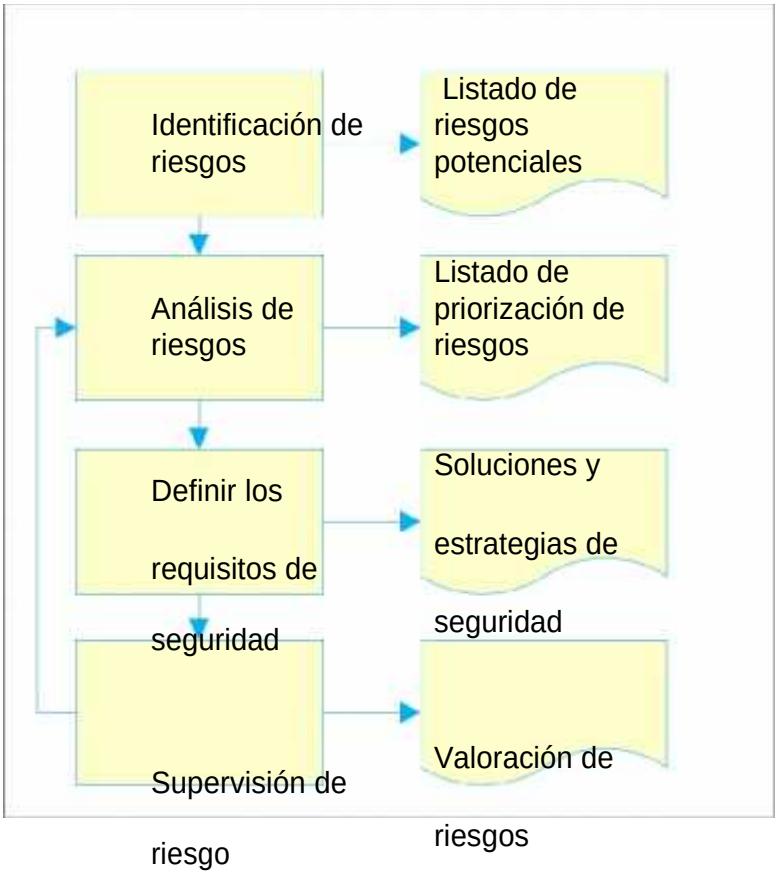


**Figura 9 Diagrama de proceso de Auditoría**

**Autor:** Bonilla Tumbaco Brenda

### 3.1.1 Descripción funcional de los procesos

La información y datos confidenciales están expuestos a diferentes amenazas como: hurto, pérdida, o su mal uso, por este motivo se debe controlar y garantizar la seguridad de la información almacenada en los servidores de bases de datos, mitigando los posibles riesgos que se presenten en las aplicaciones web, con la finalidad de proteger la confidencialidad, integridad y disponibilidad de los datos.

## 3.2 Identificación de requerimientos

- ✓ La Auditoría de Seguridad se realizará en la IP: XXX.XXX.XXX.XXX según el compromiso y autorización proporcionada por el Jefe del Departamento de Unidad de Producción
- ✓ La Auditoría a desarrollar debe estar fundamentada bajo una metodología de testeo de seguridad con licencia abierta estandarizada.
- ✓ La guía que se utilizará para ejecutar el test de intrusión y verificar los puntos débiles de las aplicaciones, será la metodología del Proyecto OWASP, quien brinda en su TOP 10, las vulnerabilidades más importantes.
- ✓ Las debilidades o vulnerabilidades halladas no serán explotadas con el fin de evitar anomalías en los sistemas informáticos, resaltando que el objetivo de una auditoria es encontrar posibles riesgos y mitigarlos.
- ✓ Informe de resultado final de la Auditoría de Seguridad a la Información que maneja la plataforma WEB con sus posibles soluciones.

## 3.3 Análisis del Proyecto

Con la obtención de los requerimientos establecidos para el desarrollo de la Auditoría de Seguridad a la Información se procede realizar un estudio de factibilidad técnico, económico y operacional del proyecto.

### 3.3.1 Análisis Técnico

Es importante señalar los recursos humanos, tecnológicos y de oficina que se requieren para el desarrollo de la Auditoría de Seguridad a los datos.

| Cantidad | Materiales de Oficina |
|---|---|
| 4 | Resma de papel |
| 2 | Cartuchos de tintas |
| 6 | Anillados |
| 2 | Empastados |

**Tabla 3 Recursos de Oficina.**

**Autor:** Bonilla Tumbaco Brenda

| Cantidad | Personal |
|---|---|
| 1 | Auditor de Seguridad |

**Tabla 4 Recurso Humano.**

**Autor:** Bonilla Tumbaco Brenda

| Cantidad | Software |
|---|---|
| 1 | S.O. Linux, Distro Kali |
| 1 | Navegador Web |
| 1 | Office 2010 |

**Tabla 5 Recursos de Software.**

**Autor:** Bonilla Tumbaco Brenda

| Cantidad | Hardware |
|---|---|
| 1 | Computadora |
| 1 | Impresora |

**Tabla 6 Recursos de Hardware.**

Autor: Bonilla Tumbaco Brenda

| Mes | Servicios |
|---|---|
| 1 | Internet |

**Tabla 7 Otros Servicios.**

Autor: Bonilla Tumbaco Brenda

### 3.3.2 Análisis Económico

Después del análisis técnico donde se establecieron los recursos indispensables para la realización de este proyecto a continuación se detalla los costos de recurso humano, de oficina y tecnológico.

| Cantidad | Materiales de Oficina | Costo |
|---|---|---|
| 4 | Resma de papel | $ 15.75 |
| 2 | Cartuchos de tintas | $ 80.00 |
| 6 | Anillados | $ 6.00 |
| 2 | Empastado | $ 14.00 |
| | **TOTAL** | **$105.75** |

**Tabla 8 Costo Recurso de Oficina.**

**Autor:** Bonilla Tumbaco Brenda

| Cantidad | Personal | Costo |
|---|---|---|
| 1 | Auditor de Seguridad | $ 3000.00 |
| **Total** | | **$ 3000.00** |

**Tabla 9 Costo de Recurso Humano.**

**Autor:** Bonilla Tumbaco Brenda

| Cantidad | Software | Costo |
|---|---|---|
| 1 | S.O. Linux, Distro Kali | $ 0.00 |
| 1 | Navegador Web | $ 0.00 |
| **Total** | | **$** 0.00 |

**Tabla 10 Costo de Software.**

**Autor:** Bonilla Tumbaco Brenda

| Cantidad | Hardware | Costo |
|---|---|---|
| 1 | Computadora | $ 1,100.00 |
| 1 | Impresora Canon | $ 120 |
| **Total** | | **$ 1,220.00** |

**Tabla 11 Costo de Hardware.**

**Autor:** Bonilla Tumbaco Brenda

| Mes | Servicios | Costo |
|---|---|---|
| 1 | Internet | $ 27.00 |

**Tabla 12 Costo de Servicios.**

**Autor:** Bonilla Tumbaco Brenda

| Descripción | Costo |
|---|---|
| Hardware | $1,220.00 |
| Software | $ 0.00 |
| Personal | $ 3000.00 |
| Materiales de oficina | $ 105.75 |
| Internet | $ 27.00 |
| **Costo del proyecto** | **$ 4352.75** |

**Tabla 13 Costo Total del Proyecto**.

**Autor:** Bonilla Tumbaco Brenda

El costo de la Auditoría de seguridad a la información tiene un costo total de $4,352.75.

### 3.3.3 Análisis Operativo

Es de suma importancia garantizar la factibilidad de la Auditoría de Seguridad a ejecutar, para esto la persona que efectuará este proyecto cuenta con la experiencia y capacidad necesaria para llevarla a cabo. La auditoría se realizará dentro de las normas legales, es decir, realizada con autorización, ética y sin explotar las debilidades.

El auditor cuenta con un perfil y ética profesional, utiliza estándares de referencia en el área de testeo como las metodologías OSSTMM y conocimiento de las más importantes vulnerabilidades, las cuales son listadas y brindadas en el Top 10 del Proyecto OWASP, logrando ser las más imprescindibles en la concentración de medidas correctivas para los sistemas informáticos.

La acogida para la realización de la Auditoría de Seguridad a la Información fue favorable por parte del Departamento de Unidad de Producción; se estableció su importancia con el fin de tener un mayor control de seguridad a la información durante el desarrollo de las aplicaciones por lo que existe falta de desconocimiento total de los ataques más comunes por parte de los desarrolladores, por lo cual podrán crear un estándar protocolario para la seguridad y vulnerabilidades de cada una de las aplicaciones desarrolladas puesta en producción por parte del centro de educación superior que controlen, manipulen y manejen datos sensibles o privados.

El objetivo de una auditoría consiste en analizar el sistema de control de seguridad e informar a los responsables las debilidades y vulnerabilidades encontradas, al mismo tiempo proponer soluciones seguras para mitigar el riesgo en estos fallos.

### 3.4 Técnicas e instrumentos de recolección de datos.

#### 3.4.1 Población y Muestra.

**Población**

La población para el presente estudio de investigación se concentrará en los usuarios que hacen uso de las aplicaciones encontradas en la WEB.

| INFORMANTES | CANTIDAD |
|---|---|
| Docentes y personal administrativo | 376 |
| **Total Población** | **376** |

**Tabla 14 Población.**

**Autor:** Bonilla Tumbaco Brenda

**Muestra**

Para obtener la muestra utilizaremos la técnica de muestreo estratificado que permite dividir la población en subgrupos con sujetos más representativos para obtener información más relevante. Para establecer el tamaño de la muestra se aplicará la siguiente fórmula de muestreo:

Dónde**:**

| SÍMBOLO | NOMBRE |
|---|---|
| **N** | Tamaño de la muestra |
| **z** | Nivel de Confianza |
| E | Margen de error |
| p | Probabilidad de éxito |
| q | Probabilidad de fracaso |

**Tabla 15 Variables. Fórmula de muestreo.**

**Autor:** Bonilla Tumbaco Brenda

N= 376

z= 95% (1.96)

p= 0.50

q= 0.50

E= 5%

El tamaño ideal de la muestra es de **191** Personas entre Docentes y Personal Administrativo.

### 3.4.2 Análisis e Interpretación de la Encuesta

Encuesta dirigida a los usuarios que utilizan las aplicaciones de la WEB.

**Pregunta # 1: ¿Tiene conocimiento de la existencia de hurto de Información en aplicaciones Web?**

| Descripción | Frecuencia |
|---|---|
| **Si** | 160 |
| **No** | 31 |
| **Total general** | **191** |

**Tabla 16 Conocimiento de la existencia de hurto de Información.**

**Autor:** Bonilla Tumbaco Brenda

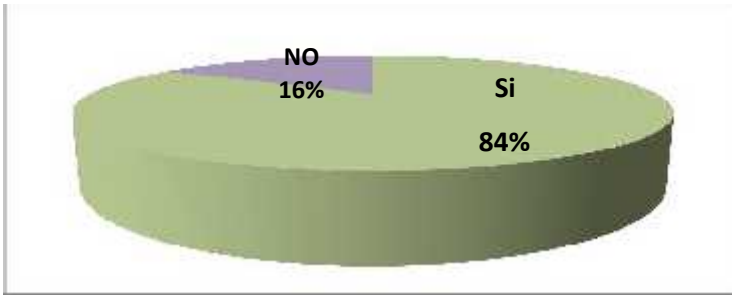


**Figura 10 Conocimiento de la existencia de hurto de Información.**

**Autor:** Bonilla Tumbaco Brenda

**Análisis:** Los datos estadísticos demuestran que gran parte de usuarios tienen conocimiento de la existencia de hurto de información en aplicaciones Web; están conscientes que todo sistema informático se encuentra expuesto a esta amenaza, por lo tanto es considerable realizar un análisis profundo sobre el real conocimiento que tienen los usuarios con respecto a este tema, siendo muy importante para la seguridad de sus Datos.

**Pregunta # 2: Los ordenadores de su trabajo, ¿Tienen instalado antivirus?**

| Descripción | Frecuencia |
|---|---|
| **Si** | 185 |
| **No** | 6 |
| **Total general** | **191** |

**Tabla 17 Ordenadores de trabajo con antivirus**.

**Autor:** Bonilla Tumbaco Brenda

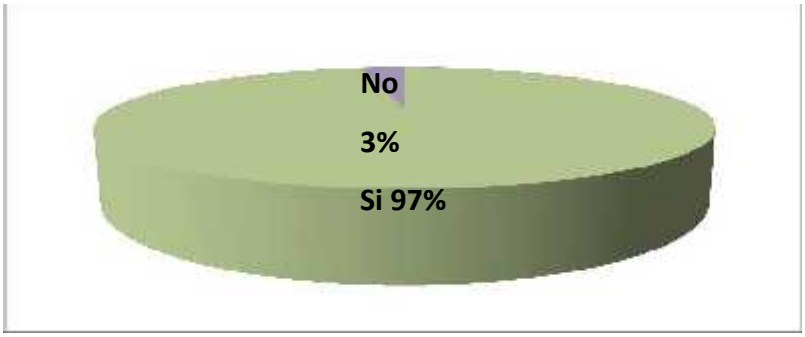


**Figura 11 Ordenadores de trabajo con antivirus.**

**Autor:** Bonilla Tumbaco Brenda

**Análisis:** En su mayoría, los usuarios utilizan antivirus en los ordenadores de trabajo como un programa de protección básico en sus ordenadores, considerándolo necesario para impedir que provoquen daños pudiendo ser causados por páginas maliciosas o elementos externos infectados por troyanos, spyware y otros virus; para proteger de alguna forma la información que es lo más valioso que posee el usuario en su ordenador.

Si la pregunta número 2 es afirmativa, se procede a responder la pregunta 3.

**Pregunta # 3: ¿El antivirus que utiliza su ordenador de trabajo se encuentra con licencia?**

| Descripción | Frecuencia |
|---|---|
| **Si** | 124 |
| **No** | 67 |
| **Total general** | **191** |

**Figura 12 Antivirus con Licencia.**

**Autor:** Bonilla Tumbaco Brenda

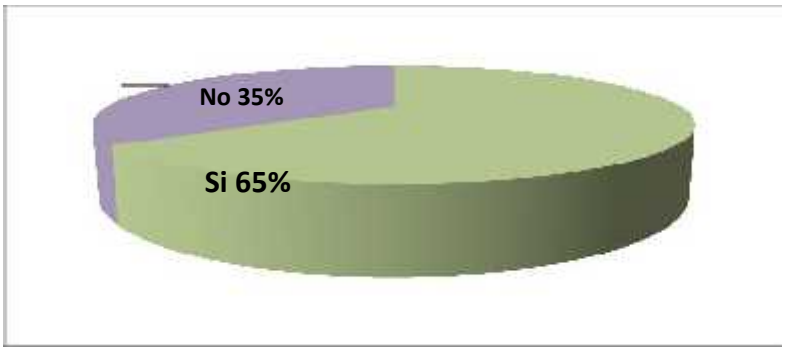


**Figura 13 Antivirus con licencia**

**Autor:** Bonilla Tumbaco Brenda

**Análisis**: Existe un gran porcentaje de usuarios que tienen instalados antivirus con licencia en sus ordenadores de trabajo; es recomendable que se utilice una versión original, de esta forma se habilitarán las herramientas con las que dispone el programa para la protección eficiente de la información en los ordenadores. Una de las herramientas importantes del antivirus es la actualización automática de la base de datos de virus ya que cada día se generan nuevas amenazas.

**Pregunta # 4: ¿Con que frecuencia usted cambia las contraseñas que utiliza en las aplicaciones de la WEB?**

| Descripción | Frecuencia |
|---|---|
| **Cada semana** | 6 |
| **Cada mes** | 12 |
| **Cada semestre** | 56 |
| **Nunca** | 117 |
| Total general | **191** |

**Tabla 18 Frecuencia cambio de contraseñas en aplicaciones.**

**Autor:** Bonilla Tumbaco Brenda

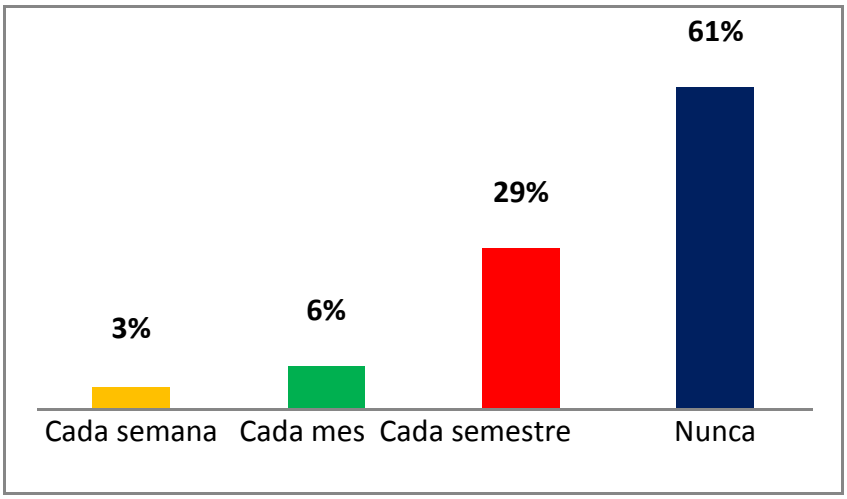


**Figura 14 Frecuencia cambio de contraseñas en aplicaciones.**

**Autor:** Bonilla Tumbaco Brenda

**Análisis:** La mayoría de los usuarios no tiene como hábito cambiar con frecuencia las contraseñas asignadas por los administradores de sistemas para acceder a las aplicaciones Web del centro de educación superior, debido a estos resultados obtenidos se deben tomar medidas para incentivar y a su vez orientar al usuario al cambio frecuente de claves para evitar el ingreso predictivo al sistema por terceras personas.

**Pregunta # 5: ¿Conoce usted las políticas de seguridad que debe tomar en cuenta al utilizar las aplicaciones de la WEB del centro de educación superior?**

| Descripción | Frecuencia |
|---|---|
| **Si** | 34 |
| **No** | 156 |
| Total general | **191** |

**Tabla 19 Conocimiento de las políticas de seguridad.**

**Autor:** Bonilla Tumbaco Brenda

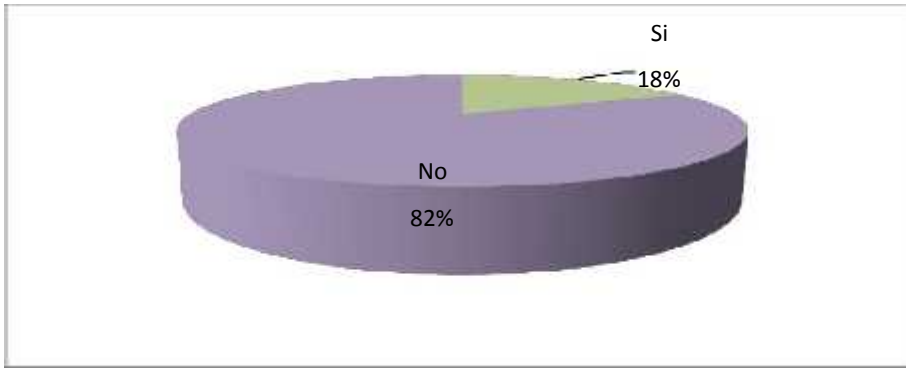


**Figura 15 Conocimiento de las políticas de seguridad.**

**Autor:** Bonilla Tumbaco Brenda

**Análisis:** Estos datos reflejan que el personal desconoce las políticas de seguridad correspondientes al uso de las aplicaciones de la WEB. Esto puede suceder cuando se brinda instrucciones de seguridad y no se llega a cumplir con el objetivo establecido al inicio de la capacitación, otra razón puede ser la falta de organización del departamento para dar a conocer las políticas de seguridad.

**Pregunta # 6. ¿Cómo califica la calidad del servicio de las aplicaciones que se encuentran en la WEB del centro de educación superior?**

| Descripción | Frecuencia |
|---|---|
| **Excelente** | 6 |
| **Muy buena** | 74 |
| **Buena** | 79 |
| **Mala** | 25 |
| **Pésima** | 7 |
| Total general | **191** |

**Tabla 20 Calidad de servicio de las aplicaciones**

**Autor:** Bonilla Tumbaco Brenda

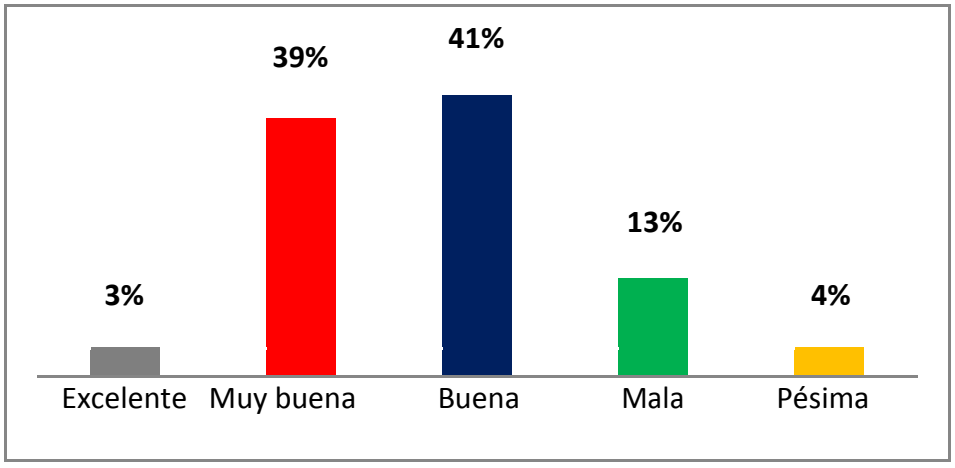


**Figura 16 Calidad de servicio de las aplicaciones**

**Autor:** Bonilla Tumbaco Brenda

**Análisis**: Los porcentajes que muestra el cuadro nos da una clara referencia, que las aplicaciones de la WEB no satisface en su totalidad las necesidades requeridas por el personal del centro de educación superior. El personal resaltó la existencia de inconvenientes con la plataforma WEB al no tener una disponibilidad constante de sus aplicaciones web.

**Pregunta # 7: ¿Qué aplicaciones de la WEB utiliza con más frecuencia?**

| Descripción | Frecuencia |
|---|---|
| **Registro de Calificaciones** | 148 |
| **Intranet** | 43 |
| Total general | **191** |

**Tabla 21 Aplicaciones utiliza con más frecuencia**

**Autor:** Bonilla Tumbaco Brenda


**Figura 17 Aplicaciones que utiliza con más frecuencia**

**Autor:** Bonilla Tumbaco Brenda

**Análisis**: Al indagar sobre que aplicaciones se utilizan con más frecuencia, los usuarios indicaron: El ingreso de calificaciones por parte de los docentes y el uso de la Intranet por parte del personal administrativo. Con estos resultados se considera necesario auditar la seguridad de datos manejados por dichas aplicaciones y hacer una inducción de las bondades de otros utilitarios de la WEB del centro de educación superior.

**Pregunta # 8: ¿Ha sufrido pérdida o cambios de información en las aplicaciones que confiere la WEB del centro de educación superior?**

| Descripción | Frecuencia |
|---|---|
| **Si** | 13 |
| **No** | 178 |
| Total general | **191** |

**Tabla 22 Pérdida o cambios de información.**

**Autor:** Bonilla Tumbaco Brenda

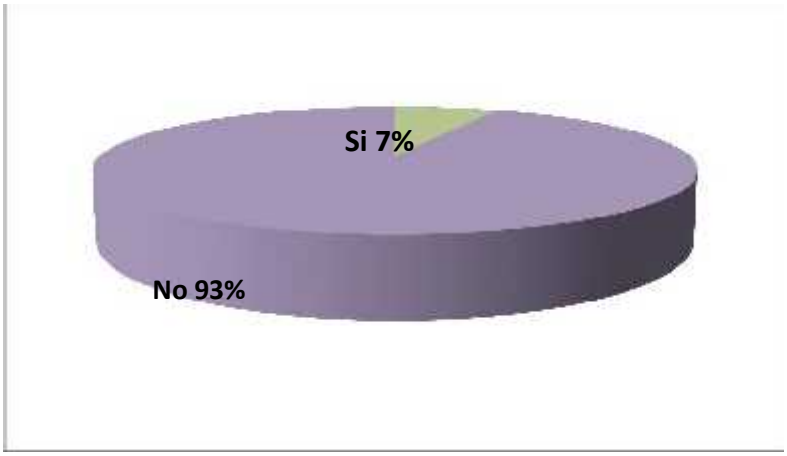


**Figura 18 Pérdida o cambios de información.**

**Autor:** Bonilla Tumbaco Brenda

**Análisis:** Los usuarios no han sufrido perjuicios con los datos que se almacenan en los servidores del centro de educación superior, sin embargo existe la posibilidad que se pueda presentar el riesgo de pérdida, alteración o hurto de datos privados, debido a que constantemente aparecen nuevos métodos o herramientas para la manipulación y obtención de información desde los servidores de datos.

**Pregunta # 9: ¿Considera necesario que se efectúe una Auditoría de Seguridad al manejo de la información en las aplicaciones de la WEB del centro de educación superior?**

| Descripción | Frecuencia |
|---|---|
| **Si** | 191 |
| **No** | 0 |
| Total general | **191** |

**Tabla 23 Consideración que se efectúe una Auditoría.**

**Autor:** Bonilla Tumbaco Brenda

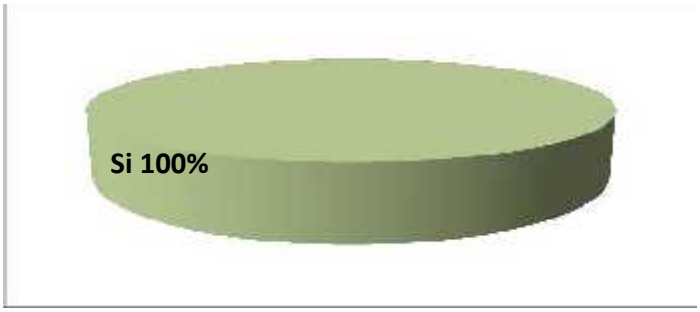


**Figura 19 Consideración que se efectúe una Auditoría**.

**Autor:** Bonilla Tumbaco Brenda

**Análisis:** El personal encuestado en su totalidad consideró la importancia de realizar una auditoría de seguridad a las aplicaciones de la WEB, para tener mayor confianza en la plataforma web, se considera que el análisis realizado mediante una auditoría, ayuda en la detección de la posible existencia de vulnerabilidades en los sistemas informáticos, de esta forma se conseguiría un óptimo control de seguridad a la información manejada por las aplicaciones.

### 3.4.3 Análisis de la Encuesta

El objetivo principal de la encuesta es “Determinar el nivel de conocimiento sobre seguridad informática por parte de los usuarios que utilizan aplicaciones Web”.

Se analizaron cada una de las preguntas que incluían en la encuesta, posteriormente a ello se consiguió recolectar información que ayuda a definir nuestros objetivos y alcance.

Los usuarios conocen de la existencia de delitos informáticos como el hurto de información. Sin embargo, la única forma de protegerse es manteniendo su ordenador de trabajo con un antivirus, muchos de ellos sin licencia original. El personal del centro de educación superior afirma no haber sufrido alteraciones, ni pérdidas de la información que reposa en los servidores del centro de educación superior, pero dan a conocer que existen eventualidades como no disponibilidad de las aplicaciones de la WEB.

Existe déficit de organización en los administrativos de la Unidad de Producción al momento de dar a conocer las políticas de seguridad para el uso de las aplicaciones web a los usuarios finales. Las aplicaciones de la WEB con mayor uso y relevancia es la Intranet junto con el sistema de ingreso de calificaciones, cabe indicar que los datos manejados por dichas aplicaciones son privados. La mayoría de los usuarios no realizan cambios de contraseña con frecuencia, esto implica que en algún momento un individuo puede haber adquirido una contraseña antigua válida provocando el riesgo de suplantación.

Los usuarios consideran necesario que se realice una auditoría de seguridad a la información para que el centro de Educación Superior pueda garantizar la integridad y protección a los datos privados.

### 3.4.4 Análisis de la Entrevista

La entrevista fue realizada al encargado del cuarto de servidores de base de datos

*El propósito de la entrevista al Administrador de Servidores es: "Determinar el nivel de seguridad informática en su entorno".*

**1. ¿Sus sistemas de información utilizan algún tipo de firewall?**

Si, Distribución personalizada de FreeBSD pfSense

**Análisis:** Cuentan con un Firewall llamado pfSense, distribución de FreeBSD con licencia libre. Este es un firewall de código abierto usado en servicios de redes LAN y WAN muy robusto permite filtrado avanzado de paquetes por protocolos y puertos, también ofrece el servicio de filtrado en la capa 7 (aplicación).

**2. ¿Poseen respaldos de sus sistemas ante sensibles pérdidas de información?**

Si, como prevención ante cualquier amenaza

**Análisis:** El departamento de servidores conserva respaldos de sus sistemas ante pérdidas de datos o daños en la información. Es importante salvaguardar la información por cualquier eventualidad de amenazas que perjudiquen el estado de los sistemas informáticos.

**3. ¿Cuentan con algún plan o están preparados frente a un ataque a los sistemas?**

SI [X] NO [ ]

**Análisis:** El departamento de Unidad de Producción cuenta con políticas de seguridad y plan de contingencia. Es necesario mantener actualizados los manuales de políticas y planes de contingencia, así mismo dar a conocer a todo el personal del departamento informático estos lineamientos para que estén preparados ante cualquier calamidad.

**4. El análisis de seguridad de sus sistemas y servidores de base de datos, ¿Quién lo realiza?**

Personal interno [X] Personal externo [ ]

**Análisis:** Existe una persona encargada de la seguridad interna de las aplicaciones y datos alojados en los servidores. Es indispensable contar con un personal de seguridad interna, con la ventaja de mantener un constante control de los sistemas mitigando riesgos que perjudiquen a los sistemas.

**5. ¿Se capacita usted constantemente acerca de los últimos fallos de seguridad informática?**

SI x NO

**Análisis:** La persona encargada de la seguridad de los sistemas informáticos se capacita constantemente. Es primordial que el personal obtenga conocimiento actualizado, mejorando sus habilidades con el objetivo de verificar eficientemente, en su totalidad la seguridad de las aplicaciones y no ser víctima de un ataque.

**6. Sabemos que constantemente salen al mercado nuevas herramientas para detectar el nivel de seguridad y técnicas para proteger la información. ¿Actualizan constantemente los sistemas de seguridad en caso de existir una que se considere importante?**

SI x NO

**Análisis:** Con la facilidad de herramientas de control de seguridad que existen actualmente en el internet, no recurren a la utilización de herramientas que son realmente necesarias para mejorar la seguridad en los sistemas.

**7. ¿Han adquirido servicios de auditoría externa de seguridad a la información en las aplicaciones de la plataforma WEB?**

SI x NO

**Análisis:** Nunca han considerado necesario adquirir auditoria externa de seguridad, debido a esto es posible la existencia de fallos en las estructura de las aplicaciones por lo que es conveniente contratar personal experto en seguridad que no tenga relación con la institución, de tal manera proporcionarán sugerencias estandarizadas, analizando la eficiencia de los sistemas informáticos de forma general y buscando puertas de accesos en las aplicaciones con técnicas de hacking ético.

# CAPÍTULO 4

# DISEÑO

## 4 Diseño

En este capítulo se describen las características principales de la Auditoría de Seguridad que se realizará en la plataforma WEB, la técnica de hacking ético para su ejecución, continuando con la descripción del contenido de cada una las fases en la que se encuentra dividida la auditoría.

## 4.1 Características de la Auditoría

La auditoría se delimita en aplicar un test de seguridad externo desde un ambiente no autorizado en la plataforma informática WEB del centro de educación superior, las cuales son las más utilizadas por la comunidad universitaria.

Se buscarán debilidades y vulnerabilidades que estén expuestas a correr el riesgo de ser explotados causando daños a las aplicaciones web del centro de educación superior; la mejor forma de probar el nivel de seguridad de los sistemas es realizando una simulación de ataques externos como lo hace un hacker, tan solo disponiendo de información pública sobre el objetivo.

- ✓ Las pruebas se llevan a cabo de forma remota, desde la oficina del auditor, fuera del centro de educación superior.

- ✓ El departamento no facilita información sobre la estructura de las aplicaciones. El auditor debe obtener esta información mediante la metodología caja negra, es decir simulando un ataque real realizado por un hacker.

- ✓ Las técnicas a utilizar son las mismas que las de un hacker de sombrero negro pero de forma ética.

- ✓ Utilización de las metodologías Open Source OSSTMM y la Guía de Pruebas OWASP


**Figura 20 Auditoría de Seguridad a Implementar**

**Autor:** Bonilla Tumbaco Brenda

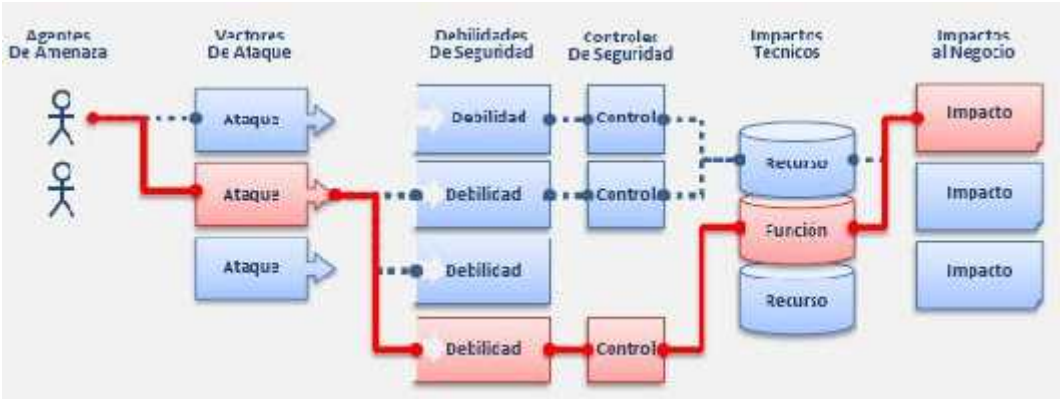


**Figura 21 Riesgo de Seguridad en Aplicaciones**

**Fuente:** https://www.owasp.org/

La técnica de caja negra que se utilizará en el desarrollo de la auditoría de seguridad se refleja en la Figura 3.13. El auditor es representado como un agente de amenaza buscando diferentes rutas (debilidades) a través de la aplicación, cada ruta representa un riesgo que puede ser o no serio, es decir, fácil o a veces extremadamente difíciles de explotar.

## 4.2 Fases del test

Para la realización del test de penetración el auditor describe a continuación las 4 fases:


**Figura 22Fases de Pentesting**

**Fuente:** https://www.owasp.org/

### 4.2.1 Fase de reconocimiento

En esta etapa el auditor busca y recopila información aplicando ingeniería social o por footprinting - fingerprinting. La información que se necesita recaudar son nombres, correos electrónicos, direcciones IPs, credenciales, entre otras que servirán para el desarrollo de las siguientes fases.

**Ingeniería Social**

Es una técnica aplicada para adquirir información confidencial con habilidades sociales y psicológicas, características propias del auditor para la obtención de información.

Por medio de una entrevista informal al Jefe del departamento de servidores, nos facilitó credenciales, pero la información que obtuvimos es que los estudiantes universitarios dan uso a la WEB para consultar sus calificaciones y son pocos quienes hacen el cambio de contraseña que le asigna el departamento de sistemas.

Las credenciales que se le asignan por parte del departamento de producción a los estudiantes sirven para realizar consultas de sus calificaciones. Comúnmente se establece, usuario: número de cédula y contraseña: número de matrícula.

**Footprinting – Fingerprinting**

Se encarga de buscar toda la información pública del centro de educación superior tales como: cuentas de correos, direcciones IP, registro del dominio, entre otros datos que sean de utilidad para realizar ataques en las siguientes etapas de la auditoría.

- ✓ **Reconocimiento mediante motores de búsqueda:** Se utilizan los buscadores de Internet, como: Yahoo, Bing, Google o cualquier otro. Es necesario conocer las características avanzadas de búsquedas de cada uno de ellos. Utilizando Google Hacking tenemos las principales características: **intitle, site, allinurl**. Referencia. OWASP-IG-002[1].

- ✓ **Identificación de puntos de entrada de las aplicaciones:** El auditor pretende entender la lógica o estructura de la aplicación, hallando puntos de accesos como formularios de autenticación. Referencia, OWASP-IG-003[2].

- ✓ **Descubrimiento de Aplicaciones:** Se requiere visitar el sitio Web del centro de educación superior y examinar cada una de las páginas para recolectar la mayor información posible, a la vez encontrar enlaces de aplicaciones en el sitio. Referencia, OWASP-IG-005**3**

- ✓ **Análisis de códigos de error:** En la IP: XXX.XXX.XXX.XXX donde se encuentran las aplicaciones del centro de educación superior, se detecta códigos de error al visitar un directorio no disponible, revelando información técnica no destinada a la vista de un usuario final. OWASP-IG-0064. Con el uso de herramientas propias de la Distribución Kali Linux, ayudará a obtener datos técnicos.

- ✓ **Información del dominio:** En el terminal de Kali, utilizando el comando WHOIS mostrará información del propietario del dominio.

- ✓ **Lista de correos electrónicos:** Otro punto interesante es listar los subdominios que dependan del dominio principal con sus direcciones IP asignadas, esta información de obtendrá mediante la herramienta FIERCE de Kali Linux.

### 4.2.2 Fase - Búsqueda de vulnerabilidades

Con la información obtenida en la fase anterior, se buscan posibles direcciones de ataque. Esta etapa consta en la búsqueda de vulnerabilidades haciendo uso de varios escáneres, a su vez la lógica aplicada por el auditor según su experiencia y conocimientos.

- ✓ **Análisis de código HTML del sitio Web:** En la WEB se analiza el código HTML para encontrar posibles vulnerabilidades.

- ✓ **Estructura del sitio Web:** La herramienta DirBusterReport, permite descubrir la estructura de un sitio Web mostrando sus directorios ocultos, el objetivo de este escaneo es encontrar posibles fallas tales como encontrar un archivo que contenga contraseñas o datos sensibles que permitan realizar algún ataque.

- ✓ **Escáner de Puertos:** La herramienta NMAP[5], que nos facilita Kali Linux sirve para realizar escaneos de puertos, se verificarán que puertos están actualmente abiertos. Con Nmap se pueden detectar fallos e intentar obtener más datos para posteriormente realizar otros tipos de ataques.

  Los estados de los puertos pueden ser: abiertos, cerrados o filtrados; Abiertos, cuando el equipo acepta peticiones, Cerrados, no acepta peticiones y Filtrados, el puerto se encuentra protegido con Firewall y evita que Nmap verifique su estado.

- ✓ **Comprobar Firewall:** Verificación de la existencia de Firewall de Aplicaciones Web (WAF), utilizando la herramienta WAFW00F.

- ✓ **Escaneo automático de vulnerabilidades:** Existe una herramienta que nos ayuda a detectar vulnerabilidades, W3AF[6] (Web Application Attack and Audit Framework), esta herramienta analiza toda la página Web en busca de vulnerabilidades.

### 4.2.3 Fase de Evaluación de vulnerabilidades

En esta etapa el auditor enumera los datos obtenidos de usuarios, servicios de red, vulnerabilidades, entre otros. Una evaluación de vulnerabilidades significa analizar los controles de seguridad con el fin de encontrar debilidades expuestas a amenazas con el objetivo de crear vectores de ataques para su explotación en la siguiente fase.

Es necesario destacar que no todas las vulnerabilidades halladas sean verdaderas, estas pueden ser falsos positivos.

### 4.2.4 Fase de explotación

Finalmente se realiza el acceso al sistema, esto se logra a partir de la explotación de aquellas vulnerabilidades detectadas que fueron aprovechadas por el auditor para comprometer el sistema; es decir, conduciendo a la violación de la integridad, confidencialidad y disponibilidad de los datos.

## 4.3 Solución / Informe

Mediante el análisis y ejecución de la Auditoría realizada en la plataforma WEB, en conjunto con las pruebas de penetración, con los resultados obtenidos, se entregará la documentación correspondiente, adjuntando las posibles soluciones.

Se emitirá un informe detallándose las vulnerabilidades encontradas y localizadas en áreas específicas así como también informe de datos expuestos a terceros usuarios que pueden ser descargados fácilmente con la utilización de herramientas de software libre.

Este informe servirá como guía a los administradores de la organización en la toma de decisiones en un momento oportuno y les permitirá implementar correctivos que crean convenientes para evitar el hurto de información manejada por las aplicaciones Web del centro de educación superior.

También una de las finalidades del informe es incentivar al personal encargado de administrar los sistemas informáticos la debida importancia a la seguridad de sus datos, así como la cultura de utilización de software libre por la gran variedad de herramientas de pruebas para un perfecto esquema y elaboración de aplicaciones para desarrolladores y personal de mantenimiento, permitiéndole la corrección o implementación necesaria y oportuna de posibles errores en la elaboración de sistemas y así conseguir un desarrollo confiable en aplicaciones

# CAPÍTULO 5

# Implementación

## 5 Implementación

Se detalla la auditoría en cada fase con herramientas Open Source, permitiendo encontrar posibles vulnerabilidades en los controles de seguridad en las aplicaciones Web, se adjuntan evidencias para poder mostrar cómo se realiza la explotación de la información con los diversos ataques maliciosos ya antes mencionados.

## 5.1 Fase de Reconocimiento

En esta etapa se consiguió información con mayor detalle, entre estas, las credenciales de los estudiantes con la técnica de ingeniería social y por footprinting datos técnicos con la ayuda de las herramientas de Kali Linux.

### 5.1.1 Aplicando Ingeniería Social

Se aplicó la técnica de ingeniería social a los estudiantes universitarios, aprovechando que muchos de ellos brindan facilidades para obtener información de sí mismo sin percatarse, por lo tanto, mediante una encuesta efectuada se obtuvo sus respectivas credenciales con el objetivo de acceder a una de las aplicaciones y buscar más anomalías con la ejecución de la auditoría.

La encuesta con preguntas diversas incluyendo preguntas de matrícula y cédula, las cuales permiten el ingreso a las aplicaciones

| CREDENCIALES OBTENIDAS | |
|---|---|
| USUARIO | CONTRASEÑAS |
| 0921236445 | ********** |
| 0912348621 | ********** |

**Tabla 24 Tabla Credenciales de estudiantes**

**Autor:** Bonilla Tumbaco Brenda

- ✓ Con la aplicación de Ingeniería Social a los estudiantes universitarios, se obtuvieron credenciales válidas, las mismas que utilizaremos para iniciar sesión en la aplicación Consulta de Calificaciones.

Es importante recalcar que la Ingeniería Social es una técnica de mucha utilidad cuando se necesita adquirir información valiosa, con la aplicación de habilidades sociales y psicológicas por parte del auditor sin que la víctima sospeche.

Ciertas personas utilizan esta técnica, por cualquier medio de comunicación para obtener información confidencial a través de los usuarios legítimos, con el fin de tener accesos a sistemas de información, para provocar perjuicios, daños o para algún fin de su conveniencia.

### 5.1.2 Footprinting – Fingerprinting

En esta etapa se procede a la recolección de información pública del centro de educación superior ubicada en internet y en su plataforma Web.

**Visitar la plataforma Web del centro de educación superior**

Lo primero que se debe realizar, es visitar la plataforma Web a la que se va a auditar con el objetivo de localizar información que serán útiles en las siguientes etapas:

- ✓ Revisando la información corporativa incluyendo el de las autoridades del centro de educación superior se hallaron los patrones usados para las direcciones de correo electrónico. Ejemplo:

**Reconocimiento mediante motores de búsqueda**

Google hacking El buscador de Google servirá como herramienta de recolección de información con la utilización de sus características avanzadas de búsqueda.

Entre ellas tenemos:

**Intitle**: Encuentra páginas con ciertas palabras en el campo título (title). **Site:** Lista toda la información del dominio fijado.

**Inurl:** Se encarga de buscar en internet direcciones con ese URL

**Identificar las entradas**

En las aplicaciones de la WEB se detectan los formularios de autenticación donde se encuentran las entradas sabiendo que estas son una puerta importante que está relacionada con la Base de Datos.

**Análisis de códigos de error**

En la IP: XXX.XXX.XXX.XXX, mediante una consulta a un directorio o enlace de página no existente, provocara un error **404 Not Found**. Ejemplo: Colocamos cualquier palabra en la URL:

**Información del dominio**

Usando el comando **WHOIS**[7] en la terminal de Kali Linux, brinda información sobre el registro del DNS (Sistema de Nombres de dominio):

root@kali:~# **whois** universidad.edu.ec

Detalla toda la información del Dominio, incluye nombre de quien lo registró, nombre de la organización junto a la ciudad ubicada, correo electrónico y números de teléfonos.

**Listar subdominios**

Usando la herramienta **FIERCE** de Kali Linux, nos ofrece listar subdominios que dependen del dominio principal con el siguiente comando:

root@kali:~# fierce.pl -**dns** **universidad.edu.ec**

**Listar correos electrónicos**

La herramienta **THEHARVESTER** sirve para obtener subdominios y cuentas de correo electrónico mediante la siguiente línea de comandos.

root@kali:~# **theharvester** -d http://universidad.edu.ec/ -l 500 -b google

| Comandos | Función |
|---|---|
| -d | Dominio a buscar |
| -l | Numero límite de resultados |
| -b | Fuente de Datos |

**Tabla 25 Comandos de Theharvester**

**Autor:** Bonilla Tumbaco Brenda

**Información de cabeceras HTTP**

Utilizando el navegador Firefox se procede a descargar el complemento **Live HTTP Headers,** el cual sirve para ver información de los encabezados de una página Web (Cookies, Método de envió GET o POST).

## 5.2 Fase – Búsqueda de vulnerabilidades

Se detectarán las posibles fallas y vulnerabilidades para poder explotarlas en la siguiente fase. La **IP XXX.XXX.XXX.XXX,** fue asignada por parte del departamento de sistemas para realizar las respectivas pruebas, en esta IP se encuentran los enlaces a las aplicaciones.

Con los conocimientos del auditor y con el uso de herramientas se obtendrá información más técnica sobre los elementos de red.

### 5.2.1 Técnica de bypass

Identificación de las entradas a las aplicaciones, intentar ingresar datos falsos o bypass[8] para lograr obtener un fallo identificando una posible vulnerabilidad y luego ser explotada con herramientas como SQLMAP.

### 5.2.2 Análisis de código HTML

Se analiza el código HTML de la WEB para encontrar posibles vulnerabilidades.

- ✓ Analizando el código HTML del formulario Intranet del centro de educación superior (Ver Figura 5.10), se identificó un plugin llamado Uploadify, que es utilizado para subir archivos.


**Figura 5.1 Plugin Uploadify**

**Autor:** Bonilla Tumbaco Brenda

Este plugin por defecto es vulnerable a **XSS (Cross Site Scripting),** dicha vulnerabilidad fue reportada en la siguiente página Web: (http://seclists.org/fulldisclosure/2013/Sep/96).

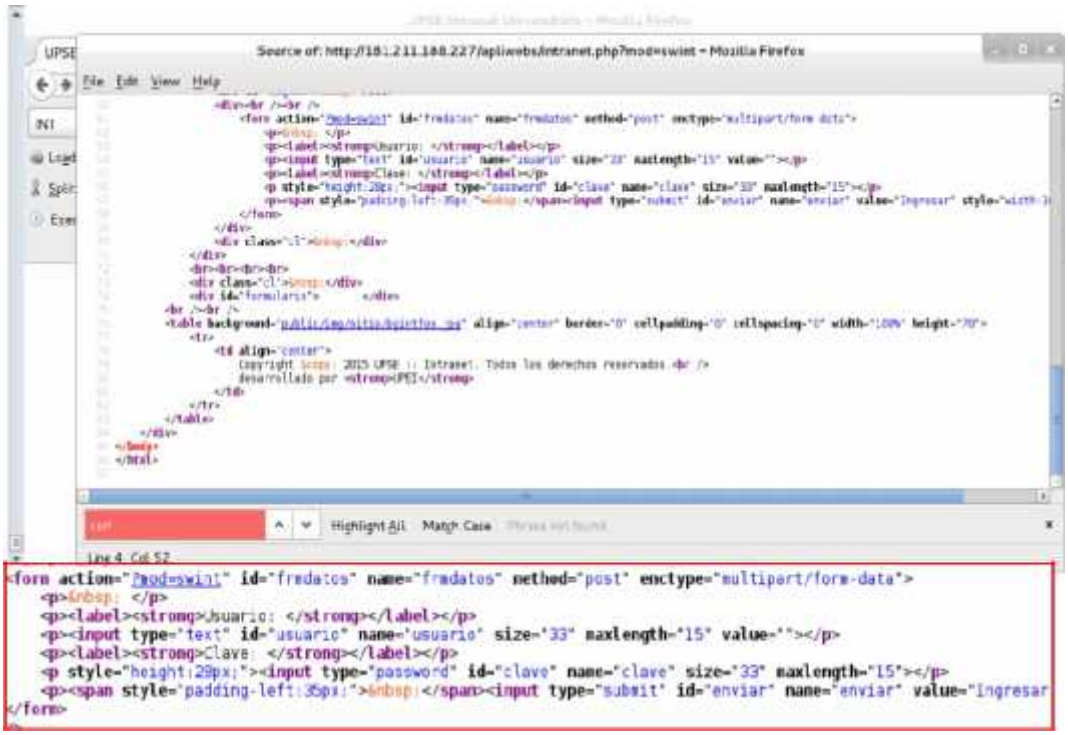


**Figura 5.2 Sin Token**

**Autor:** Bonilla Tumbaco Brenda

En la Figura 5.11 se observa que el código fuente con los input para usuario, clave e ingresar no contienen ningún código java script de Token o ANTICSRF.

Un Token es mecanismo de seguridad representado por una cadena de caracteres con un significado lógico o coherente en su mayoría suelen ser preguntas que consta de cadenas alfanuméricas utilizadas como palabras o conjunto de letras claves para identificar a un usuario que envía una petición , en este caso para validar la autenticación de ingreso a un sistema como usuario en las aplicaciones Web, teniendo como respuesta una autenticación no valida o un ingreso correcto e interacción con un servidor.

### 5.2.3 Técnica para detectar inyección SQL

En la fase de obtención de información, aplicando la técnica de Ingeniería Social se consiguió credenciales de estudiantes, estas sirvieron para autenticarnos en la aplicación consulta de calificaciones.

Dentro de la aplicación usada por los estudiantes encontramos un error con tan solo colocar en la URL un carácter especial.

***http://XXX.XXX.XXX.XXX/app/sisacaest.php?sid=13&rid=186'***

No deben surgir estos errores al colocar caracteres especiales en las URLs de las aplicaciones, son puertas de acceso hacia las bases de datos al explotar esta vulnerabilidad.

### 5.2.4 Comprobar existencia de Firewall

Con la herramienta **WAFW00F** se verifica si existe un Firewall de Aplicaciones Web (WAF).

Con la siguiente línea de comando obtendremos respuesta:

```
root@kali:~# wafw00f XXX.XXX.XXX.XXX
```

Un WAF a diferencia de un firewall común actúa en la capa de aplicación del modelo OSI, protege de los ataques maliciosos que los IDS/IPS[10] no lo hacen, como inyección SQL, denegación de servicios, spam entre otros.

### 5.2.5 Análisis de estructura del sitio Web

Con la herramienta **DirBusterReport**, creada para descubrir directorios ocultos de sitios Web, esta es de mucha utilidad para observar el árbol de directorios y encontrar posibles archivos que contengan contraseñas o datos sensibles.

- ✓ Se logró navegar en los diferentes directorios; esta lista de directorios puede revelar archivos como copias de seguridad o cualquier fichero que contenga información sensible.

### 5.2.6 Detección de puertos y servicios abiertos

Utilizaremos la herramienta **NMAP** para detectar que servicios y puertos se encuentran actualmente filtrados, abiertos o cerrados en el servidor.

| Comandos | Función |
|---|---|
| -v | Información detallada de IP |
| -Sv | Versión especifica del servicio |
| -p- | Busca todos los puertos |
| --reason | Razón , indica porque ha concluido el estado de un puerto |
| --script | Llama los script que se desea utilizar |
| -oA | O: output, A: All, crea archivos con información del escaneo |

**Tabla 26 Comandos Nmap**

**Autor:** Bonilla Tumbaco Brenda

Al ejecutar la herramienta de **Nmap** como usuario root, podemos observar en proceso de ejecución mostrando información de servicios y puertos específicos se encuentran abiertos, por medio de ellos intentar realizar un ataque dirigido.

Ejecutamos la siguiente línea de comandos para que analice la IP y arroje información sobre que puertos se encuentran abiertos.

```
root@kali:~# nmap -v -sV -p- --reason --script="not *brute* and not
*flood*" XXX.XXX.XXX.XXX -oA escaneofullpuertos
```

### 5.2.7 Detectando automáticamente vulnerabilidades

Otra herramienta de mucha utilidad es **W3Af**, es un escáner de vulnerabilidades de páginas Web. Con la misma podemos observar las diferentes vulnerabilidades halladas con el perfil de OWASP TOP 10, así detectará las más comunes e importantes amenazas.

Con la herramienta w3af se encontraron las siguientes vulnerabilidades:

- ✓ Blind SQLi (Inyección SQL)
- ✓ Click-Jacking
- ✓ Cross Site Request Forgery (CSRF)
- ✓ Cross Site Tracing (XST)
- ✓ XPATH Injection. (Encontrada en la página web http://bibliotecas.Universidad.edu.ec/pmb/opac_css/)

## 5.3 Fase evaluación de vulnerabilidades halladas.

Esta fase es muy importante porque se va a determinar qué camino seguir para realizar ataques a las vulnerabilidades encontradas. Con todos los fallos y vulnerabilidades detectadas se elige que vector tiene una mayor posibilidad de éxito para producir un ataque.

### 5.3.1 Inyecciones SQL

La inyección SQL “Ocurre cuando datos no confiables son enviados a un intérprete como parte de un comando o consulta. Los datos hostiles del atacante pueden engañar al interprete en ejecutar comandos no intencionados o acceder datos no autorizados” (Owasp.org, OWASP Top 10 - 2013, 2013).

**Blind Sqli:** Es cuando la inyección Sqli no presenta o muestra un mensaje de error al no producir resultados correctos en una consulta a la base de datos. Puede ser explotable manualmente.

**Inyección SQLi:** También de forma manual se encontró esta vulnerabilidad en la aplicación Consulta de Calificaciones del WEB utilizando los caracteres especiales en la URL exactamente en la variable rid=186**'**.

### 5.3.2 Denegación de servicios.

**"**El concepto fundamental de un ataque DoS de red es un usuario malicioso inundando con suficiente tráfico una máquina objetivo para conseguir hacerla incapaz de sostener el volumen de peticiones que recibe" (Owasp.org, 2008).

Un ataque de denegación de servicios por Slowloris tiene como objetivo mantener ocupado al servidor Web con peticiones HTTP, haciendo uso de su ancho de banda el mayor tiempo posible.

### 5.3.3 Click-Jacking

Es una vulnerabilidad de "secuestro de clic", se trata de un fallo hallado en el diseño de una página web en HTML.

Esta técnica se produce cuando un atacante utiliza múltiples capas transparentes para que el usuario dé clic en algún enlace o en un elemento y realice una acción distinta a la que desea sin el conocimiento del usuario.

### 5.3.4 Cross Site Request Forgery (CSRF)

Falsificación de Petición en Sitios Cruzados es: **"**Forma de forzar a un usuario a ejecutar acciones no deseadas en una aplicación Web en la que se encuentra actualmente autenticado" (Owasp.org, 2008).

En nuestro sitio Web existen formularios que no se encuentra con protección a la Falsificación de Petición en Sitios Cruzados (CSFR).

### 5.3.5 Cross Site Tracing (XST)

Es una vulnerabilidad común en las aplicaciones Web, generada por el método HTTP TRACE, dicho método muestra las cookies que contiene el navegador. Referencia a OWASP-CM-008[11].

Para evitar la explotación XST, se necesita deshabilitar HTTP TRACE fijando TraceEnable en Off, en el caso de las aplicaciones del centro de educación superior que utiliza un servidor Apache.

### 5.3.6 Cookies

El uso de cookies en protocolo HTTP no es seguro, un atacante puede acceder a los datos almacenados en las cookies.

### 5.3.7 XSS (Cross Site Scripting)

Secuencia de comandos en sitios cruzados, esta vulnerabilidad permite inyectar código Script en las páginas Web con el fin de robar información delicada o secuestrar sesiones que comprometen la integridad del sistema.

## 5.4 Fase de Explotación

Es la fase de penetración donde se efectiviza el ataque con la ayuda de herramientas de explotación.

No todas la vulnerabilidades se llegan a explotar porque ciertas suelen ser falso positivos, no se trata de explotarla para confirmar su existencia, simplemente se la reporta.

### 5.4.1 Vulnerabilidad: CSRF (Cross Site Request Forgery)

La vulnerabilidad CSRF se encuentra en algunos formularios de autenticación para el acceso a las aplicaciones entre ellos el formulario de acceso a la Intranet.

Como atacar:

- ✓ Es necesario realizar un script utilizando un diccionario de datos, el cual pretende probar todas las combinaciones posibles para la obtención de usuarios y claves.
- ✓ Otra forma es utilizar herramientas de explotación por fuerza bruta o diccionario de datos como la herramienta Hyndra.

El formulario de la Intranet no utiliza CAPTCHA para la autenticación de un usuario. Esta es una debilidad que aprovecha un atacante al no contar con un método que evite ataques de fuerza bruta o ataques de diccionario.

Utilizando la herramienta HYDRA por consola se procede a realizar un ataque de diccionario.

Antes de atacar se necesita saber el método de envío de datos y obtener los nombre de los inputs. Esto se obtiene mediante el complemento de Firefox, Live HTTP Headers.

Línea de comandos para realizar ataques de diccionario con Hydra:

```
root@kali:~# hydra -l 099254260 -P dic.txt XXX.XXX.XXX.XXX http-post-form
"/apliwebs/intranet.php:usuario=^USER^&clave=^PASS^:pudo verificar" –vV
```

| COMANDOS | FUNCIÓN |
|---|---|
| http-post-form | Tipo de servicio a atacar |

| | |
|---|---|
| -l | Contendrá usuario especifico |
| -P | Fichero que contendrá la lista de passwords |
| *"var_user"*, | Nombre del parámetro del formulario que contendrá el usuario |
| *"var_pass"* | Nombre del parámetro del formulario que contendrá la contraseña |
| "pudo verificar". | cadena que indicará que el login es correcto |

**Tabla 27 Comandos Hydra**
**Autor:** Bonilla Tumbaco Brenda

Se realizó el ataque de diccionario intentando averiguar las contraseñas, son pocas las posibilidades de éxito, siendo más eficientes realizar un ataque de fuerza bruta.

El ataque de fuerza bruta no se realizó por el nivel de estrés que le podría causar al servidor Web.

### 5.4.2 Vulnerabilidad: Denegación de Servicios

Esta vulnerabilidad no la explotaremos para no perjudicar nuestro servidor Web. El motivo de no atacar a esta vulnerabilidad es para evitar la pérdida de conectividad y la inaccesibilidad a los usuarios legítimos a las aplicaciones. Como se puede atacar:

1. Se procede a utilizar la herramienta slowloris.pl, esta trabaja enviando peticiones HTTP.

2. Se ejecuta la siguiente línea de comando en la terminal de linux:
   **root@kali:¼# perl slowloris.pl –dns XXX.XXX.XXX.XXX**

3. Así mantenemos ocupado el servidor con las peticiones enviadas constantemente lo que provoca inaccesibilidad o caída del servidor.

### 5.4.3 Vulnerabilidad: Blind SQLi

La vulnerabilidad Blind SQLi es hallada en la intranet, pero el método de envío es por POST, en este caso realizar un ataque manual no se logra porque la URL no contiene las variables que se envían, es preferible utilizar herramientas que automatizan este proceso.

Estas vulnerabilidades tienen son fácil de explotar y conseguir acceso a las bases de datos.

Con la siguiente línea de comando realizamos el ataque a Blind- SQLi en la herramienta SQLMAP:

```
root@kali:~# sqlmap --url
```

| Comandos | Función |
|---|---|
| --url | Link con vulnerabilidad |
| -p | Especifica parámetro vulnerable |
| -- dbms | Especifica el motor de base de datos que utiliza el sistema |
| -- level | Nivel de testeo |
| -- risk | Nivel de riesgo |
| --dbs | Busque todas las bases de datos |
| -- data | Especificar el método post |

**Tabla 28 Tabla SQLmap**
**Autor:** Bonilla Tumbaco Brenda

### 5.4.4 Vulnerabilidad: SQLi (SQL Injection)

El ataque de Inyección SQL se logra con la herramienta SQLMAP, el objetivo es hallar datos sensibles desde los servidores de bases de datos.

Se usa la URL, es decir el link que provoco un error de inyección SQL para realizar la explotación.

| Comandos | Función |
|---|---|
| --url | Link con vulnerabilidad |
| -p | Especifica parámetro vulnerable |
| -- cookie | Se especifica la cookie utilizada |
| -- dbms | Especifica el motor de base de datos que utiliza el sistema |
| -- level | Nivel de testeo |
| -- risk | Nivel de riesgo |
| --dbs | Busque todas las bases de datos |
| -- Random-agent | Usar navegador aleatorio |
| -T | Especificar nombre de tabla |
| -- tables | Extrae nombres de tablas |
| - C | Especificar nombre de columna |
| -- columns | Extraer todas las columnas |
| -- dump | Extrae todo los registros especificados |

**Tabla 29 Tabla Comandos SQLmap**
**Autor:** Bonilla Tumbaco Brenda

**Explotando vulnerabilidad**

Para obtener nombres de las bases de datos encontradas en el servidor se ejecuta la siguiente línea de comandos.

root@kali:~# **sqlmap** --

Para obtener los nombres de tablas de una base de datos llamada Bd_accesos ejecutamos la siguiente línea de comandos:

root@kali:~# **sqlmap** --
url="http://XXX.XXX.XXX.XXX/app/sisacaest.php?sid=13&rid=186" -p rid
-- cookie="PHPSESSID=mteggsbo1m93f1iq55b4c3pmv5" --
dbms="Microsoft SQL Server" --level 5 --risk 5 –D Bd_accesos --tables --
random-agent

Mostrar columnas de la tabla usuarios, perteneciente a la base de datos Bd_accesos:

root@kali:~# **sqlmap** --

Adquiriendo datos sensibles de la base de datos acceso, tabla usuarios:

root@kali:~# **sqlmap** –

Desde un agujero detectado se consiguió acceso a todas las bases de datos que contiene el servidor del centro de educación superior. Entre los datos privados están los del personal administrativo, docentes, estudiantes, en si todos los que conforman la comunidad universitaria.

### 5.4.5 Vulnerabilidad: XST (Cross-Site Tracing)

Esta vulnerabilidad se presenta por utilizar método HTTP TRACE, esta técnica se encarga de realizar bypass a la etiqueta HTTP-only.

**Como atacar:**

- ✓ Al igual que el XSS se utiliza script para obtener información de la cookie de sesión, a diferencia que el XST sirve para obtener credenciales de usuario por medio del método TRACE del HTTP, esta técnica de explotación es compleja porque los navegadores se encuentran actualizados y evitan que este tipo de ataques salten la

seguridad del HTTP only que protege la lectura y escritura de las cookies; el XST tiene un nivel medio de riesgo a que se produzca este ataque.

### 5.4.6 Vulnerabilidad: Click-Jacking

Asociación de botones o emergentes ajenos en la WEB del centro de educación superior conocido como Click-Jacking.

La página vulnerable permite la inserción de X-Frame-Options en una página HTML.

Como atacar:

- ✓ Se inserta código o script detrás del sitio Web original de la Institución para obligar al usuario realizar ciertas acciones, como hacer clic en un botón visible cuando realmente se da clic en un botón invisible para realizar una función diferente.

## 5.5 Soluciones / Informe

En el informe se detallará las anomalías encontradas durante la auditoría, sus posibles soluciones, conclusiones y recomendaciones.

Dicho informe servirá para mejorar la toma de decisiones por parte del jefe del Departamento de Producción con el fin de optimizar los controles de seguridad.

***A continuación se detalla las posibles soluciones a las vulnerabilidades encontradas.***

**Inyección SQLi y Blind SQLi**

Para evitar este tipo de vulnerabilidad que se encuentra ubicada en la posición A1 del Top 10 de las vulnerabilidades más críticas en las aplicaciones Web.

- ✓ Usar variables y consultas parametrizadas.
- ✓ Filtrar los caracteres especiales de entrada: comillas simples (‘), comillas dobles (“) caracteres \x00 o \x1); añadiendo “\” delante de las consultas SQL.
- ✓ Utilizar Firewall de Aplicaciones Web.

**Denegación de Servicio**

Para minimizar el riesgo de saturar al servidor Web con múltiples peticiones se debe realizar lo siguiente:

- ✓ Configurar Firewall para filtrar conexiones con paquetes mal intencionados, así como establecer ACLs[12] en caso sea necesario.
- ✓ Otra potencial solución pero de mayor costo es configurar un proxy reverso para establecer solo conexiones reales por autenticación de navegador u otros algoritmos.

**Cross Site Tracing - XST**

Para evitar la explotación XST, se necesita deshabilitar el método HTTP TRACE en el servidor Apache como en el caso de las aplicaciones del centro de educación superior.

- ✓ Para solucionar esto al final del fichero de configuración del servidor apache se fija la siguiente línea TraceEnable en Off.

**Croos Site Scripting – XSS**

El uso del plugin Uploadify por defecto es vulnerable la solución a esto es:

- ✓ Validar el contenido en la variable folder encontrada en el complemento UPLOADIFY antes de mostrárselas al usuario.

**Cross Site Request Forgery – CSRF**

Owasp propone el uso de Token, para evitar ataques **CSRF**, al momento de autenticación y dentro de una sesión para evitar que un atacante realice acciones involuntarias a la que estamos realizando.

**Click-Jacking**

Para evitar este tipo de vulnerabilidad se debe:

- ✓ Activar la cabecera X-FRAME-OPTIONS para evitar que un atacante pueda montar un sitio sobre el real.

Protege que un archivo HTML se inserte dentro de un **iframe**. El uso de esta etiqueta en la cual se puede mostrar una página web dentro de otra página web.

## 5.6 Comprobación de la Hipótesis

Para mejorar la protección de los datos manejados por las aplicaciones de la WEB se implementarán recomendaciones para mitigar las vulnerabilidades encontradas.

OWASP, facilita un esquema para identificar el nivel de riesgo que provocan las vulnerabilidades encontradas en la auditoría realizada. En la siguiente Figura 5.42 observamos el esquema guía para valorar el tipo de riesgo:


**Figura 23 Esquema valoración del riesgo**
Fuente: www.owasp.org/images/5/5f/OWASP_Top_10_-_2013_Final_-_Espa%C3%B1ol.pdf

En el siguiente cuadro observamos las vulnerabilidades halladas y el nivel de riesgo que están propensas a ser explotadas por terceras personas:

| Vulnerabilidad | Vector de Ataque | Valoración del Riesgo |
|---|---|---|
| Inyección SQL – Blind Sqli | **Fácil** | **Alta** |
| Click-Jacking | **Fácil** | **Alta** |
| Denegación de servicios | **Fácil** | **Alta** |
| CSRF | **Fácil** | **Alta** |
| XST (Cross-Site Tracing) | **Promedio** | **Media** |
| XSS(Cross Site Scripting) | **Promedio** | **Media** |

**Tabla 30Tabla Nivel de Riesgo**
**Autor:** Bonilla Tumbaco Brenda

Podemos observar la existencia de varias falencias que contiene el sistema informático en general, por esta razón en muy factible la implementación de una auditoria externa al sistema para contribuir en gran parte a la formación de un óptimo funcionamiento y eficiente servicio a los usuarios en general del centro de educación superior referenciando técnicas de soluciones para el alcance del perfeccionamiento estructural como lógico reduciendo a la mínima posibilidad de sufrir una ataque malicioso provenientes de cualquier tipo o locación.

## CONCLUSIONES

- ✓ Con la aplicación de las metodologías de testeo de seguridad informática de licencia abierta, se pudo optimizar el orden metodológico del proceso de la auditoría y se consiguió un test de intrusión eficiente

- ✓ En el proceso de la auditoria se encontraron diversas vulnerabilidades, entre las más relevantes, Inyección SQL al igual que Blind-SQL, permitió introducir pequeños fragmentos de códigos obteniendo acceso a las bases de datos; Denegación de servicios también conocido como ataque de DOS que ocasiona que un servicio o recurso sea inaccesible, la vulnerabilidad XSS permite inyectar código Script en páginas web, todas estas vulnerabilidades deben ser controladas para mitigar el riesgo que exista explotación en una de ellas.

- ✓ Los usuarios no han sufrido perjuicios con los datos que se almacenan en los servidores del centro de educación superior; esto no quiere decir que deje de existir el riesgo de pérdida, alteración o hurto de datos privados. Durante el análisis realizado por la auditoria podemos tener claro que existen varias posibilidades de poder tener acceso a las aplicaciones y servidores permitiéndonos de esta manera la manipulación, modificación y sustracción de información de los mismos debido a que constantemente aparecen nuevos métodos o herramientas con este fin.

## RECOMENDACIONES

- ✓ Mantenerse al tanto de ataques que se han realizado a otros sistemas para estar actualizados y establecer controles de seguridad.
- ✓ Mantener el nivel de seguridad intacto, realizando comprobaciones de mantenimiento en las aplicaciones Web mensualmente para asegurar que no se han introducido nuevos riesgos.
- ✓ Construir un marco de trabajo de pruebas que evidencie la seguridad en cada una de las fases del ciclo de vida de un Software para mejorar la seguridad de las aplicaciones.
- ✓ Se deben implementar seguridades en cada una de las etapas de desarrollo de las aplicaciones incluso en la fase de pruebas para su última comprobación de seguridad.
- ✓ Es imperioso utilizar un Firewall de Aplicaciones Web (WAF) el cual protege de los ataques maliciosos, como inyección SQL, denegación de servicios, spam entre otros.
- ✓ Brindar información de seguridad al usuario final para evitar caer en técnicas de Ingeniería Social y dar hincapié al cambio de claves frecuentemente.
- ✓ Implementar medidas preventivas de seguridad constantes para no tener inconvenientes en un futuro.

## GLOSARIO

**Bypass:** Archivo o líneas de códigos que puede inferir en las bases de datos

**Click-Jacking:** Es una vulnerabilidad de “secuestro de clic”, se trata de un fallo hallado en el diseño de una página web en HTML.

**Cross Site Request Forgery (CSRF): “**Forma de forzar a un usuario a ejecutar acciones no deseadas en una aplicación Web en la que se encuentra actualmente autenticado” (Owasp.org, 2008).

**Cross Site Tracing (XST)**
Es una vulnerabilidad común en las aplicaciones Web, generada por el método HTTP TRACE, dicho método muestra las cookies que contiene el navegador.

**Denegación de servicios**: “El concepto fundamental de un ataque DoS de red es un usuario malicioso inundando con suficiente tráfico una máquina objetivo para conseguir hacerla incapaz de sostener el volumen de peticiones que recibe” (Owasp.org, 2008).

**Hacker ético:** Tiene la necesidad de mantenerse dentro de la Ley y siempre actuar de manera profesional.

**Live HTTP Headers:** Sirve para ver información (Cookies, Método de envió GET o POST) de los encabezados de una página Web.

**NMAP:** Mapeador de Redes

**OWASP:** OWASP (Open Web Application Security Project)

**Pentest:** Test de Penetración.

**SQLi (SQL Injection).** Ataque de Inyección SQL con la herramienta SQLMAP con el fin de hallar datos sensibles desde los servidores de bases de datos.

**THEHARVESTER:** Otra herramienta para recabar subdominios y cuentas de correo electrónico.

**WAF (Web Application Firewall):** Firewall de Aplicación Web.

**Whois:** Protocolo TCP, permite realizar una petición y devuelva información sobre el propietario de un dominio.

**Bibliografía**


José Antonio Echenique García. (2001). *Auditoría en Informática* (2da. edicion ed.). Mexico: Mc Graw - Hill Interamericana.

Piattini Velthuis, M., & Del Peso Navarro, E. (2001). *Auditoría informática: Un enfoque práctico* (2a ed ed.). Bogotá, Colombia: Alfaomega Colombiana.

Caballar Falcon, J. (2006). *Firewall : La seguridad de la banda ancha.*

Mexico: Alfaomega.

ACISSI. (2013). *Seguridad informática - Ethical Hacking* (Segunda edición ed.). España: ENI.

0xdeadlock.org. (Noviembre de 2014). Obtenido de http://0xdeadlock.org/web-pentesting/

Cabrera, C. (Febrero de 2015). *Blog Informática*. Recuperado el 20 de Febrero de 2015, de http://cesarcabrera.info/blog/%C2%BFcomo-funcionan-las-acl-en-cisco-i-conceptos/

Centro de Investigaciones Sociológicas. (2013). Recuperado el 21 de Junio de 2014, de http://www.cis.es/cis/opencms/ES/1_encuestas/ComoSeHacen/queesunaencuesta.html

COBIT. (JUNIO de 2012). *Jaisraal's Blog*. Recuperado el 30 de Julio de 2014, de https://jaisraal.wordpress.com/2011/08/22/cobit-4-1-objetivos-de-control-para-la-informacion-y-tecnologias-relacionadas/

El Código Orgánico Integral Penal. (10 de Febrero de 2014). Recuperado el 30 de Julio de 2014, de http://www.ministeriointerior.gob.ec/wp-content/uploads/downloads/2014/03/CODIGO-PENAL.pdf

Ley N° 162 Sistema Nacional de Registro de Datos Públicos. (24 de Marzo de 2010). *RED IBEROAMERICANA DE PROTECCION DE DATOS.* Recuperado el 30 de Mayo de 2014, de http://www.redipd.org/legislacion/common/legislacion/ecuador/Ley_N_162.pdf

Ley No. 2002-67 Ley de Comercio Electrónico, Firmas y Mensajes de Datos . (17 de Abril de 2002). *Red Iberoamericana de protección* de datos. Recuperado el 30 de Julio de 2014, de http://www.redipd.org/legislacion/common/legislacion/ecuador/ecua dor_ley_2002-67_17042002_comelectronico.pdf