ANÁLISIS Y EVALUACIÓN DE LA SEGURIDAD INFORMÁTICA PARA LA PÁGINA WEB PUBLICADA EN HOSTING GRATUITO DE LA INSTITUCIÓN TÉCNICA DE FIRAVITOBA, PARA LA DETECCIÓN Y REMEDIACIÓN DE VULNERABILIDADES Y RIESGOS EN LA INFORMACIÓN.

Ing:

GLORIA MIREYA RINCON
FLORALBA ALBARRACIN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA –UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
SOGAMOSO BOYACA
2018

ANÁLISIS Y EVALUACIÓN DE LA SEGURIDAD INFORMÁTICA PARA LA PÁGINA WEB PUBLICADA EN HOSTING GRATUITO DE LA INSTITUCIÓN TÉCNICA DE FIRAVITOBA, PARA LA DETECCIÓN Y REMEDIACIÓN DE VULNERABILIDADES Y RIESGOS EN LA INFORMACIÓN.

Ing:
GLORIA MIREYA RINCON
FLORALBA ALBARRACIN

Trabajo de grado para optar el título de Especialistas en Seguridad Informática

DIRECTOR:
ING. JUAN JOSE CRUZ GARZON

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA –UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
SOGAMOSO BOYACA
2018

Nota aceptación:

_____
_____
_____
_____

_____

Firma Presidente del jurado

_____

Firma Jurado

_____

Firma Jurado

Sogamoso, Febrero del 2018

DEDICATORIA

A DIOS
Por ser el creador de la vida
A MIS PADRES Y FAMILIA
Por el apoyo incondicional y granito de arena
Que me suministran en lo que hago.

GLORIA MIREYA RINCON

A DIOS
Por ser el autor de mis días
A MIS PADRES
“Floralba y Olegario” (Q.E.P.D).
Por el apoyo incondicional
y sus sabios consejos.
A MI FAMILIA
Mi esposo Guillermo y mis hijos Valeria y Guillermo
Quienes con su amor, comprensión y colaboración
Me ayudaron a culminar esta etapa con éxito.

FLORALBA ALBARRACIN

AGRADECIMIENTOS

Al Director de nuestro proyecto Ingeniero JUAN JOSE CRUZ GARZON quien con sus conocimientos y experiencia nos orientó y apoyo en el desarrollo del proyecto, quien siempre estuvo dispuesto a colaborarnos y guiarnos incondicionalmente.

A los profesores de la Universidad Nacional Abierta y a Distancia por su conocimiento, paciencia y ayuda para permitirnos culminar nuestro proyecto de Grado.

A la institución educativa técnica de Firavitoba por permitirnos desarrolla el proyecto de grado, suministrándonos la información correspondiente para el análisis y desarrollo del proyecto y el apoyo brindado en cada uno de los momentos que lo necesitamos.

TABLA DE CONTENIDO

Pág.

TABLA DE ILUSTRACIONES

TABLA DE TABLAS

RESUMEN

Teniendo en cuenta los diferentes medios y herramientas para realizar un correcto análisis de la seguridad en la información de una Página web, el presente trabajo tiene como finalidad conocer las vulnerabilidades a las que está expuesta la información de la Página Web de la institución educativa técnica de Firavitoba por la falta de mecanismos de controles de seguridad.

El análisis está dirigido a una Institución educativa Técnica, teniendo como objetivo principal el estudio de la seguridad de la información de la Página Web a la cual tiene acceso la institución educativa y la comunidad que pertenece a esta. Por medio de visitas, revisión de la aplicación Web, observación, consultas, encuestas y ejecución de pruebas, se logró identificar los riesgos actuales a los que se exponen los datos tanto físicos como lógicos de la página Web.

La ejecución del análisis de riesgos da a conocer el nivel de impacto con respecto a las amenazas identificadas en la información que se comparte por la Web.

Los resultados obtenidos dan a conocer que para minimizar los riesgos en el flujo de la información, es necesario implementar controles y acciones de seguridad, lo que ayudara a fortalecer tres aspectos importantes en la seguridad de la información: la confidencialidad, integridad y disponibilidad de la información.

INTRODUCCION

Actualmente la seguridad informática en aplicaciones web ha adquirido gran auge, dadas las cambiantes condiciones y nuevas tecnologías de la Información y comunicación disponibles, situación que contribuye con la aparición de nuevas amenazas en los sitios web.

La información es el activo más importante de la Institución Educativa, asegurarla trae beneficios y credibilidad para ella, Por esto debemos preguntarnos ¿Está la información segura?, por lo tanto no podemos dejar de hablar de la seguridad en aplicaciones Web, ya que a partir de ellas podemos obtener información. Ofrecer una herramienta para garantizar la seguridad en la página web puede ser de gran utilidad para la tranquilidad de toda la Institución Educativa.

De acuerdo con lo anterior, se pretende realizar un análisis de riesgo a la página web de la institución educativa de Firavitoba con la finalidad de minimizar los riesgos presentados en el manejo de la información ya que la información contenida requiere un alto compromiso con la Institución y con la comunidad que tiene acceso a la página web.

1. TITULO DEL PROYECTO

ANÁLISIS Y EVALUACIÓN DE LA SEGURIDAD INFORMÁTICA PARA LA PÁGINA WEB PUBLICADA EN HOSTING GRATUITO DE LA INSTITUCIÓN TÉCNICA DE FIRAVITOBA, PARA LA DETECCIÓN Y REMEDIACIÓN DE VULNERABILIDADES Y RIESGOS EN LA INFORMACIÓN.

AREA DE INVESTIGACION: Seguridad informática en página web

2. DEFINICIÓN DEL PROBLEMA

2.1. ANTECEDENTES DEL PROBLEMA

En la actualidad las tecnologías de la información y la comunicación (TIC) en las empresas son de gran utilidad, llegando a posicionarse como indispensables para diversos procesos como la producción y comercialización ya que favorecen el flujo de información, fortalecen el trabajo en equipo, gestión de inventarios y existencias, análisis financieros y; promoción y comercialización de productos en el mercado.

Las pequeñas empresas, que utilizan para la promoción de sus productos hosting gratuitos, a veces no consideran la seguridad web como primordial ya que piensan que no representan un objetivo importante para los atacantes. Sin embargo, cualquier emprendimiento en línea debe enfrentar a una variedad de peligros y amenazas que deben comprenderse, evaluarse y contrarrestarse, Turner (2014), afirma que la base de datos “CVE (Vulnerabilidades y Exposiciones Comunes) incluye más de 59.000 amenazas conocidas contra la seguridad de la información, y una búsqueda en la base de datos de apache devuelve una lista de más de 500 vulnerabilidades conocidas”.

Las vulnerabilidades a las que se exponen las páginas web afectan potencialmente su integridad, disponibilidad y confidencialidad por ello se desarrolla un protocolo de evaluación de la seguridad de páginas web con hosting gratuito, basados en el proyecto OWASP, con miras a identificar si éstas páginas son o no seguras para las empresas, detectar estas vulnerabilidades antes de que un atacante lo haga, permitirá tomar las medidas necesarias y así evitar afectaciones en la imagen corporativa y mantener la confianza de los clientes. Cabe resaltar que la institución educativa de Firavitoba no es ajena a este tipo de vulnerabilidades, ya que se debería contar con mecanismos que ayuden a mitigar las amenazas por las cuales puede estar enfrentada la página web.

2.2. FORMULACION DEL PROBLEMA

¿Qué mecanismos de mitigación se deben tener en cuenta para la detección y remediación de vulnerabilidades de la página web de la Institución educativa técnica de firavitoba en cuanto a la seguridad de la información?

2.3. DESCRIPCION DEL PROBLEMA:

Actualmente la Institución Educativa Técnica de Firavitoba cuenta con una página web donde se maneja mucha información sensible. La falta de garantía de la Institución respecto a la seguridad de la información, para contrarrestar y prevenir los ataques a los que están expuestas diariamente es preocupante, por esta razón es importante detectar por medio de herramientas de diagnóstico los diferentes riesgos y ataques a los cuales

se encuentra expuesta la página web de la institución educativa de Firavitoba, con el fin de garantizar el nivel de seguridad informática en la Institución y, adoptar mecanismos de protección y poder contar con un conjunto de recomendaciones que los orienten como parte de la estrategia de seguridad en la información que manejan desde la web.

Con el uso correcto de la herramienta Owasp se analiza y se evalúa el nivel de seguridad a la que se encuentra expuesta la página web de la institución educativa técnica de Firavitoba, esto permitirá detectar el riesgo y amenazas a las que se encuentra expuesta la página web, con el fin de redir un informe que los invite a manejar protocolos y estrategias de seguridad en la página web, lo cual garantizara el manejo y consulta de la información por el personal y comunidad en general que accede a sus servicios y lo más importante contar con un porcentaje elevado de su seguridad y protección en sus datos.

3. JUSTIFICACION

Las Tics, (Tecnologías de información y Comunicación), especialmente el internet ha abierto un sin número de posibilidades de acceso a la información y de igual manera se han generado nuevos riesgos que involucran la seguridad de la misma, este es un momento crítico de cambio, pues hay una gran apertura en las comunicaciones y las posibilidades para compartir información en internet, demandan más seguridad para cada acción que se tome[1], para evitar fugas de información.

Con los conocimientos y la implementación correcta de medidas de seguridad, se pueden proteger los recursos, así como proporcionar un entorno seguro donde los usuarios trabajen cómodos con su aplicación.

La mayoría de las aplicaciones informáticas se encuentra en aplicaciones Web, debido a la accesibilidad en cualquier momento y lugar, es necesario mantener controlado el tráfico de información por medio de su seguridad, todo ambiente Web es propenso a posibles ataques, mal uso e incluso al robo o fuga de información. Por ende, es necesario implementar medidas de seguridad adecuadas para cada tipo, tamaño y necesidad de una empresa, ya que los modelos de seguridad en aplicaciones Web reducen vulnerabilidades y los gastos en solucionar eventualidades.

Una aplicación web con altos niveles de seguridad, es un elemento diferenciador, generador de confianza y valor para la empresa, las empresas en Latinoamérica cada vez más encuentran en la seguridad de la información una forma para marcar la diferencia como socio estratégico del negocio[2].

Para esto es vital contar con herramientas robustas para revisar el nivel de calidad y seguridad de las aplicaciones, generando por consiguiente nuevas oportunidades de trabajo en un área que continuamente exige la participación de profesionales en seguridad informática[3].

---

[1] AMÓRTEGUI T. Diego J., Ciberseguridad y Ciberterrorismo [en línea], <http://www.acis.org.co/fileadmin/Revista_119/informe_Diego_Amortegui.pdf>, [citado el 02 de Septiembre de 2011]

[2] ASOCIACION DE INGENIEROS DE SISTEMAS. Seguridad de la información en Latinoamérica, Tendencias en 2011 [en línea], Tomado de: <http://www.acis.org.co/fileadmin/Revista_119/informe_Latinoamerica 2011.pdf>, [citado el 02 de Septiembre de 2011]

[3] ASOCIACION DE INGENIEROS DE SISTEMAS. Seguridad de la información en Latinoamérica, Tendencias en 2011 [en línea], Tomado de: <http://www.acis.org.co/fileadmin/Revista_119/informe_Latinoamerica 2011.pdf>, [citado el 02 de Septiembre de 2011]

4. OBJETIVOS

4.1. OBJETIVO GENERAL

Analizar y evaluar la seguridad informática para la página web publicada en hosting gratuito de la institución técnica de Firavitoba, para la detección y remediación de vulnerabilidades y riesgos en la información.

4.2. OBJETIVOS ESPECÍFICOS

1. Analizar los conceptos y fundamentos de seguridad en aplicaciones web para diagnosticar la página web de la Institución educativa técnica de Firavitoba.

2. Clasificar los activos de información de la página web de la Institución Educativa.

3. Determinar que herramientas existen actualmente para detección de vulnerabilidades en aplicaciones web.

4. Comprobar las características principales de algunas metodologías existentes para la seguridad en aplicaciones web.

5. Establecer los tipos de vulnerabilidades que se detectan a través de las pruebas realizadas a la página web de la Institución Educativa en la aplicación web.

6. Suministrar un informe relacionando los diferentes riesgos a los cuales se encuentra expuesta la página web de la Institución Educativa y las posibles soluciones para mejorar la seguridad de su información.

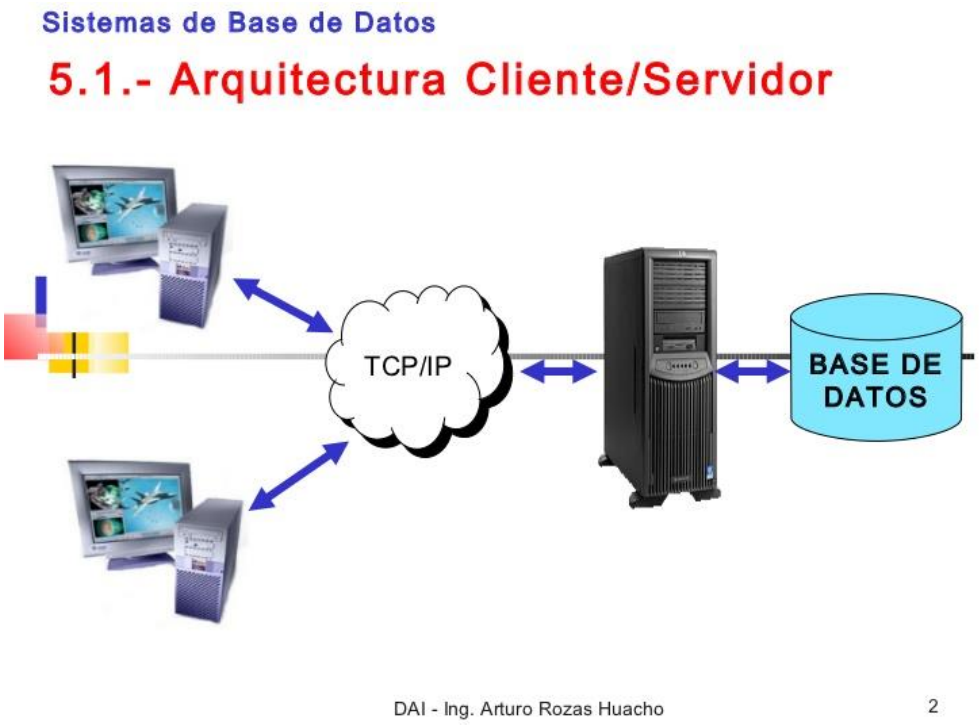
5. MARCO REFERENCIAL

5.1. MARCO TEORICO

5.1.1. Definición de página web.

En la ingeniería de software se denomina aplicación web a aquellas herramientas que los usuarios pueden utilizar accediendo a un servidor web a través de Internet o de una intranet mediante un navegador. Es una aplicación software que se codifica en un lenguaje soportado por los navegadores web en la que se confía la ejecución al navegador (Mozilla Firefox, Google Chrome, Internet Explorer) etc.

ILUSTRACIÓN 1 ING. ARTURO ROZAS HURTADO.



La arquitectura cliente-servidor es un modelo de aplicación distribuida en el que las tareas se reparten entre los proveedores de recursos o servicios, llamados servidores, y los demandantes, llamados clientes.

Un cliente realiza peticiones a otro programa, el servidor, quien le da respuesta. Esta idea también se puede aplicar a programas que se ejecutan sobre una sola computadora, aunque

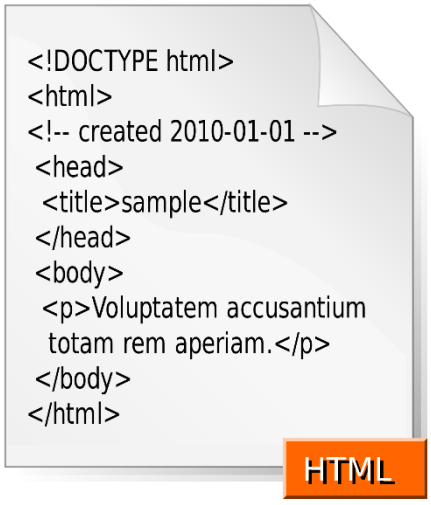
es más ventajosa en un sistema operativo multiusuario distribuido a través de una red de computadoras.

Actualmente existen diferentes lenguajes de programación desarrollar las aplicaciones web, a medida del tiempo van avanzando de acuerdo a las tendencias y necesidades, al inicio estas páginas eran estáticas y con las nuevas tecnologías surgen las dinámicas, permitiendo bases de datos para interactuar con los usuarios.

Algunos lenguajes de programación son:

HTML

Ilustración 2 CODIGO FUENTE.



Es uno de los lenguajes de programación web más importante y uno de los más usados para la creación de documentos. El Hyper Text Markup Language (HTML) es un lenguaje de marcado que se diseñó con el objetivo de estructurar documentos y mostrarlos en forma de hipertexto.[4]

Html cumple con dos objetivos fundamentales para el diseño y visualización de un documento digital:

- ✓ Organiza un documento en elementos lógicos, tales como: encabezado, párrafo, etc.
- ✓ Define las operaciones tipográficas y las funciones que debe ejecutar un programa visualizador sobre dichos elementos.

JAVASCRIPT

[4] CODEBOX, Glosario[en línea],<http://www.codebox.es/glosario>, [citado el 05 de Septiembre de 2011]

JavaScript es un lenguaje de programación orientado a objetos, es dinámico, las variables no necesitan ser introducidas antes de su uso y los tipos de variables se resuelven dinámicamente durante su ejecución. Se trata de un lenguaje de programación del lado del cliente, porque es el navegador el que soporta la carga de procesamiento.

PHP
Es un lenguaje que está implementado especialmente para el desarrollo web. PHP: HypertextPreprocessor (PHP) es un lenguaje de programación web de alto nivel que se ejecuta en el servidor.[5]

ILUSTRACIÓN 3 PHP CODE.

```php
//Función que genera un rtf
function rtf($sql, $plantilla, $fsalida, $matequivalencias){
$pre=time();
$fsalida="/teleusers/certificados/".$pre.$fsalida;
mysql_connect("localhost","usuario","contraseña");
//Paso nº1.- Leo la platilla rtf
$txtplantilla = leef($plantilla);
//Paso nº2.- Saca cabecera, el cuerpo y el final.
$matriz=explode("sectd",$txtplantilla);
$cabecera=$matriz[0]."sectd";
$inicio=strlen($cabecera);
$final=strrpos($txtplantilla,"}");
$largo=$final-$inicio;
$cuerpo=substr($txtplantilla,$inicio,$largo);
//Paso nº3.- Escribo el fichero
$punt = fopen($fsalida , "w");
fputs($punt,$cabecera);
$result = mysql("base_datos", $sql);
While($row=mysql_fetch_object($result)){
    $despues=$cuerpo;
    foreach ($matequivalencias as $dato) {
        $datosql=$row->$dato[1];
        $datosql = stripslashes ($datosql);
        $datortf=$dato[0];
        $despues=str_replace($datortf,$datosql,$despues);
    }
    fputs($punt,$despues);
    $saltopag="\par \page \par";
    fputs($punt,$saltopag);
}
fputs($punt,"}");
fclose ($punt);
return $fsalida;
}
```

5.1.2. Elementos de seguridad en la web

La red mundial Internet y sus elementos asociados son mecanismos ágiles que proveen una alta gama de posibilidades de comunicación, interacción y entretenimiento, tales como elementos de multimedia, foros, chat, correo, comunidades, bibliotecas virtuales entre otros que pueden ser accedidos por todo tipo de público. Sin embargo, estos elementos deben contener mecanismos que protejan y reduzcan los riesgos de seguridad alojados, distribuidos y potencializados a través del mismo servicio de Internet.

MEDIA COMMERCE como proveedor del servicio de TELECOMUNICACIONES está convencida de que las relaciones con nuestros clientes se deben fortalecer desde una

[5] New Web Star. Los diferentes lenguajes de programación para la web [en línea],<http://www.newwebstar.com/ebooks/133193-los-diferentes-programas- de- programación-para-la-html>, [citado el 06 de Septiembre de 2011]

comunicación asertiva, sana y orientada a proporcionar las herramientas y concejos prácticos necesarios para la protección adecuada de los elementos de cómputo y los servicios asociados a la Internet. Por esta razón ponemos a disposición de todos nuestros clientes y de la comunidad en general, conceptos teórico - prácticos que pueden evitar o reducir los riesgos a que se está expuesto cuando se interactúa con la Internet y sus elementos asociados.

5.1.3. Conceptos generales de seguridad

El objetivo de la seguridad informática es mantener la integridad, disponibilidad, privacidad, control y autenticidad de la información manejada por un sistema informático en cualquier organización. La seguridad Informática abarca mucho más que la protección de la información, pero sin duda es ésta el activo más atractivo para los hackers, teniendo en cuenta que la información es la base económica de las empresas y de toda organización.

La Seguridad Informática en aplicaciones Web se basa en tres características y principios fundamentales:

ILUSTRACIÓN 4 PRINCIPIOS DE LA SEGURIDAD INFORMÁTICA.

• Confidencialidad: Se refiere a que la información solo puede ser conocida por individuos autorizados impidiendo la divulgación de esta a entidades no autorizadas, la pérdida de confidencialidad de la información se refleja en muchos aspectos desde el momento en que una persona puede observar lo que se está haciendo en el pc, cuando se publica información privada, cuando se roba información, cuando se divulga la información por teléfono o de forma directa. Lo anterior exprese la violación de la confidencialidad de la información.

• Integridad: Se refiere a la seguridad de que una información no ha sido alterada, borrada, reordenada, copiada, etc., durante el proceso de transmisión o en su propio equipo de origen, donde se evita que la información sea manipulada por un tercero. La violación de la integridad se evidencia cuando un tercero, software o proceso ya sea por accidente o por mala intención edita, o borra los datos importantes de un sistema web.

Con la integridad se garantiza la seguridad de los datos excepto cuando es modificada por personal autorizado por la empresa. Evidenciando el registro de la modificación de la información.

• Disponibilidad: Se refiere a que la información pueda ser recuperada o esté disponible en el momento que se necesite para quien desee acceder a ella ya sean personas, procesos, programas y o aplicaciones. La disponibilidad es el acceso a la información o sistemas por personas autorizadas en el momento que lo requieran. La alta disponibilidad de los sistemas debe estar disponibles en todo momento evitando perdida el servicio por cortes de energía, fallas de hardware, transferencia de datos en la red de internet y posibles actualizaciones del sistema.

5.1.3.1. Metodologías para la seguridad de aplicaciones web

Teniendo presenta estas característica las cuales forman parte de diferentes metodologías para la seguridad de aplicaciones web como lo son OWASP, OSSTMM, ISSAF, nos podemos dar cuenta que cumplen un papel fundamental en la ejecución de la seguridad de aplicaciones Web.

A continuación se plasma a groso modo un resumen relacionado con la metodología OWASP, OSSTMM, ISSAF.

5.1.3.1.1. Metodología OWASP:[6]

Ilustración 5 METODOLOGÍA OWASP.

La Herramienta OWASP (Open Web Application Security Project), está diseñada como un marco de trabajo que ayude en el proceso del ciclo de desarrollo del software ésta provee una solución flexible que mejora el proceso de desarrollo, teniendo en cuenta desde el inicio el tema de la seguridad en la ingeniería de software.

---

[6] Guía de pruebas OWASP V 3.0 [En línea], disponible en: https://www.owasp.org/images/8/80/Gu%C3%ADa_de_pruebas_de_OWASP_ver_3.0.pdf >, [Citado 2008]

Estructuralmente esta herramienta consta de las siguientes fases:

FASE 1: ANTES DE EMPEZAR EL DESARROLLO

Antes de que el desarrollo de la aplicación haya empezado:

Comprobación para asegurar que existe un SDLC adecuado, en el cual la seguridad sea inherente.

Comprobación para asegurar que están implementados la política y estándares de seguridad adecuados para el equipo de desarrollo.

Desarrollar las métricas y criterios de medición.

FASE 2 - DURANTE EL DISEÑO Y DEFINICIÓN FASE

Los requisitos de seguridad definen como funciona una aplicación desde una perspectiva de la seguridad. Es indispensable que los requisitos de seguridad sean probados. Probar, en este caso, significa comprobar los supuestos realizados en los requisitos, y comprobar si hay deficiencias en las definiciones de los requisitos. Por ejemplo, si hay un requisito de seguridad que indica que los usuarios deben estar registrados antes de tener acceso a la sección de Documentos de un site, ¿Significa que el usuario debe estar registrado con el sistema, o debe estar autenticado? Asegúrate de que los requisitos sea lo menos ambiguo posible. A la hora de buscar inconsistencias en los requisitos, ten en cuenta mecanismos de seguridad como:

Gestión de Usuarios (reinicio de contraseñas, etc.)

Autenticación OWASP Testing Guide v3.0 49 Autorización

Confidencialidad de los Datos

Integridad

Contabilidad

Gestión de Sesiones

Seguridad de Transporte

Segregación de Sistemas en Niveles

Privacidad

FASE 3: DURANTE EL DESARROLLO

En teoría, el desarrollo es la implementación de un diseño. Sin embargo, en el mundo real, muchas decisiones de diseño son tomadas durante el desarrollo del código. A menudo son decisiones menores, que o bien eran demasiado detalladas para ser descritas en el diseño

o, en otros cosas, incidencias para las cuales no había ninguna directriz o guía que las cubriese. Si la arquitectura y el diseño no eran los adecuados, el desarrollador tendrá que afrontar muchas decisiones. Si las políticas y estándares eran insuficientes, tendrá que afrontar todavía más decisiones.

FASE 4: DURANTE LA IMPLEMENTACIÓN FASE

Tras haber comprobado los requisitos, analizado el diseño y realizado la revisión de código, debería asumirse que se han identificado todas las incidencias. Con suerte, ese será el caso, pero las pruebas de intrusión en la aplicación después de que haya sido implementada nos proporcionan una última comprobación para asegurarnos de que no se nos ha olvidado nada.

La prueba de intrusión de la aplicación debería incluir la comprobación de cómo se implementó y securizó su infraestructura. Aunque la aplicación puede ser segura, un pequeño detalle de la configuración podría estar en una etapa de instalación predeterminada, y ser vulnerable a explotación.

FASE 5: MANTENIMIENTO Y OPERACIONES FASE

Debe existir un proceso que detalle como es gestionada la sección operativa de la aplicación y su infraestructura.

Deberían realizarse comprobaciones de mantenimiento mensual o trimestral, sobre la aplicación e infraestructura, para asegurar que no se han introducido nuevos riesgos de seguridad y que el nivel de seguridad sigue intacto.

5.1.3.1.2. Metodología ISSAF[7]:

ISSAF, de OISSG (Open Information System Security Group) ha presentado formalmente su versión “Draft 0.2". Es uno de los frameworks más interesantes dentro del ámbito de metodología de testeo. Realiza un análisis detallado de todos los posibles aspectos que afectan al testeo de seguridad.

La información contenida dentro de ISSAF, se encuentra organizada alrededor de lo que se ha dado en llamar “Criterios de Evaluación”, cada uno de los cuales ha sido escrito y revisado por expertos en cada una de las áreas de aplicación. Estos criterios de evaluación a su vez, se componen de los siguientes ítems:

- Una descripción del criterio de evaluación.
- Puntos y objetivos a cubrir.
- Los prerrequisitos para conducir la evaluación.

[7] Metodología y Frameworks de testeo de la seguridad en aplicaciones, [En línea], disponible en: http://www.juntadeandalucia.es/servicios/madeja/sites/default/files/historico/1.3.0/contenido-recurso-216.html#OSSTMM

- El proceso mismo de evaluación.
- El informe de los resultados esperados.
- Las contramedidas y recomendaciones.
- Referencias y Documentación Externa.

Para organizar de forma sistemática las labores de testeo, dichos “Criterios de Evaluación”, se han catalogado, desde los aspectos más generales, como pueden ser los conceptos básicos de la “Administración de Proyectos de Testeo de Seguridad”, hasta técnicas tan puntuales como la ejecución de pruebas de Inyección de Código SQL o como las “Estrategias del Cracking de Contraseñas”.

5.1.3.1.3. Metodología OSSTMM:[8]

El “Manual de la Metodología Abierta de Testeo de Seguridad” se ha convertido en un estándar de facto. Sin duda supuso el primer acercamiento a una estructura global de concepto de seguridad. Si bien las pruebas incluidas y los test que se ejecutan no son especialmente innovadores, se ha convertido en una auténtica referencia para los organismos que quieren desarrollar un Testing de calidad, ordenado y eficiente.

Para organizar estructurar su contenido, la metodología se subdivide en los aspectos más importantes de los sistemas de información. Se destacan los siguientes aspectos como:

- Seguridad de la Información
- Seguridad de los Procesos
- Seguridad en las Tecnologías de Internet
- Seguridad en las Comunicaciones
- Seguridad Inalámbrica
- Seguridad Física

De manera sencilla se identifican una serie de actividades de testeo específicas por área, sobre las que se comprueban las especificaciones de seguridad, integradas con las verificaciones realizadas en las revisiones rutinarias.

Con esta metodología, se realiza un esfuerzo para convertir en predecible QUE se debe de probar, COMO se puede hacer y CUANDO es necesario ejecutarlo. De esta manera se aumenta la calidad del desarrollo, ya que al seguir esta metodología, se tiene la certeza de que se cumplen unos objetivos prefijados.

Un aspecto importante de esta metodología, es que no solo se centra en los aspectos eminentemente técnicos de seguridad tradicionales, sino que abarca aspectos sobre los responsables del testeo. Trata de estandarizar las credenciales del desarrollador a cargo del

[8] Metodología y Frameworks de testeo de la seguridad en aplicaciones, [En línea], disponible en: http://www.juntadeandalucia.es/servicios/madeja/sites/default/files/historico/1.3.0/contenido-recurso-216.html#OSSTMM

test, el formato de los resultados, crear un código ético, un plan temporal de ejecución, etc… Un aspecto muy importante de la metodología, es la incorporación del concepto de Valores de Evaluación de Riesgo, que permiten diferenciar y clasificar las diferentes problemáticas.

OSSTMM plantea categorizaciones estándar, que permiten identificar claramente el alcance de cada una de las actividades, evitando inconvenientes en tal sentido:

Búsqueda de Vulnerabilidades: Orientado principalmente a realizar comprobaciones automáticas de un sistema o sistemas dentro de una red.

Escaneo de la Seguridad: Orientado a las búsquedas principales de vulnerabilidades en el sistema que incluyen verificaciones manuales de falsos positivos, identificación de los puntos débiles en el sistemas y análisis individualizado.

Test de Intrusión: Se plantean test de pruebas que se centran en romper la seguridad de un sistema determinado.

Evaluación de Riesgo: se refiere a los análisis de seguridad a través de entrevistas e investigación de nivel medio que incluye la justificación negocios, las justificaciones legales y las justificaciones específicas de la industria.

Auditoria de Seguridad: Se refiere a la continua inspección que sufre el sistema por parte de los administradores que controlan que se cumplan las políticas de seguridad definidas.

Hacking Ético: Orientado a tratar de obtener, a partir de los test de intrusión, objetivos complejos dentro de la red de sistemas.

5.1.3.2. Principios de las políticas de seguridad:

Se encuentran otros principios transversales a tener en cuenta según las políticas de seguridad en una organización:

• Seguridad de la Información: Son aquellas acciones que están encaminadas al establecimiento de directrices que permitan alcanzar la confidencialidad, integridad y disponibilidad de la información, así como la continuidad de las operaciones ante un evento que las interrumpa.

• Activo: Recursos con los que cuenta la empresa y que tiene valor, pueden ser tangibles (servidores, desktop, equipos de comunicación) o intangibles (Información, políticas, normas, procedimientos)

• Vulnerabilidad: Exposición a un riesgo, fallo o hueco de seguridad detectado en algún programa o sistema informático.

• Amenaza: Cualquier situación o evento posible con potencial de daño, que pueda presentarse en un sistema.

• Riesgo: Es un hecho potencial, que en el evento de ocurrir puede impactar negativamente la seguridad, los costos, la programación o el alcance de un proceso de negocio o de un proyecto.

- Correo electrónico: El correo electrónico es un servicio de red que permite que los usuarios envíen y reciban mensajes incluyendo textos, imágenes, videos, audio, programas, etc., mediante sistemas de comunicación electrónicos.

5.1.4. Gestión de riesgo en la seguridad informática.

La Gestión de Riesgo es un método para determinar, analizar, valorar y clasificar el riesgo para posteriormente implementar mecanismos que permitan controlarlo. La Gestión de Riesgo se divide en cuatro fases, Análisis, Clasificación, Reducción y Control:

- *Análisis*: En la fase de análisis se determina los componentes del sistema que requieren protección, las vulnerabilidades que lo debilitan y las amenazas que lo ponen en peligro, con el objetivo de revelar su grado de riesgo. Por lo tanto, al identificar las vulnerabilidades y las amenazas del sistema, permitirá conocer los riesgos potenciales que atentan la seguridad del sistema.

- *Clasificación*: En la fase de Clasificación se determina si los riesgos encontrados y los riesgos restantes son aceptables Y justificables.

- *Reducción*: En la fase de Reducción se define e implementa las medidas de protección y de igual forma se sensibiliza y capacita a los usuarios conforme a las necesidades requeridas para tal fin.

- *Control*: En la fase de Control se analiza el funcionamiento, la efectividad yel cumplimiento de las medidas y si es el caso ajustarlas al requerimiento de la empresa u organización.

5.1.5. Elementos de protección

• Firewall: Elemento de protección que sirve para filtrar paquetes (entrada o salida) de un sistema conectado a una red, que puede ser Internet o una Intranet. Existen firewall de software o hardware. Este filtrado se hace a través de reglas, donde es posible bloquear direcciones (URL), puertos, protocolos, entre otros.

• Anti-virus: Programa capaz de detectar, controlar y eliminar virus informáticos y algunos códigos maliciosos (Troyanos, Works, Rootkits, Adware, Backdoor, entre otros).

• Anti-spam: Programas capaz de detectar, controlar y eliminar correos spam.

• Criptografía: Es el arte cifrar y descifrar información con claves secretas, donde los mensajes o archivos sólo puedan ser leídos por las personas a quienes van dirigidos, evitando la interceptación de éstos.

5.1.6. Amenazas técnicas de seguridad.

• Spam: Envío de cualquier correo electrónico, masivo o no, a personas a través de este medio que incluyen temas tales como pornografía, bromas, publicidad, venta de productos, entre otros, los cuales no han sido solicitados por el(los) destinatario(s).

• Ingeniería social: Es la manipulación de las personas para convencerlas de que ejecuten acciones, actos o divulguen información que normalmente no realizan, entregando al atacante la información necesaria para superar las barreras de seguridad.

• Código Malicioso: Hardware, software o firmware que es intencionalmente introducido en un sistema con un fin malicioso o no autorizado. Ejemplo: Troyanos, Works, Spyware, Rootkits, Adware, Backdoor, Cookies, Dialers, Exploit, Hijacker, keyloggers, Pornware, etc.

• Hoax: Es un mensaje de correo electrónico con contenido falso o engañoso y normalmente distribuido en cadena, aparte de ser molesto, congestiona las redes y los servidores de correo, pueden ser intencionales para la obtención de direcciones de correo para posteriormente ser utilizadas como spam. Algunos de los Hoax más conocidos son correos con mensajes sobre virus incurables, temática religiosa, cadenas de solidaridad, cadenas de la suerte, Regalos de grandes compañías, entre otros.

• Suplantación: Hacerse pasar por algo o alguien, técnicamente el atacante se hace pasar por un servicio o correo original.

• Fuga de información: La fuga de información es una problemática que no es ninguna novedad para la seguridad de la información ya que a menudo ocurren casos que aquejan especialmente a las organizaciones, aunque también puede afectar a cualquier individuo en su ámbito personal. La pérdida de información puede ser un inconveniente muy grave para una empresa en caso de no implementar controles para que no suceda una fuga y se deben tener en cuenta medidas en el caso desafortunado que así ocurra.

5.1.7. Herramientas de análisis para páginas web

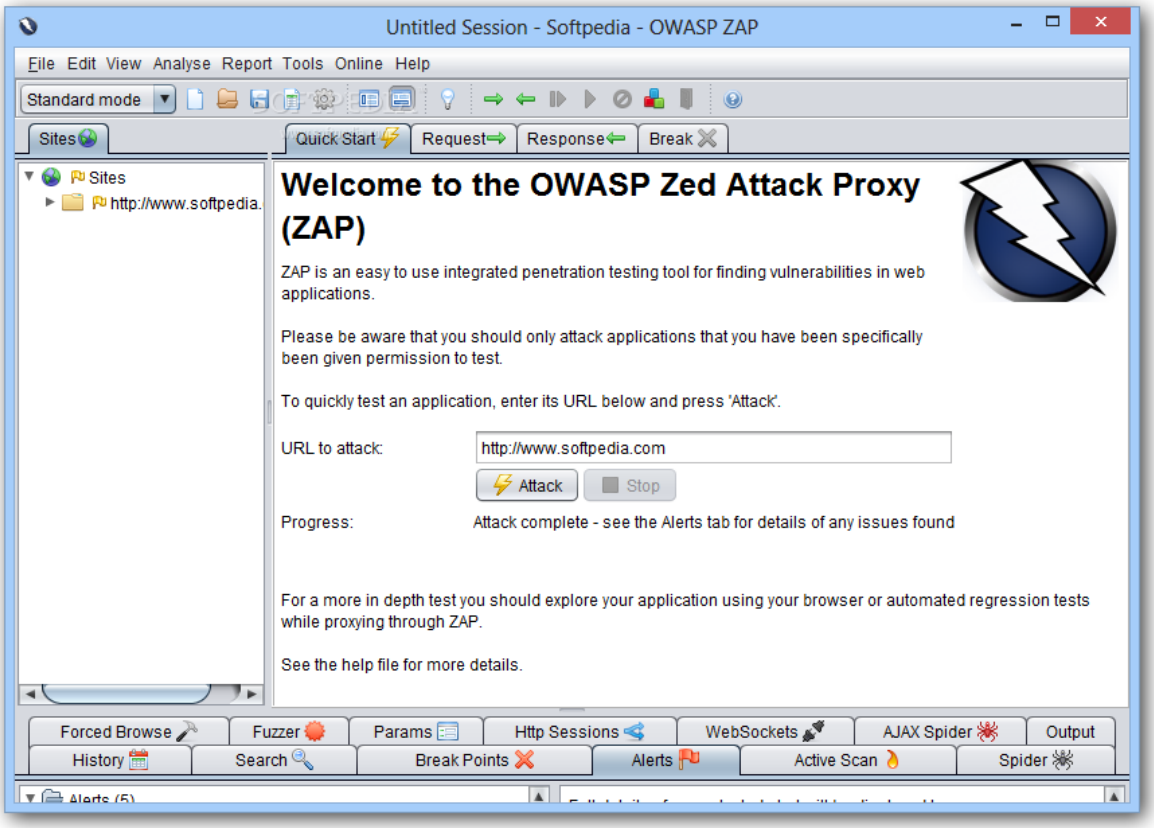
5.1.7.1. Hereramienta Owasp Zap[9]

Una de las herramientas más potentes del programa OWASP es ZAP (Zed Attack Proxy). Esta plataforma está diseñada especialmente para monitorizar la seguridad de las

[9] VELAZCO, Ruben., OWASP ZAP, herramienta para auditar la seguridad de una página web, [En línea], disponible en: https://www.redeszone.net/2015/04/25/seguridad-web-owasp-zap/ , [citado el 25 de Abril de 2015]

aplicaciones web de las compañías, siendo una de las aplicaciones del proyecto más activas en cuanto a auditorías de seguridad.

ILUSTRACIÓN 6: HERRAMIENTA OWASP ZAP



Las principales características de OWASP ZAP son:

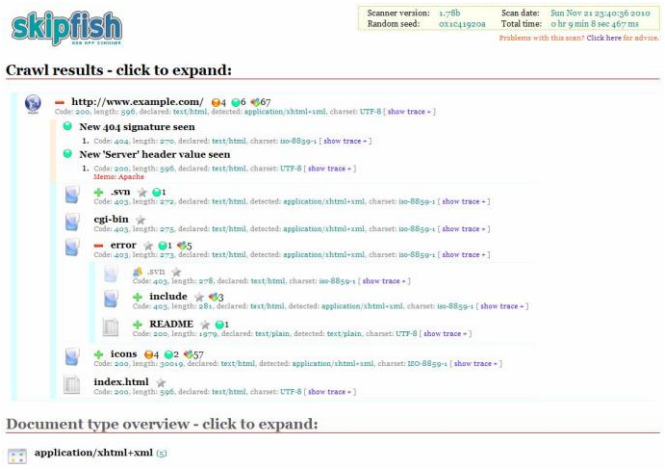
- Herramienta totalmente gratuita y de código abierto.
- Herramienta multi-plataforma, compatible incluso con Raspberry Pi.
- Fácil de instalar, dependiendo únicamente de Java 1.7 o superior.
- Posibilidad de asignar un sistema de prioridades.
- Traducida a más de 12 idiomas, entre ellos, el español.
- Excelente manual de ayuda y gran comunidad en la red.

5.1.7.2. Hereramienta Skipfish[10]

[10] MELON, Luis, 10 herramientas para escanear vulnerabilidades web, [En línea], disponible en: https://ciberseguridad.blog/10-herramientas-para-escanear-vulnerabilidades-web/10 herramientas para escanear vulnerabilidades web, [citado el 17 de Febrero de 2017]

Skipfish rastrea el sitio web y luego revisa cada página buscando varias amenazas de seguridad para después preparar un informe final. Esta herramienta está escrita en C y está muy optimizada para el manejo HTTP y muy pocos recursos de CPU. En la descripción dice que puede manejar fácilmente 2000 solicitudes por segundo sin agregar una carga en la CPU. Utiliza un enfoque heurístico al rastrear y probar páginas web. Esta herramienta también pretende ofrecer alta calidad y menos falsos positivos.

ILUSTRACIÓN 7: HERRAMIENTA SKIPFISH



5.1.7.1. Hereramienta Sucuri[11]

Sucuri es el más popular sitio web gratuito de escáner de malware y seguridad. Se puede hacer una prueba rápida para el Malware, la lista negra del Web site, SPAM inyectado y Defacements. Sucuri limpia y protege tu sitio web contra amenazas en línea y funciona en cualquier tipo de plataformas, incluyendo sitios webs de WordPress, Joomla, Magento, Drupal, phppp, etc.

[11] CACERES, Jesus., 12 herramientas gratuitas en línea para analizar vulnerabilidades de seguridad y malware en sitios web, [En línea], disponible en: http://www.xn--apaados-6za.es/tenemos-que-apanar/internet-tutoriales-y-trucos/71269-herramientas-gratuitas-en-linea-analizar-vulnerabilidades-seguridad-malware-sitios-web.html, [citado el 28 de Diciembre de 2016]

ILUSTRACIÓN 8: HERRAMIENTA SUCURI

5.1.8. Estándares en la seguridad de la información

LA SERIE 27000

ISO/IEC 27000: Conjunto de estándares de seguridad con las mejores prácticas recomendadas en Seguridad de la Información, algunas de ellas son:

- ✓ *ISO 27001: Esta n*orma contiene los requisitos para implantación del sistema de gestión de seguridad de la información (SGSI). Es certificable.

- ✓ *ISO 27002: Guía* que describe los objetivos de control y controles recomendables en la seguridad de la información.

- ✓ *ISO 27005:* Establece las directrices para la Gestión del riesgo en la seguridad dela información.

- ✓ *ISO 27007: G*uía de auditoría de un Sistema de Gestión de Seguridad en la Información.

- ✓ *ISO 27032:* Guía relativa a la Ciberseguridad. Que se encarga de proteger la información digital en los sistemas interconectados. está comprendida dentro de la seguridad de la información.

- ✓ ISO 27001: La información es un bien intangible importante para el correcto funcionamiento de cualquier empresa. Por lo tanto es importante que las empresas establezcan un mecanismo que realice esta tarea de forma clara, sistemática, documentada basada en objetivos precisos de seguridad y una valoración de los riesgos a los que está expuesta la información de la organización.

A continuación, se relacionan las distintas normas que componen la Serie ISO 27000:

En 1995 la British Standards Institution publica la norma BS 7799 con el objeto de

proporcionar a cualquier empresa un conjunto de buenas prácticas para la gestión de la seguridad de la información.

El Estándar para la seguridad de la Información ISO 27001 fue diseñado para proveer un modelo para el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejoras de todos los procesos que involucran la Seguridad de la Información en una organización por medio del Sistema de la Gestión de la Seguridad de la Información (SGSI).La ISO 27001 adopta el modelo del proceso (PDCA) Planear Hacer Chequear Actuar, que se puede aplicar a los procesos SGSI.

Las actividades que se llevan a cabo en la planificación, implementación, seguimiento y mejora continua son las siguientes:

PLANIFICACIÓN

Definir el alcance del SGSI, se recomienda iniciar por un alcance limitado y que no abarque toda la organización.

Definir política de seguridad incluyendo un marco general y los objetivos de seguridad de la información de la organización. Es importante alinear la gestión de riesgos con los requisitos legales y contractuales en cuanto a seguridad de la empresa, estableciendo criterios de evaluación aprobados por la Dirección.

Se debe definir desde el inicio una metodología para la evaluación de riesgos, esta evaluación debe ser apropiada para el SGSI y las necesidades de la organización.

IMPLEMENTACIÓN

- Definir el plan de tratamiento de riesgos: Que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.
- Implantar plan de tratamiento de riesgos: Con la meta de alcanzar los objetivos de control identificados.
- Implementar los controles: Todos los que se seleccionaron en la fase anterior.
- Formación y concienciación: De todo el personal en lo relativo a la seguridad de la información.

  Desarrollo del marco normativo necesario: normas, manuales, procedimientos e instrucciones.

- Gestionar las operaciones del SGSI y todos los recursos que se le asignen.

- Implantar procedimientos y controles de detección y respuesta a incidentes de seguridad.

SEGUIMIENTO

- Ejecutar procedimientos y controles de monitorización y revisión: En esta etapa se detectan errores en resultados de procesamiento e incidentes de seguridad.

- Revisar regularmente la eficacia del SGSI: Esta revisión se hace en función de los resultados de auditorías de seguridad, incidentes, mediciones de eficacia, sugerencias y feedback de todos los interesados.

- Medir la eficacia de los controles: Se realiza para verificar que se cumple con los requisitos de seguridad.

- Revisar regularmente la evaluación de riesgos: Cualquier cambio en la organización, tecnología, procesos y objetivos de negocio, amenazas, eficacia de los controles o el entorno tienen una influencia sobre los riesgos evaluados, el riesgo residual y el nivel de riesgo aceptado.
- Realizar regularmente auditorías internas: Con el fin de determinar si los controles,
- procesos y procedimientos del SGSI mantienen la conformidad con los requisitos de ISO 27001.

MEJORA CONTINUA

- Implantar mejoras: Poner en marcha todas las mejoras que se hayan propuesto en la fase anterior.

- Acciones correctivas: Para solucionar no conformidades detectadas.

- Acciones preventivas: Para prevenir potenciales no conformidades.

- Comunicar las acciones y mejoras: A todos los interesados y con el nivel adecuado de detalle.

- Asegurarse de que las mejoras alcanzan los objetivos pretendidos: La eficacia de cualquier acción, medida o cambio debe comprobarse siempre.

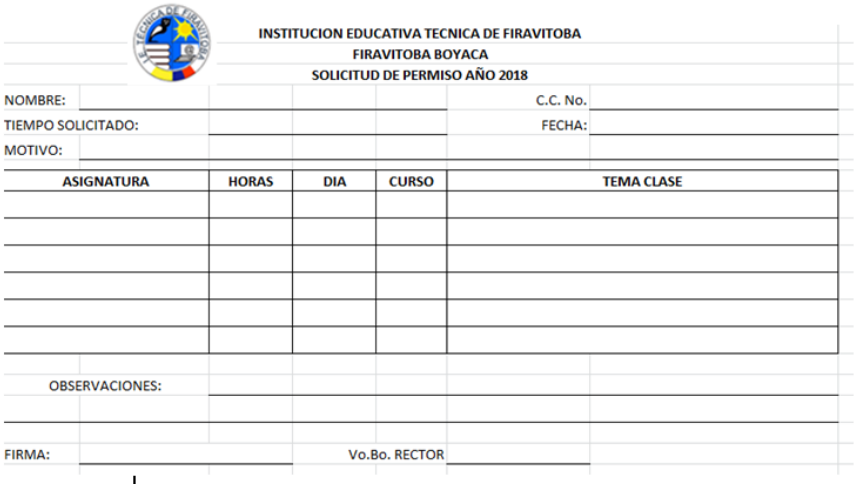
5.2. MARCO CONCEPTUAL

La página web que se diseñó para proteger la información y seguridad en la Institución Educativa Técnica de Firavitoba está diseñada bajo el lenguaje de programación HTML (Lenguaje de marcas de hipertexto). Está conformada por: Una página de inicio o home page, que a su vez incluye un sub menú. El logo y nombre de la Institución Educativa. En el menú encontramos los siguientes botones o activos de información.

- Botón inicio: Se da la Bienvenida, se explica el tipo de educación que se brinda, la ubicación municipio y Departamento. Su filosofía institucional, Perfil del estudiante y contáctenos.
- Botón Localidad: En este botón nos da la opción de hacer un recorrido con google maps de la Institución Educativa.
- Botón Nosotros: Contiene un Submenu de Visión, Misión, símbolos, manual de convivencia, PEI y reseña histórica.
- Botón Directivos: Breve descripción de cada uno de los directivos de la institución
- Botón Docentes: Breve descripción de cada uno de los docentes de la institución, Acompañada de las fotografías de cada uno de los docente
- Botón Estudiantes: Breve descripción del número de estudiantes de la institución, uniformes utilizados
- Botón Especialidades: Breve resumen de las especialidades Articuladas con el Sena, perfil y requisitos.
- Botón Formatos: Da la opción de descargar los formatos que deben utilizar los profesores y estudiantes cuando solicitan un permiso.
- Botón Mallas: Breve descripción del PEI de cada área.
- Botón Sedes: Breve descripción de cada una de las sedes de la Institución.
- Botón Eventos: Se resalta los eventos de la Institución Educativa como deportivos, culturales y técnicos.

Dentro de los activos de la información que hace referencia a los formatos institucionales se encuentran los permisos tanto para docentes como estudiantes, los cuales evidencian y permiten gestionar el permiso o excusa de la inasistencia a la institución Educativa, explicando los motivos de su respectiva ausencia, los cuales son remitidos en físico a la dependencia de rectoría y reposados en el archivo del solicitante.

ILUSTRACIÓN 9 FORMATO PERMISOS I.E. FIRAVITOBA



INSTITUCION EDUCATIVA TECNICA DE FIRAVITOBA
FIRAVITOBA BOYACA
SOLICITUD DE PERMISO AÑO 2018

NOMBRE: _____ C.C. No. _____
TIEMPO SOLICITADO: _____ FECHA: _____
MOTIVO: _____

ASIGNATURA	HORAS	DIA	CURSO	TEMA CLASE

OBSERVACIONES: _____

FIRMA: _____ Vo.Bo. RECTOR _____

La información suministrada por la página web de la institución educativa a la comunidad en generar es un activo muy importante, que se encuentra a disposición de cualquier persona, una de las desventajas es que no cuenta con accesos de seguridad a los usuarios que constantemente visitan la página, y se ve expuesta a riesgos de descarga de información, copias, entre otras.

El servidor donde se encuentra alojada la página web de la Institución Educativa es www.miarrroba.com, este servidor es gratuito, las características del espacio web son:

- ✓ 500 MB de espacio web
- ✓ Transferencia ilimitada
- ✓ Soporte del lenguaje de scripts PHP5
- ✓ Acceso a los ficheros del Espacio, usando tanto un cliente FTP normal como usando nuestro Administrador WebFTP.
- ✓ Adicionalmente el servidor ofrece 5 GB de capacidad según el contenido de la página y las visitas realizadas
- ✓ Potente administrador WEB el cual permite subir, actualizar, renombrar y borrar archivos y directorios del espacio WEB desde cualquier computador que tenga acceso a internet y sin necesidad de FTP.

Se intentó realizar el análisis de vulnerabilidades al servidor www.miarrroba.com bajo la herramienta Owasp - zap pero no fue posible, esta metodología está diseñada para realizar escaneo de vulnerabilidades únicamente a páginas web.

Los servidores gratuitos no son recomendables para alojar páginas web empresariales ya que no cuentan con un sistema de seguridad de la información al 100%. Como el espacio es gratuito si algún día desaparece la página Web, no se puede reclamar a nadie. Debido a lo anterior constantemente se debe realizar copia de seguridad ya que el hosting no ofrece este

servicio, no brindan soporte. En ocasiones añaden publicidad en la página sin poder controlar el tipo de publicidad.

En conclusión es importante y recomendable que la Institución Educativa adquiera un hosting de Pago ya que con este van a tener muchas garantías. Las características con las cuales se puede tener acceso al servidor son:

* 20.000MB (20GB) de espacio
* 20 cuentas de Correo Electrónico Corporativas
* Alojamiento para Sitio Web con soporte Flash/PHP/MySQL
* Soporte Técnico y asesoría durante todo el año de servicio.
* Constructor de sitios.
* Email Marketing.

El plan más recomendado actualmente es el ColHost2. Este plan lo pueden adquirir en el Hosting Colombia ya que es una empresa recomendable por su cumplimiento y responsabilidad.

5.3. MARCO LEGAL

LEY 1273 DE 2009[12]

Los principios fundamentales de la seguridad son la confidencialidad, la integridad y la disponibilidad de la información. Para preservar estos principios el Congreso de Colombia aprobó la Ley 1273 de 2009, que procura proteger la información, los datos y la conservación de los sistemas que utilicen tecnologías de la información y la Comunicación.

La ley tiene en cuenta los siguientes artículos, que son indispensables y necesarios tener en cuenta para la protección de la información:

- ✓ Acceso abusivo a un sistema informático.
- ✓ Obstaculización ilegítima de sistema informático o red de telecomunicación.
- ✓ Interceptación de datos informáticos.
- ✓ Daño informático.

  Uso de software malicioso.

[12] Secretaría del Senado, Ley1273 de 2009 [En línea], <http://www.secretariasenado.gov.co/senado/basedoc/ley/2009/ley_1273_2009.html>, [Citado el 3 de Octubre de 2011]

- ✓
- ✓ Violación a datos personales.
- ✓ Suplantación de sitios web para capturar datos personales.

Esta ley es de vital importancia como apoyo legal para proteger la información de las organizaciones o personas, ya que no están exentas a estos problemas y a menudo se presentan. Además, conocer las multas y penas que acarrean estas violaciones, viabilizan un mecanismo de respuesta rápido y efectiva de las organizaciones o personas para defender y proteger su activo más importante que es la información o los datos que procesa toda organización.

LEY ESTATUTARIA 1581 DE 2012:[13]

(Octubre 17) Reglamentada parcialmente por el Decreto Nacional 1377 de 2013.

Por la cual se dictan disposiciones generales para la protección de datos personales.

EL CONGRESO DE COLOMBIA

DECRETA:

TÍTULO I

OBJETO, ÁMBITO DE APLICACIÓN Y DEFINICIONES

Artículo 1°. Objeto. La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

Artículo 2°. Ámbito de aplicación. Los principios y disposiciones contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada.

La presente ley aplicará al tratamiento de datos personales efectuado en territorio colombiano o cuando al Responsable del Tratamiento o Encargado del Tratamiento no

[13] Ley Estatutaria 1581 de 2012, [En línea], http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4998 [Citado por Diario Oficial 48587 de octubre 18 de 2012]

establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales.

El régimen de protección de datos personales que se establece en la presente ley no será de aplicación:

a) A las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico.

Cuando estas bases de datos o archivos vayan a ser suministrados a terceros se deberá, de manera previa, informar al Titular y solicitar su autorización. En este caso los Responsables y Encargados de las bases de datos y archivos quedarán sujetos a las disposiciones contenidas en la presente ley;

b) A las bases de datos y archivos que tengan por finalidad la seguridad y defensa nacional, así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo;

c) A las Bases de datos que tengan como fin y contengan información de inteligencia y contrainteligencia;

d) A las bases de datos y archivos de información periodística y otros contenidos editoriales;

e) A las bases de datos y archivos regulados por la Ley 1266 de 2008;

f) A las bases de datos y archivos regulados por la Ley 79 de 1993.

Parágrafo. Los principios sobre protección de datos serán aplicables a todas las bases de datos, incluidas las exceptuadas en el presente artículo, con los límites dispuestos en la presente ley y sin reñir con los datos que tienen características de estar amparados por la reserva legal. En el evento que la normatividad especial que regule las bases de datos exceptuadas prevea principios que tengan en consideración la naturaleza especial de datos, los mismos aplicarán de manera concurrente a los previstos en la presente ley.

Artículo 3°. Definiciones. Para los efectos de la presente ley, se entiende por:

a) Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales;

b) Base de Datos: Conjunto organizado de datos personales que sea objeto de Tratamiento;

c) Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables;

d) Encargado del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento;

e) Responsable del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos;

f) Titular: Persona natural cuyos datos personales sean objeto de Tratamiento;

g) Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

6. DISEÑO METODOLOGICO PRELIMINAR

6.1. TIPO DE INVESTIGACIÓN

El presente proyecto es una investigación tipo aplicada ya que se busca describir situaciones y eventos poniendo de manifiesto la estructura de los fenómenos en estudio para el caso la seguridad informática en páginas web. Este tipo de investigación presenta en forma detallada las características de su objeto de estudio.

Los intentos de encontrar vulnerabilidades en aplicaciones web por parte de atacantes se han incrementado constantemente, por eso es necesario que se utilicen aplicaciones que sigan un modelo de seguridad que disminuyan dichas vulnerabilidades.

Actualmente la mayoría de las aplicaciones son ejecutadas en ambientes Web, esto ocasiona que los sistemas y la información de las empresas se enfrenten a cierto tipo de vulnerabilidades al ser publicados en la Web. Al hacer uso de un modelo de seguridad desde el planteamiento del sistema hasta su implementación, se asegura que el sistema será confiable, y sobre todo que cumplirá con las necesidades establecidas por su administrador.

6.2. MÉTODO O METODOLOGÍA

Para llevar a cabo el proceso de análisis y evaluación de la página web de la Institución Educativa, se emplea el siguiente método basado bajo el esquema del ciclo de mejora continua de la ISO 27000 PHVA (Planear, Hacer, Verificar Y Actuar)

La seguridad en aplicaciones web requiere:

I FASE INICIAL:

1. Estudio preliminar.

2. Diagnóstico: Verificar el estado físico (Hardware y/o recursos) y Lógico (Software, programas, aplicaciones) de la empresa.

3. Organización y distribución de tareas según lo obtenido en el diagnóstico.

II FASE EJECUCION:

4. Realizar un seguimiento paso a paso de la información que suministra la institución a la Comunidad educativa por medio del tráfico de la red.

5. Identificar las vulnerabilidades y riesgos a la página web o software que se maneja

como: seguridad, comunicación, información, integridad, productividad, ancho de banda, teniendo en cuenta la mayoría de técnicas de ataques, con la finalidad mantener la integralidad, disponibilidad y seguridad de la página web.

El análisis de vulnerabilidades se hará utilizando la herramienta de Owasp zap que consiste en el análisis de la ejecución de herramientas en la búsqueda de vulnerabilidades, este enfoque conocido como pruebas de intrusión, el código fuente no se encuentra disponible y el funcionamiento interno de la aplicación web no es conocida por el auditor.

6. Utilizar métodos de autenticación, validación de datos y manejo de sesiones que permita limitar accesos a personas no autorizadas que puedan afectar los movimientos informáticos de la Institución educativa.

III Fase: Pruebas:

7. Realizar las respectivas pruebas de validación a la página principal y páginas de enlace como lo es la seguridad de código fuente y consulta esperada ya sea magnética o impresa.

IV Fase: Final:

8. Recomendaciones: tener en cuenta los diferentes ataques y riesgos presentados en la página web y buscar soluciones tal como alojamiento de la página en un Hosting seguro, utilizar técnicas de seguridad para proteger los datos de la página web y atender a los a los requerimientos del administrador del sistema, quien es el encargado del ingreso, administración y alimentación de la página web.

Al ejecutar los pasos anteriores se obtiene una disminución de vulnerabilidades de los sistemas, menos propensa a recibir ataques, lo cual garantiza la disminución de costos y tiempo en los movimientos informáticos que efectúa la Institución educativa. Y de esta forma prevenir el mal uso de la información que se procesa. Ya que al implementar un modelo de seguridad se obtiene mayor confianza en el manejo de la información de cualquier Entidad ya sean instituciones o Empresa.

El sistema de seguridad informática debe garantizar el rango más amplio posible de la información para que pueda ser visualizada por personas de la Institución y de la comunidad educativa en general.

6.2.1. Enfoque caja negra:

Básicamente consiste en el análisis de la ejecución de herramientas en la búsqueda de vulnerabilidades. Este enfoque también es conocido como pruebas de intrusión, el auditor no conoce el funcionamiento interno de la aplicación web (el código fuente no está disponible) y utiliza técnicas de pruebas automatizadas, que son capaces de generar y

enviar datos secuenciales o aleatorios a una aplicación web o a las solicitudes HTTP, esta técnica es conocida también como Fuzzing.[14]

La prueba de Intrusión será llevada a cabo en las siguientes fases:

- Recolección de Información.
- Mapeo de la red.
- Identificación de vulnerabilidades.
- Intrusión.
- Presentación del reporte.

Recolección de información: En esta fase se recolecta toda la información posible (desde Internet, periódicos, anuncios) de la organización que se quiere auditar, como, correos, direcciones, nombres, proveedores, infraestructura, etc. Con el fin de hacer un mapa general de la organización.

Mapeo de la red: En esta fase se identifica que servicios y puertos tiene abierto el servidor Web donde se encuentra alojada la aplicación Web, este proceso puede hacerse con la herramienta ***nmap***. Cuando se empieza a analizar la red se revisa la seguridad tanto física como lógica, ya que cualquiera de las dos puede ser un hueco de seguridad para vulnerar el sistema.

Identificación de vulnerabilidades: En esta fase se usan las herramientas de pruebas de intrusión mencionadas anteriormente, aunque si se identifican algunas herramientas adicionales, éstas pueden utilizarse.

Intrusión: Una vez encontradas las vulnerabilidades, se descartan cuales son falsos positivos. Luego de haberlas clasificado, explotarlas y revisar si el sistema ha sido comprometido.

Presentación de Reporte o informe: Esta fase es la más importante, debido que con ella se demuestra que el sistema es o no seguro.

El reporte debe contener:

Fecha.

Duración de las pruebas de Intrusión.

Persona responsable de las pruebas de Intrusión.

Vulnerabilidades clasificadas por categoría e impacto.

[14] VIEIRA, Marco., ANTUNES, Nuno., MADEIRA, Henrique. “Using Web Security Scanners to in Web Services”. IEEECISUC, Departament of informatics Engineering Detect Vulnerabilities” University of Coimbra, Portugal, 2009.

Puntos por donde se logró el acceso.

6.2.2. Enfoque caja blanca:

La esencia de este enfoque es analizar el código fuente en búsqueda de vulnerabilidades. Esto puede traer una serie de complicaciones si el código es muy complejo, debido a que se dificulta encontrar los problemas de seguridad.

Por lo tanto se plantea hacer estos análisis en el ciclo de desarrollo del Software (SDLC) para quitarle complejidad a éste problema, en conjunto con el Sistema de Gestión de la seguridad de la Información (la norma ISO 27001), que es el estándar de facto que las organizaciones deben certificar para demostrar que ofrecen seguridad en la información de sus clientes, además de darle una gestión eficiente a los riesgos y vulnerabilidades. A continuación se citan consideraciones adicionales a tener en cuenta en la fase de desarrollo. [15]

Para el desarrollo de esta metodología se utilizara el enfoque de caja blanca ya que ofrece seguridad en la información para los usuarios, se centra en el escaneo o recorrido profundo al código fuente, detectando posibles fallas o vulnerabilidades que se presentan dentro de la página web impidiendo la seguridad de la información. Se aplica a las unidades de software, su función es comprobar los flujos de ejecución dentro de cada unidad, realizando pruebas de flujo de datos y control en el direccionamiento de la información.

6.3. VARIABLES E INDICADORES:

Variable1 Nivel de seguridad de la página web.

Nivel de seguridad bajo.

La página web no cuenta actualmente con técnicas apropiadas para proteger la seguridad, por esta razón diariamente está expuesta a varias amenazas.

---

[15] ASCENCIO, Martha., MORENO, Pedro., Desarrollo de una Propuesta Metodológica para Determinar la Seguridad en una Aplicación Web. [En línea], http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/2511/0058A811.pdf?sequence=1 >, [Citado el 15 de Octubre de 2011] Pereira, 2011.

6.4. HIPÓTESIS

Hipótesis de tipo investigación (Hi).

Descriptiva No existen mecanismos para la detección y remediación de vulnerabilidades y riesgos en la información de la página web de la IE de Firavitoba.

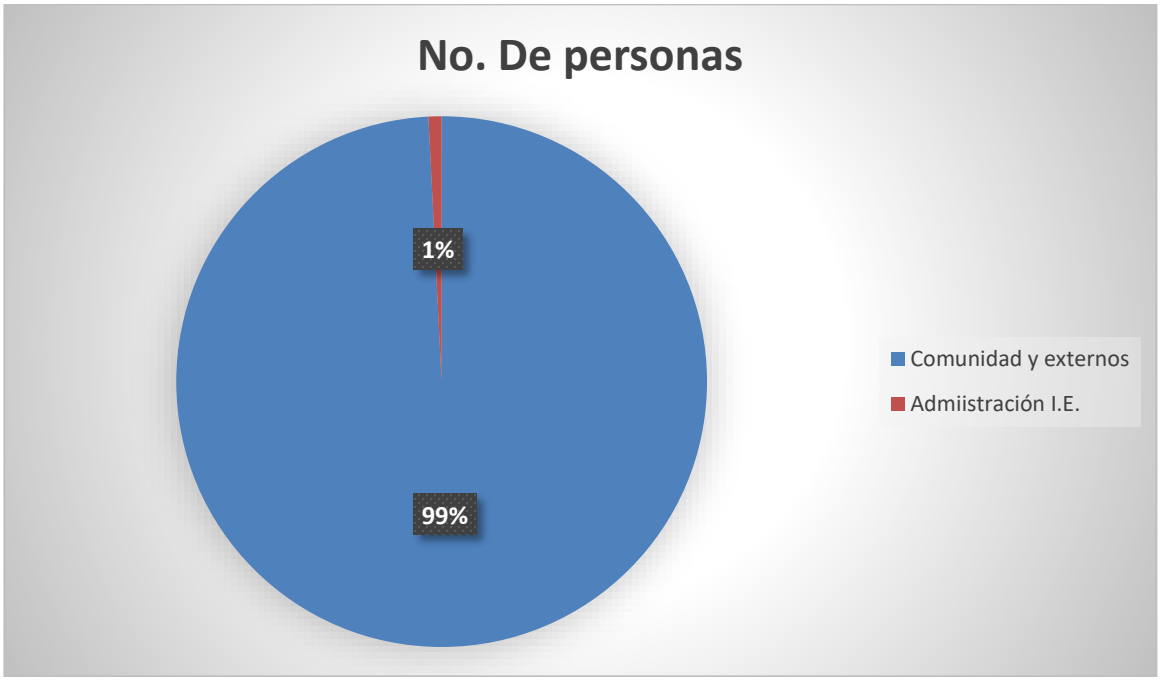
6.5. POBLACIÓN Y MESTRA

La población está conformada por la Comunidad educativa de Firavitoba y personas externas, y la muestra por la parte administrativa de la I.E.

Población y comunidad: 1500

Administración: 12

ILUSTRACIÓN 10: POBLACIÓN Y MUESTRA I.E.



6.6. TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

Principalmente la técnica e instrumento para la recolección de la información será la encuesta, puesto que se quiere captar la opinión de los miembros de la empresa, ya que para ellos es a quienes va dirigido el proyecto, así pues, una encuesta llenaría todos los vacíos de información que tenemos respecto a los riesgos y vulnerabilidades de la web.

Se usaran formatos para la encuesta, en donde se estipulen las preguntas con sus respectivas respuestas (si o no), lo que facilita la tabulación de los datos, y las opiniones más unificadas y más precisas a la hora de hablar de seguridad en aplicaciones web.

Formato de encuesta seguridad en la página web.

ENCUENSTA SEGURIDAD EN LA PAGINA WEB DE LA I.E. TECNICA DE FRAVITOBA

TIPO DE USUARIO: _____

FECHA DE DILIGENCIAMIENTO: _____

Lea detenidamente cada pregunta y responda con una X Si cumple o No.

1. ¿Cuando consulta la página de la empresa los enlaces se encuentran bien direccionados? ☒Si ☐No
2. ¿La página web la puede ejecutar sin ningún problema sobre cualquier navegador de internet? ☐Si ☐No
3. ¿Al consultar la página web se puede realizar copia de la información? ☐Si ☐No
4. ¿La información que suministra la página web es clara? ☐Si ☐No
5. ¿Accede periódicamente a la página Web de la I.E.? ☐Si ☐No

Gracias…

ILUSTRACIÓN 11: ENCUESTA PÁGINA WEB

ENCUENSTA SEGURIDAD EN LA PAGINA WEB DE LA I.E. TECNICA DE FRAVITOBA

TIPO DE USUARIO: _____

FECHA DE DILIGENCIAMIENTO: _____

Lea detenidamente cada pregunta y responda con una X Si cumple o No.

1. ¿Cuando consulta la página de la empresa los enlaces se encuentran bien direccionados? ☒Si ☐No
2. ¿La página web la puede ejecutar sin ningún problema sobre cualquier navegador de internet? ☐Si ☐No
3. ¿Al consultar la página web se puede realizar copia de la información? ☐Si ☐No
4. ¿La información que suministra la página web es clara? ☐Si ☐No
5. ¿Accede periódicamente a la página Web de la I.E.? ☐Si ☐No

Gracias…

Se aplicó la encuesta al 100% de la muestra, correspondiendo a 12 personas encuestadas, y los resultados obtenidos se relacionan a continuación:

ILUSTRACIÓN 12: TABULACIÓN PREGUNTA NO. 1

ILUSTRACIÓN 13: TABULACIÓN PREGUNTA NO. 2

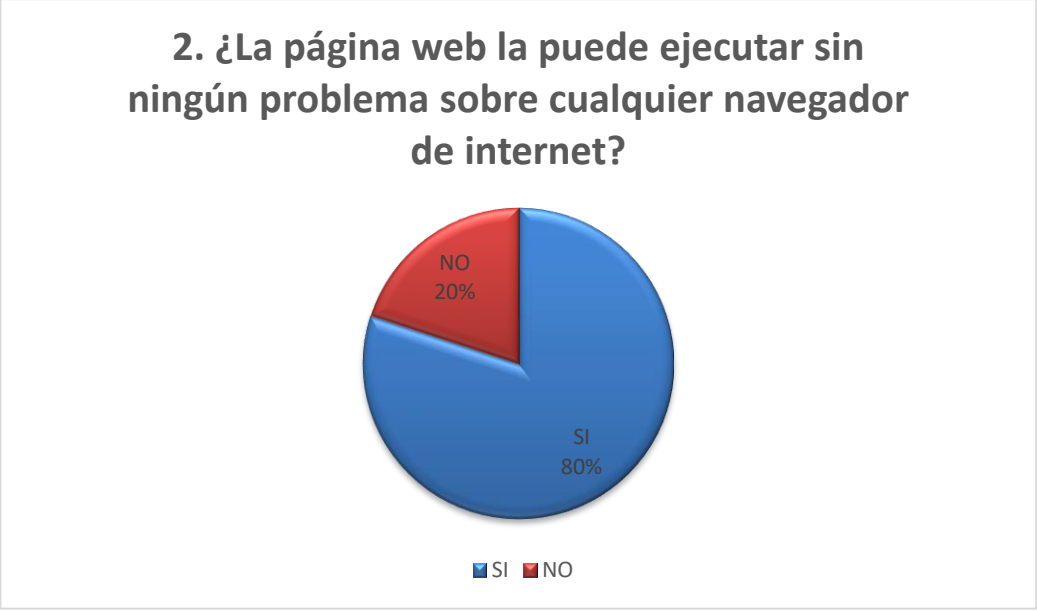


ILUSTRACIÓN 14: TABULACIÓN PREGUNTA NO. 3

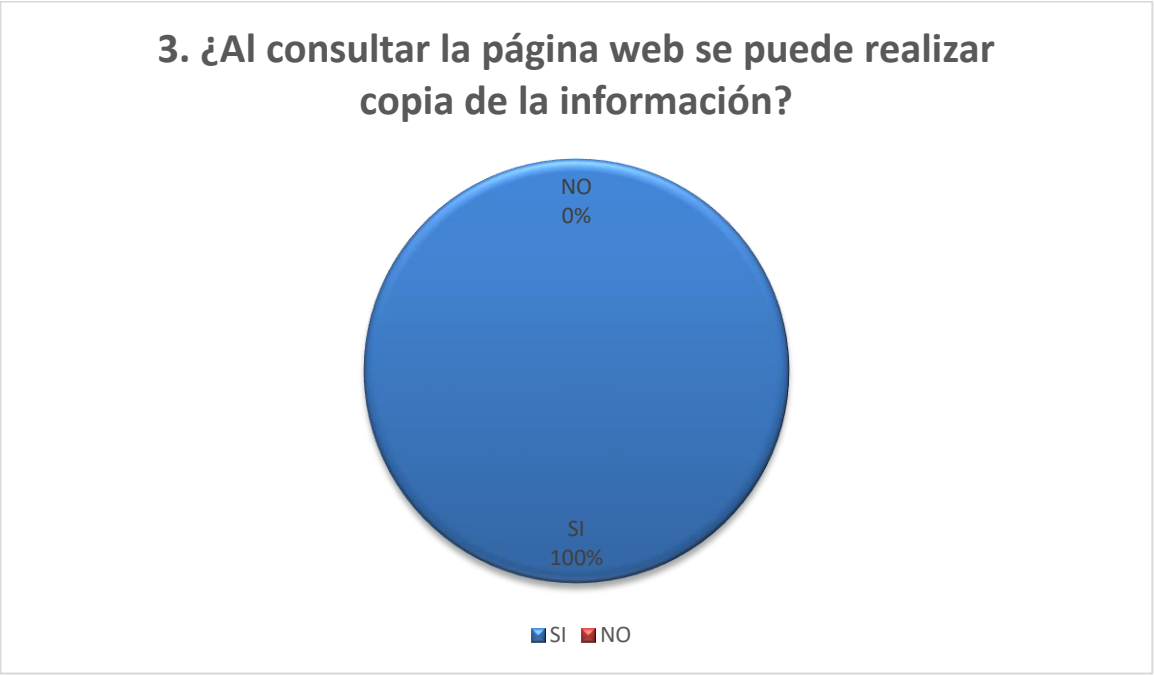


ILUSTRACIÓN 15: TABULACIÓN PREGUNTA NO. 4

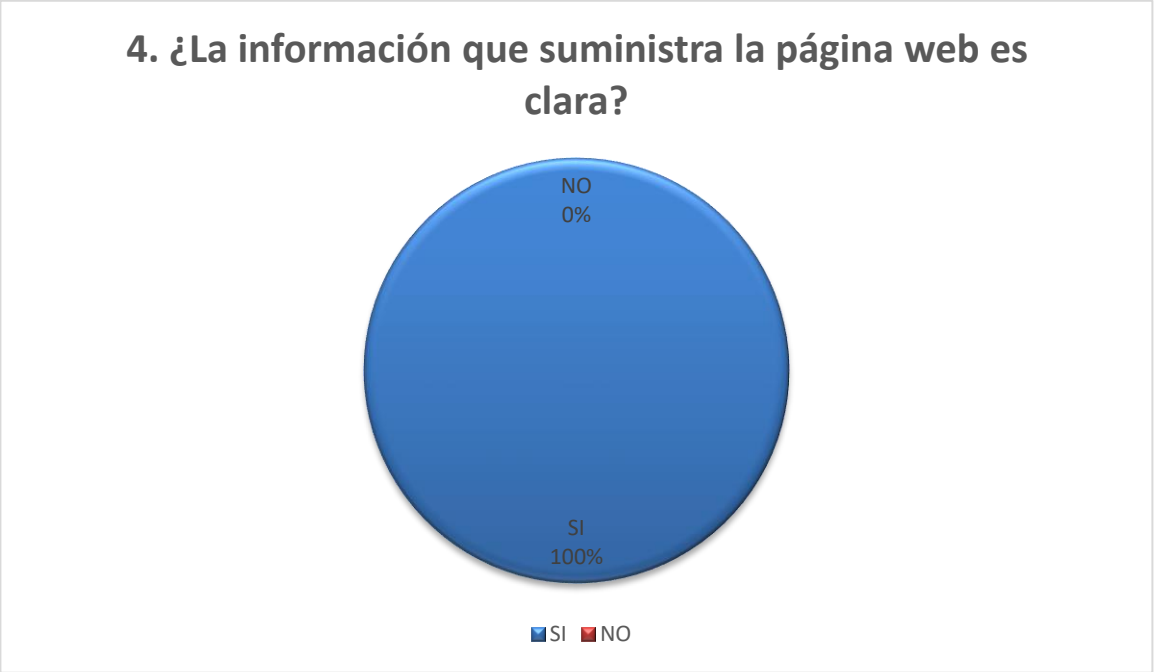
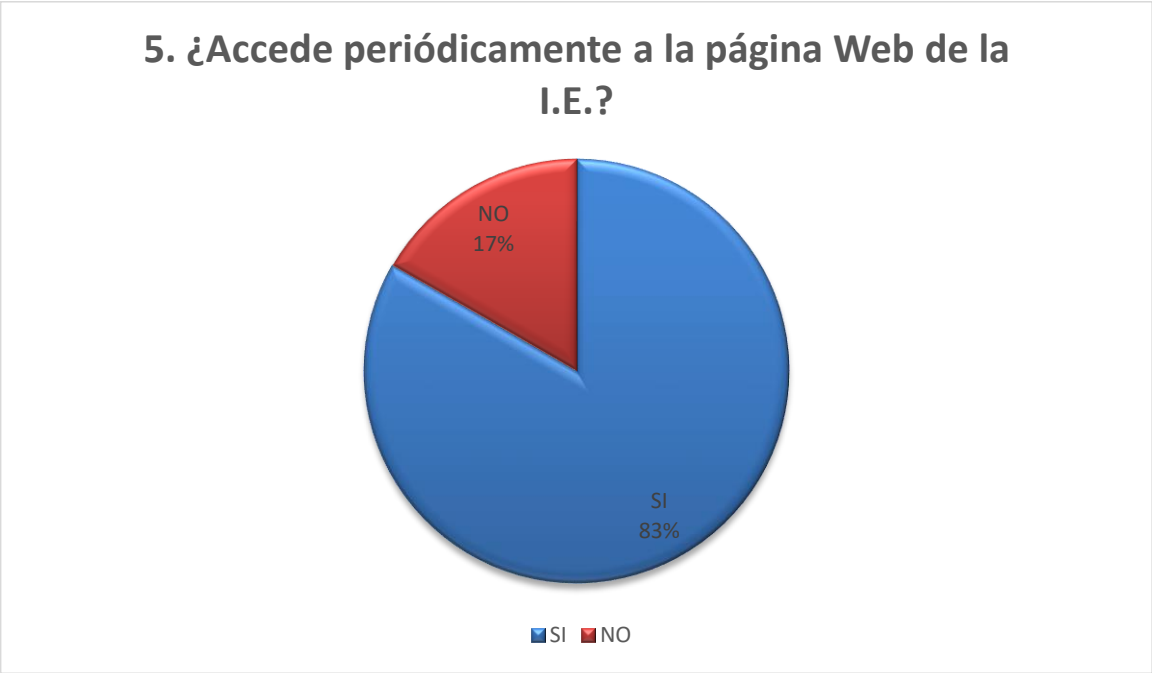


ILUSTRACIÓN 16: TABULACIÓN PREGUNTA NO. 5



7. ESQUEMA TEMÁTICO

7.1. DESCRIPCIÓN DE LA PÁGINA WEB.

Teniendo en cuenta que la página web de la institución educativa Técnica de Firavitova se encuentra publicada en el Host gratuito miarriba.com.

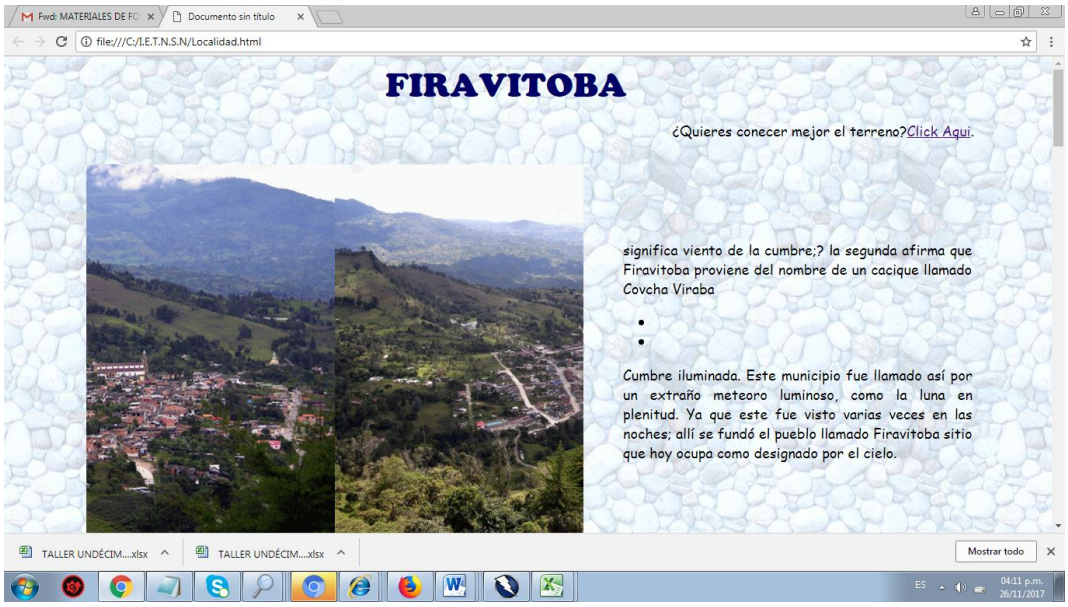
Se verifican los enlaces a cada página de acceso donde presenta detalladamente información importante de la institución tales como:

Botón de inicio: encontramos la ubicación de la institución educativa, los servicios que presta, la filosofía institucional y el perfil del estudiante.

ILUSTRACIÓN 17: VENTANA PRINCIPAL PÁGINA WEB

Botón de localidad: presenta una descripción del nombre de la institución según el municipio donde se encuentra ubicada, nombre fundador, clima, su agricultura e información acerca del terreno y sus límites.

ILUSTRACIÓN 18: LOCALIDAD PÁGINA WEB

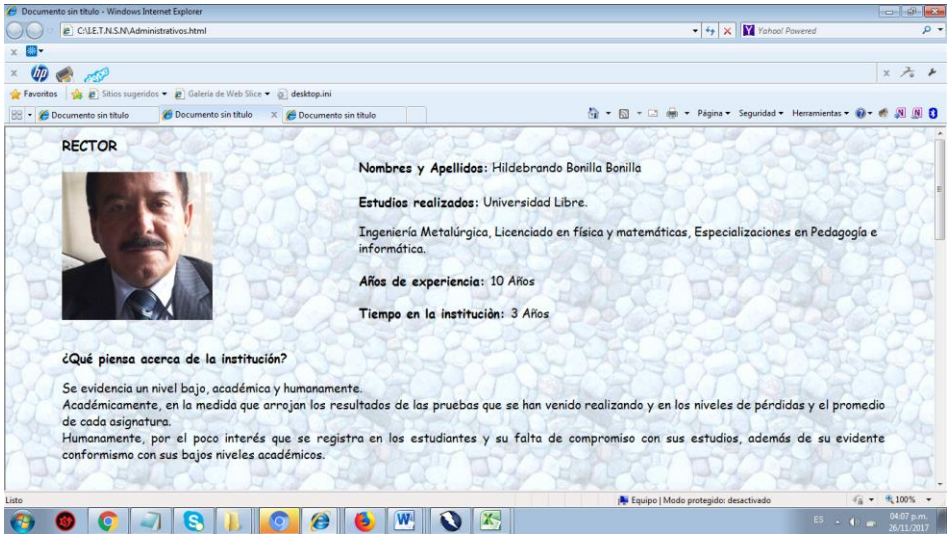


Botón Nosotros: en este botón se encuentra un menú desplegable donde se observa Misión, Visión; Símbolos, Manual de convivencia, PEI y reseña histórica de la IE.

Ilustración 19: NOSOTROS PÁGINA WEB

Botón Directivos: se encuentra la foto del Rector Hildebrando Bonilla Bonilla, junto con su Perfil y dos interrogantes sobre la IE.

ILUSTRACIÓN 20: DIRECTICTIVOS PÁGINA WEB



Botón Docentes: se describe las seis sedes con las cuales cuenta la IE y los docentes a cargo de cada una.

ILUSTRACIÓN 21: DOCENTES PÁGINA WEB

Botón estudiantes: describe el número de estudiantes que existe en cada sede, junto con un submenú donde detalla el uniforme y número de estudiantes actuales.

ILUSTRACIÓN 22: ESTUDIANTES PÁGINA WEB

Botón especialidades: resume la información correspondiente a la especialidad que se encuentra articulada con el SENA: Técnico en Sistemas.

ILUSTRACIÓN 23: ESPECIALIDADES PÁGINA WEB

Botón formatos: presenta la opción de descarga de formatos de permisos manejados dentro de la IE. Se manejan 2 formatos: estudiantes, docentes y administrativos.

ILUSTRACIÓN 24: FORMATOS PÁGINA WEB

Botón Mallas: se encuentra el plan de área de cada materia relacionada con todos lo grados, y permite la descarga de cada plan de área.

ILUSTRACIÓN 25: MALLAS - PLA DE AREA PÁGINA WEB

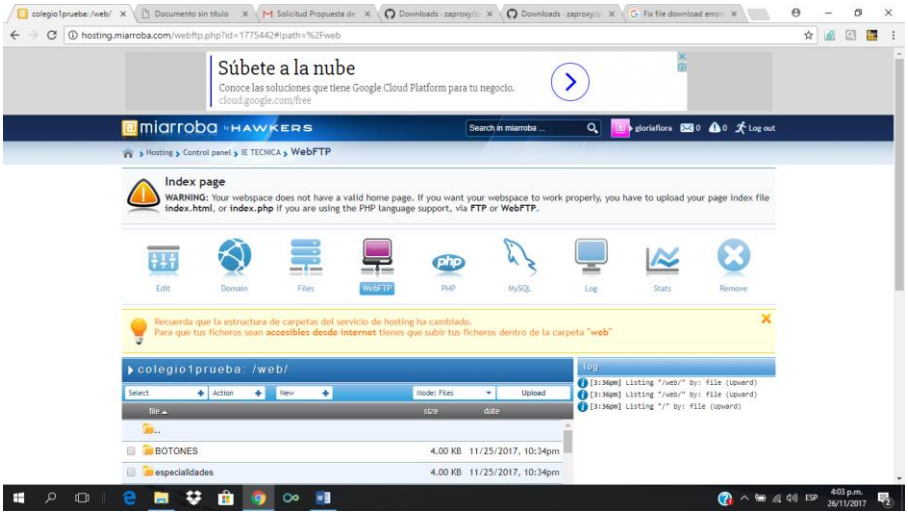
Botón Sedes: describe cada una de las sedes con su respectiva foto, actualmente cuenta con 6 sedes ubicadas en zona urbana y rural.

ILUSTRACIÓN 26: SEDES PÁGINA WEB

7.2. VERIFICACIÓN DEL SITIO WEB.

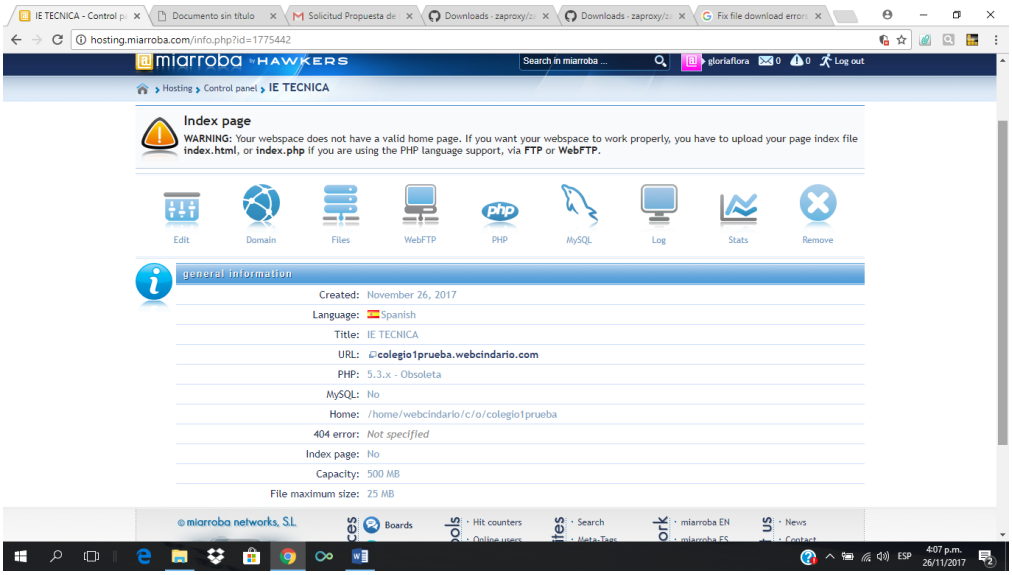
Se solicitó a la Institución Educativa el permiso para acceder al espacio web. Nos suministraron la dirección del servidor gratuito: www.miarroba.com, la clave y contraseña de acceso:

ILUSTRACIÓN 27: SITIO WEB MIARROBA.COM



Se verifica el dominio creado:

ILUSTRACIÓN 28: DOMINIO SITIO WEB



Se corrobora los insumos subidos al dominio como son las carpetas con sus páginas, imágenes y archivos.

ILUSTRACIÓN 29: INSUMOS DOMINIO1

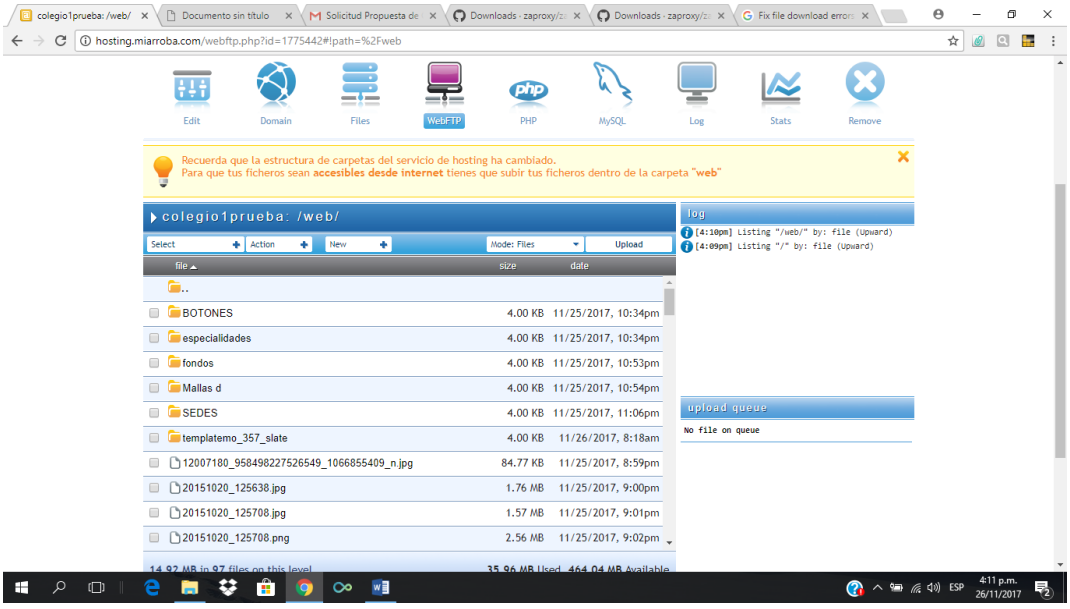


ILUSTRACIÓN 30: INSUMOS DOMINIO2

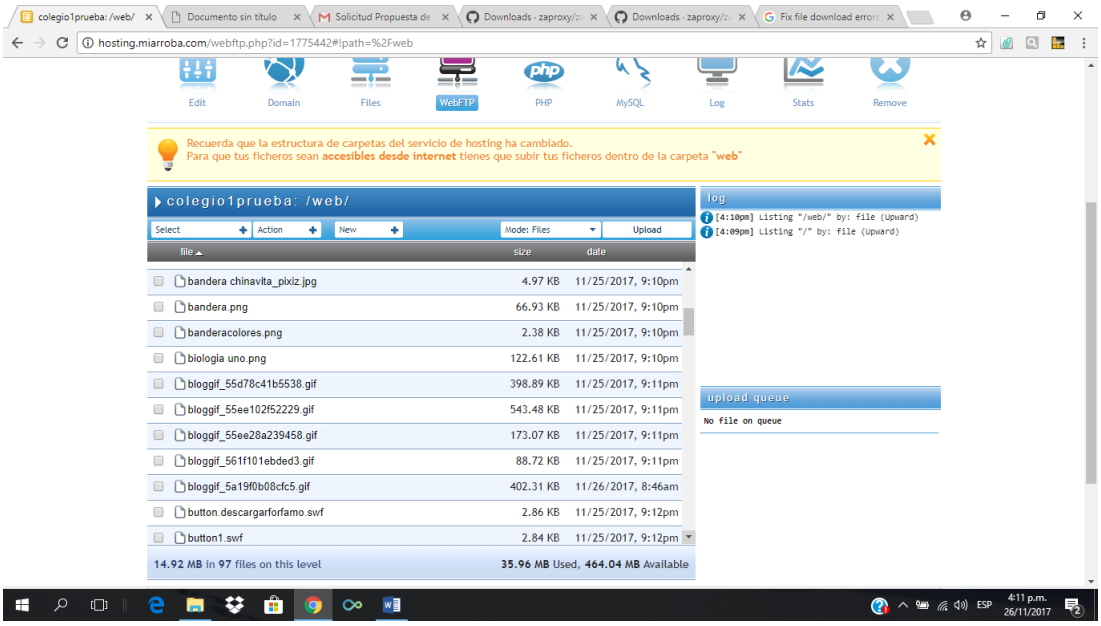


ILUSTRACIÓN 31: INSUMOS DOMINIO3

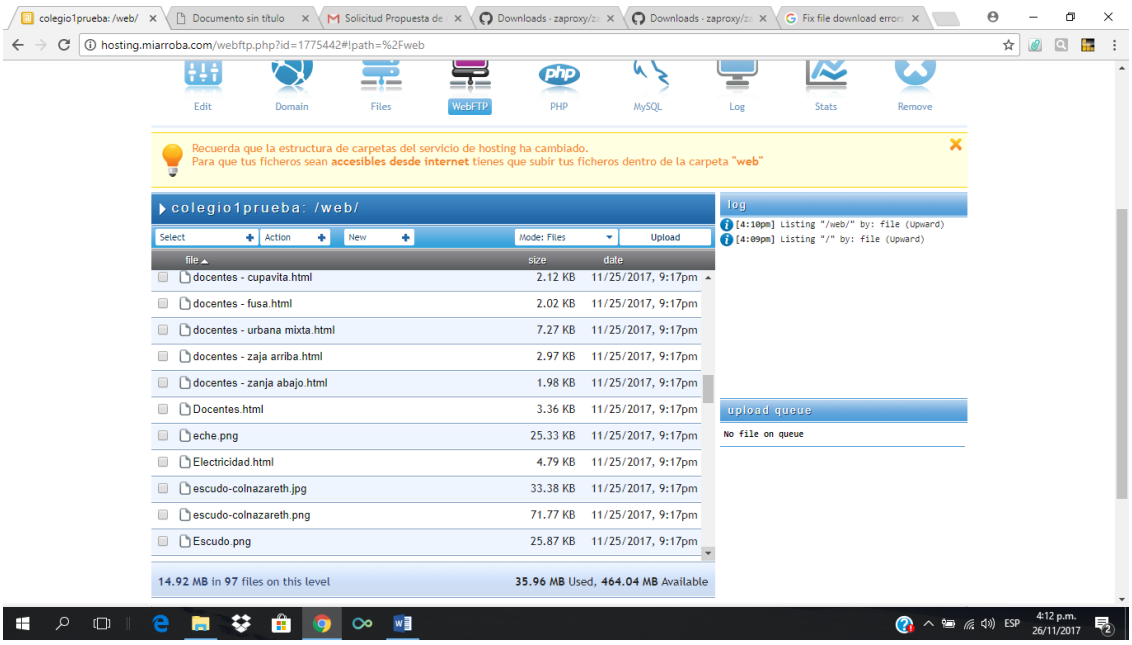


ILUSTRACIÓN 32: INSUMOS DOMINIO4

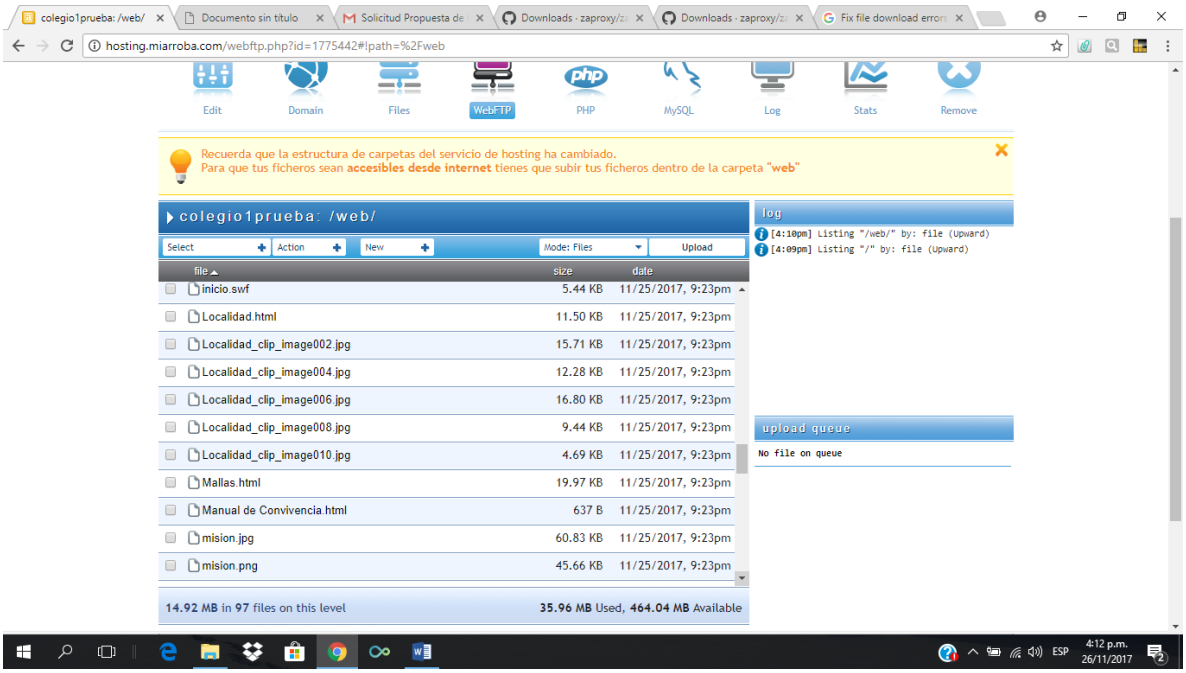
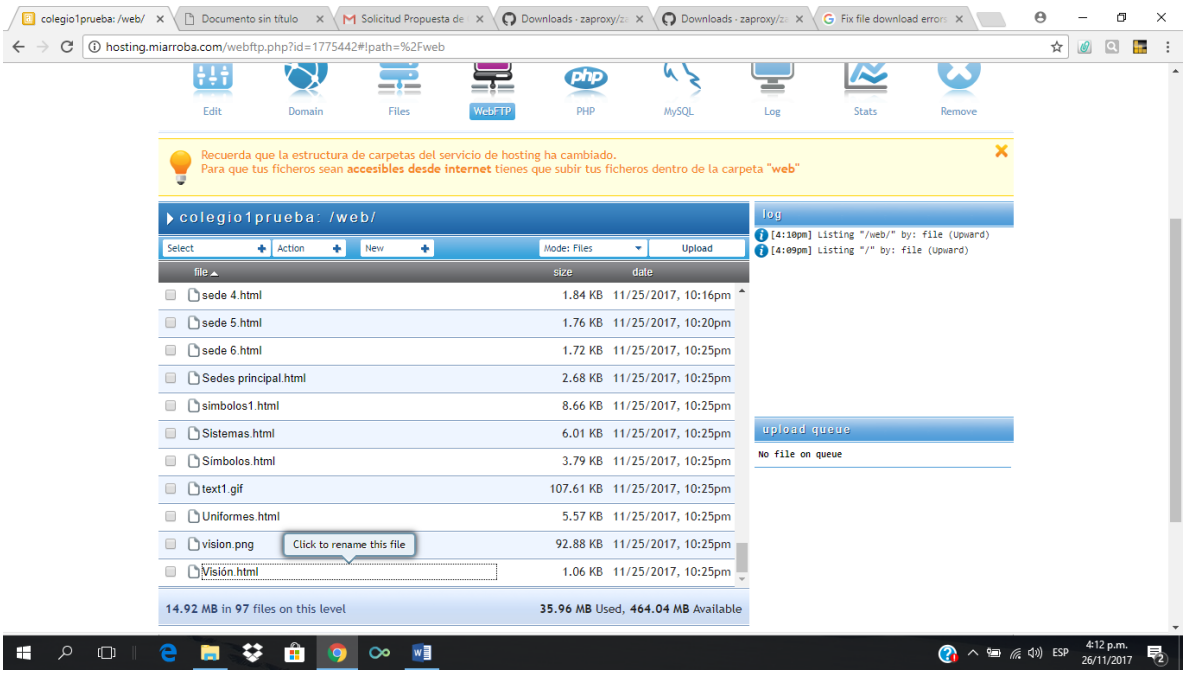


ILUSTRACIÓN 33: INSUMOS DOMINIO5



7.3. ESCANEO DE LA PÁGINA WEB BAJO LA HERRAMIENTA OWASP ZAP

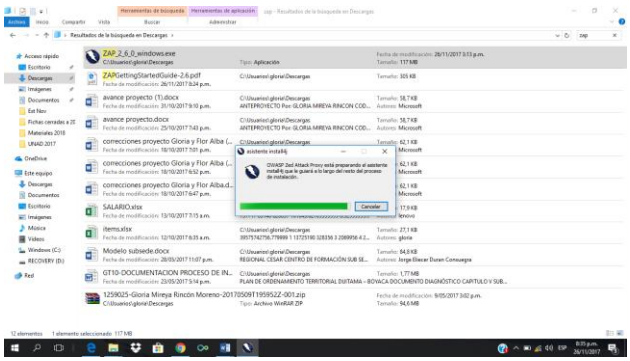
La metodología aplicada para la detección de vulnerabilidades y o riesgos en la página web de la Institución educativa es el Top 10 de OWASP, ya que es un proyecto sin ánimo de lucro, destinado a mejorar la seguridad en diferentes aplicaciones. Y su herramienta de trabajo OWAPS ZAP (Zed attack proxy), la cual será instalada y ejecutada para el desarrollo de este proyecto. ZAP se destaca por las siguientes características y ventajas:

- Es un programa o aplicación gratuita
- Es libre
- Disponible a las organizaciones para desarrollar, comprar y mantener sus aplicaciones confiables
- Cuenta con herramientas de trabajo gratuitas y de código abierto
- Es multiple-plataforma
- Fácil de instalar
- Traducido a más de 12 idiomas
- Cuenta con manuales de apoyo y usuarios que la aplican en la red.
- Tiene la posibilidad de comprobar todas las peticiones y respuestas entre cliente / servidor.

Se descargó específicamente la herramienta Owasp –zap (Zed Attack Proxy), exclusiva para auditar el sitio web, es fácil de usar para realizar las pruebas de penetración, detectando de esta manera posibles vulnerabilidades o amenazas en la aplicación web de la Institución educativa. El proceso es el siguiente:

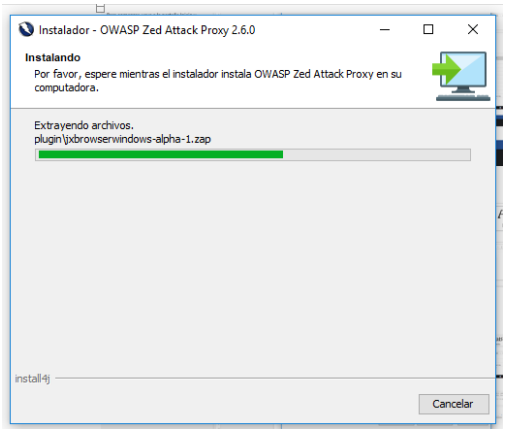
Se descarga la herramienta Owasp zap 2.6.0

ILUSTRACIÓN 34: DESCARGA OWASP-ZAP



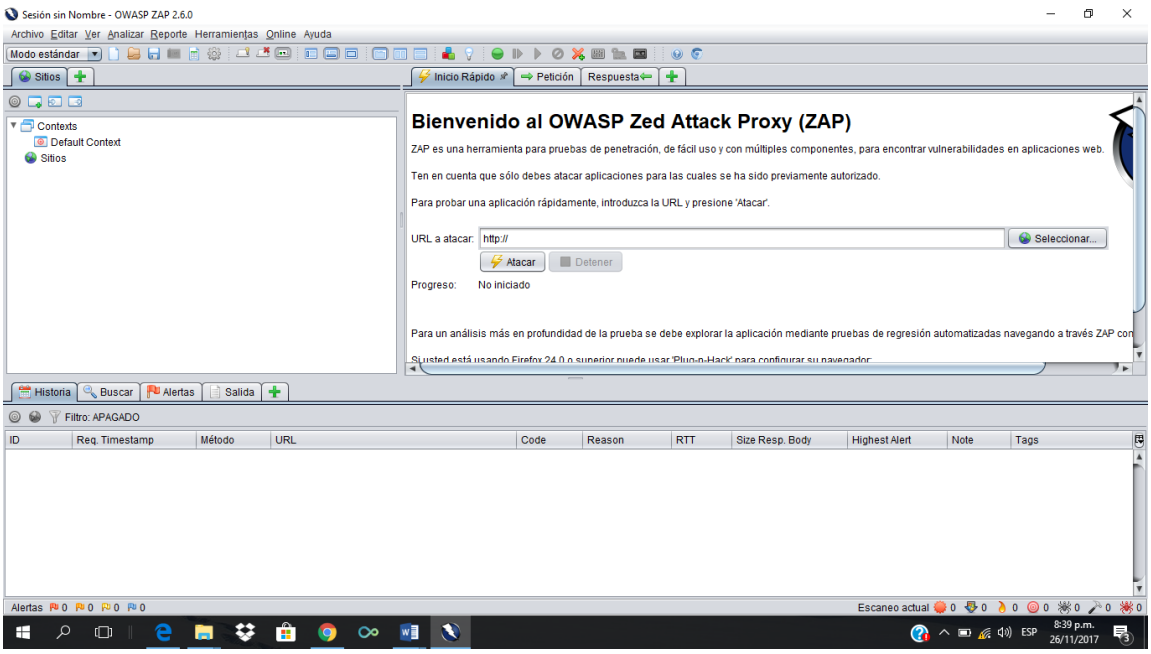
Se ejecuta la instalación del programa:

ILUSTRACIÓN 35: INSTALACIÓN OWASP



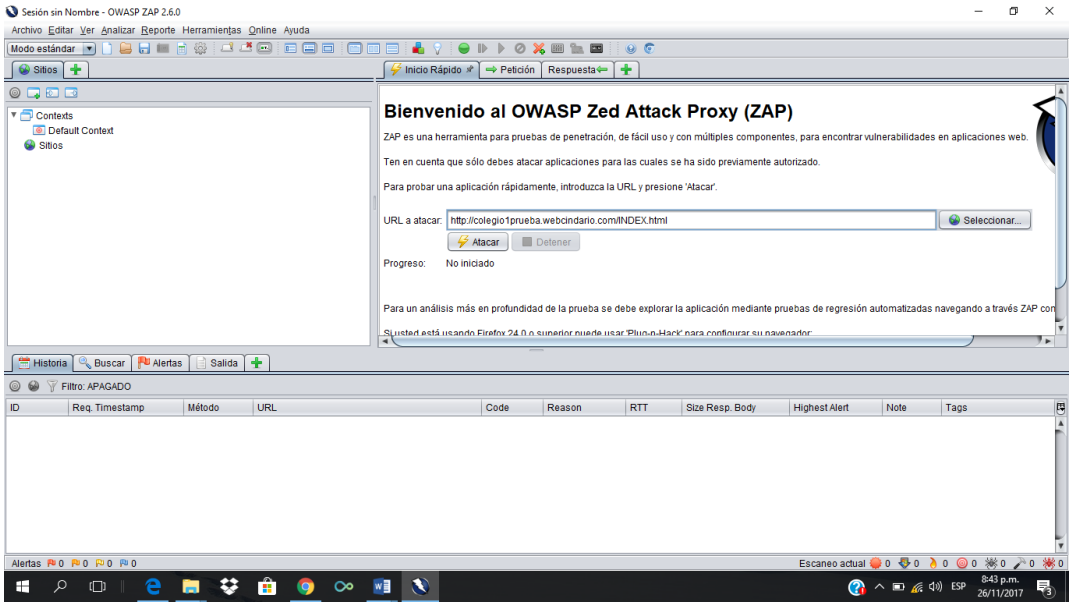
Se procede a abrir la aplicación:

ILUSTRACIÓN 36: APLICACIÓN OWASP



Digitamos la dirección de la página Web:

ILUSTRACIÓN 37: EJECUCIÓN OWASP



Se realiza el proceso de ataque a la página web:

ILUSTRACIÓN 38: ATAQUE OWASP1

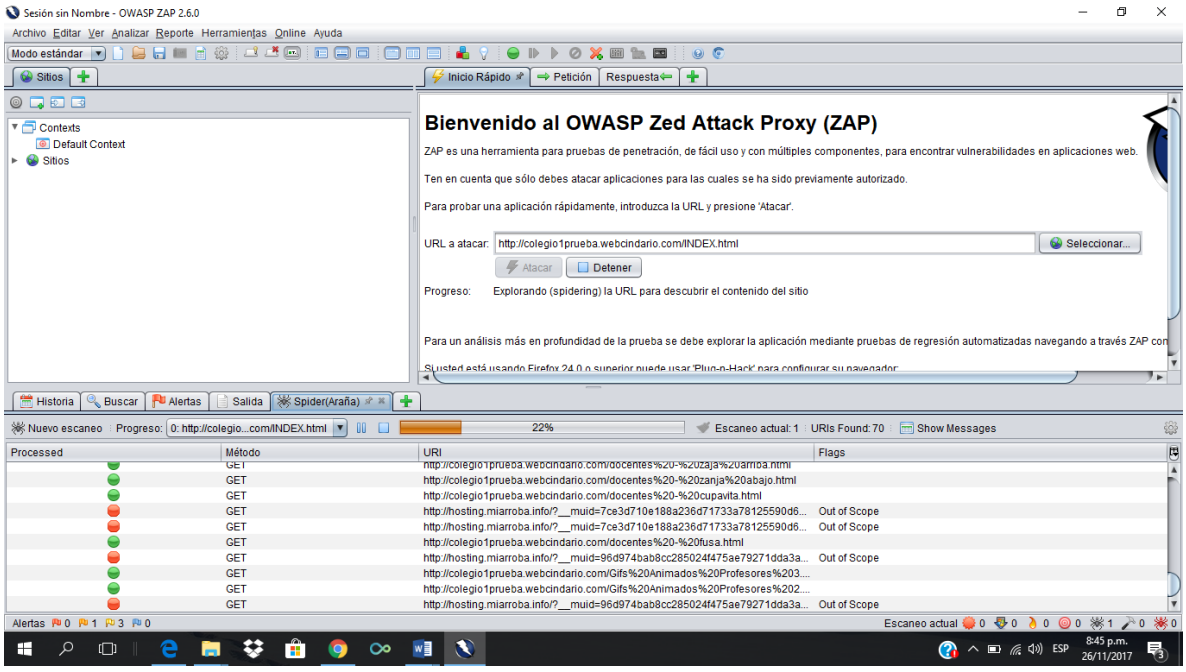
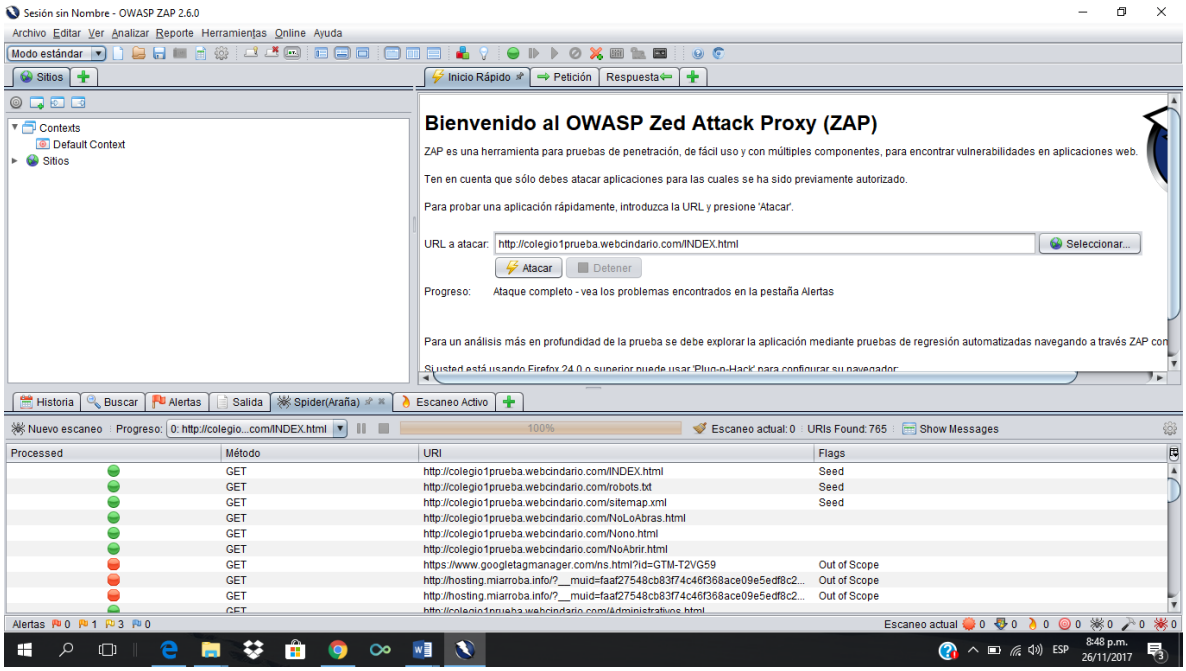


ILUSTRACIÓN 39: ATAQUE OWASP2

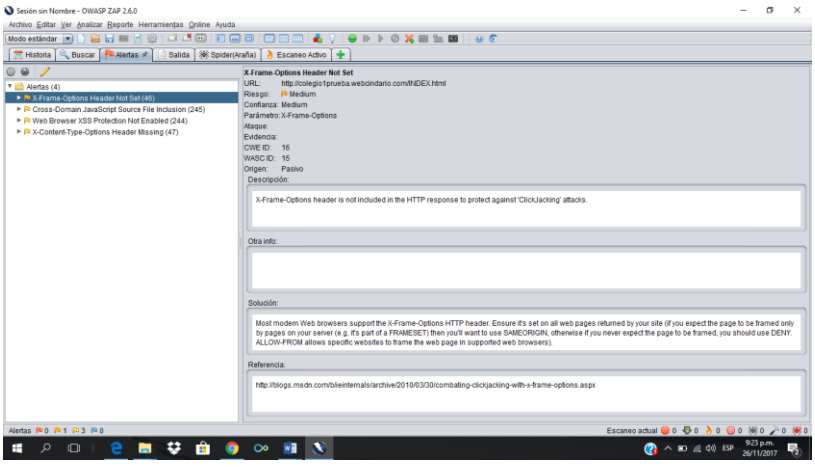


Al realizar el ataque a su 100% muestra un resumen de las alertas relacionadas con los riesgos encontrados:

7.3.1. X-Frame-Options Header Not Set:

El encabezado de opciones no está configurado:

ILUSTRACIÓN 40: RESUMEN DE ALERTA OWASP1



Riesgo medio, Confianza media.

Encabezado no establecido: el encabezado no está incluido en la respuesta HTTP (protocolo de transferencia de hipertextos) para proteger contra los ataques de 'ClickJacking'. El atacante "disfraza" un enlace no deseado, volviéndolo atractivo para la víctima. Para conseguirlo, se basa en el juego de capas que se puede conseguir con HTML e "iframe". Iframe es una (anticuada en cierta forma) técnica para cargar una web dentro de otra. **Clickjacking** está basado normalmente en el iframe. Desviando el direccionamiento de una página a otra abriendo una página o enlace diferente.

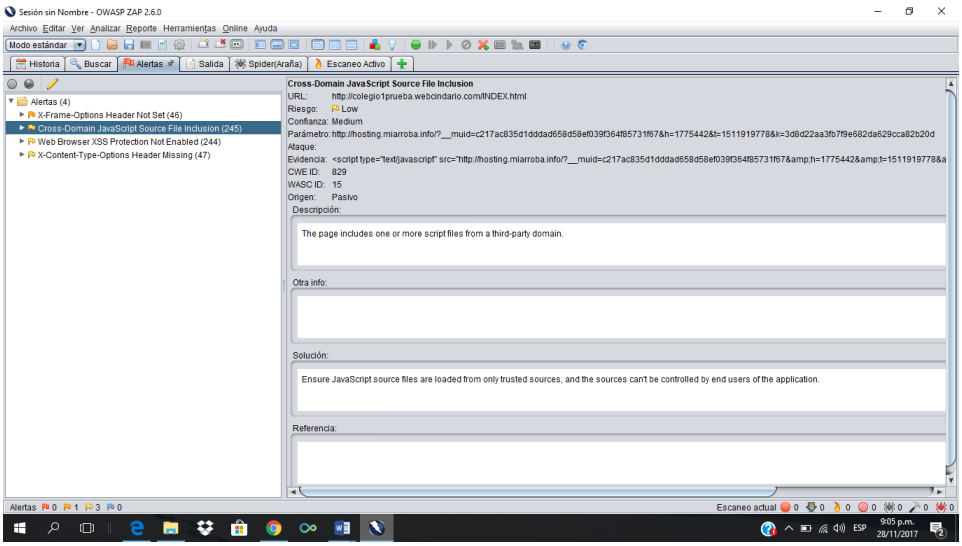
La mayoría de los navegadores web modernos admiten el encabezado HTTP X-Frame-Options. Es necesario que esté configurado en todas las páginas web devueltas por su sitio (si espera que la página esté enmarcada solo por páginas en su servidor (por ejemplo, es parte de un FRAMESET), entonces querrá usar SAMEORIGIN, de lo contrario, si nunca espera la página para enmarcar, debe usar DENY. ALLOW-FROM permite que sitios web específicos marquen la página web en navegadores web compatibles).

En uno de los muchos navegadores web o plataformas con alguna vulnerabilidad, un ataque de clickjacking puede tomar la forma de código embebido o script que se ejecuta sin el conocimiento del usuario.

7.3.2. Cross-Domain JavaScript Source File Inclusion:

Cruzar dominio: Inclusión de archivo de código JavaScript

ILUSTRACIÓN 41: RESUMEN DE ALERTA OWASP2



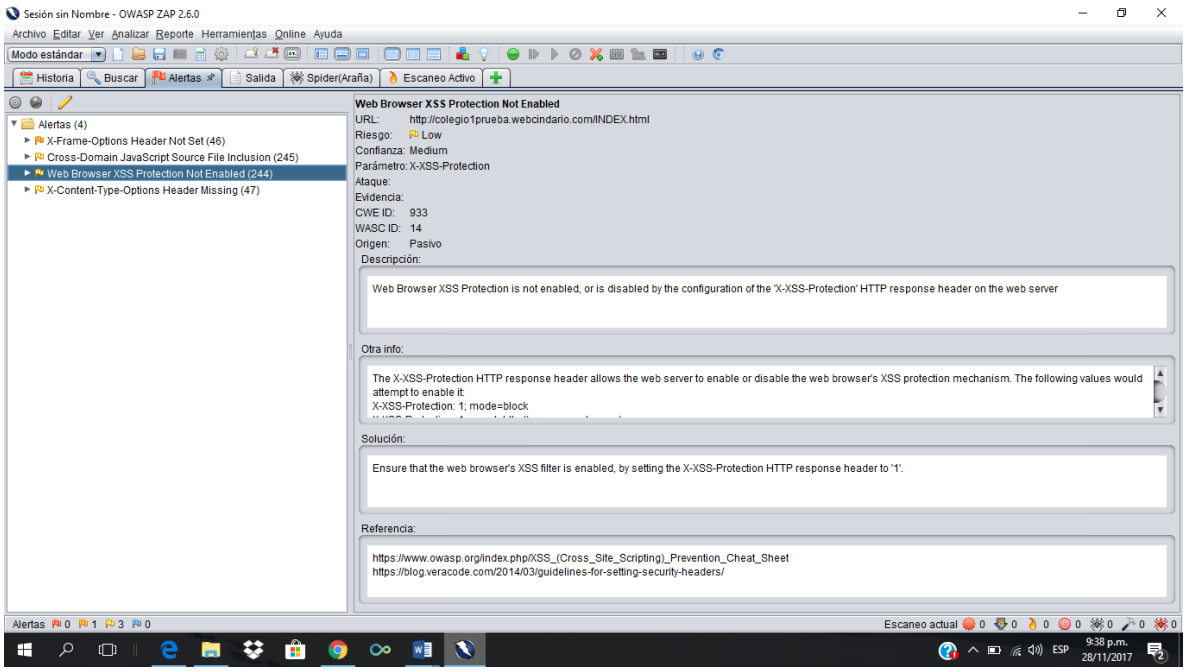
Riesgo bajo, Confianza media.

La página incluye uno o más archivos de script de un dominio de terceros. Es necesario asegurarse de que los archivos fuente de JavaScript se carguen solo de fuentes confiables y que los orígenes de las aplicaciones no puedan controlarlas.

7.3.3. Web Browser XSS Protection Not Enabled:

Navegador web Protección XSS no habilitada.

ILUSTRACIÓN 42: RESUMEN DE ALERTA OWASP3



Riesgo bajo, Confianza media.

La vulnerabilidad conocida como **Cross Site Scripting** (XSS) o ejecución de comandos en sitios cruzados es una de las más habituales donde los atacantes **explotan la confianza que un usuario tiene en un sitio en particular**, Si un sitio web contiene esta vulnerabilidad, un atacante puede realizar diversos tipos de ataques basándose en la **confianza** que inspira la plataforma en el usuario. Desde redirigir a otro sitio para robar

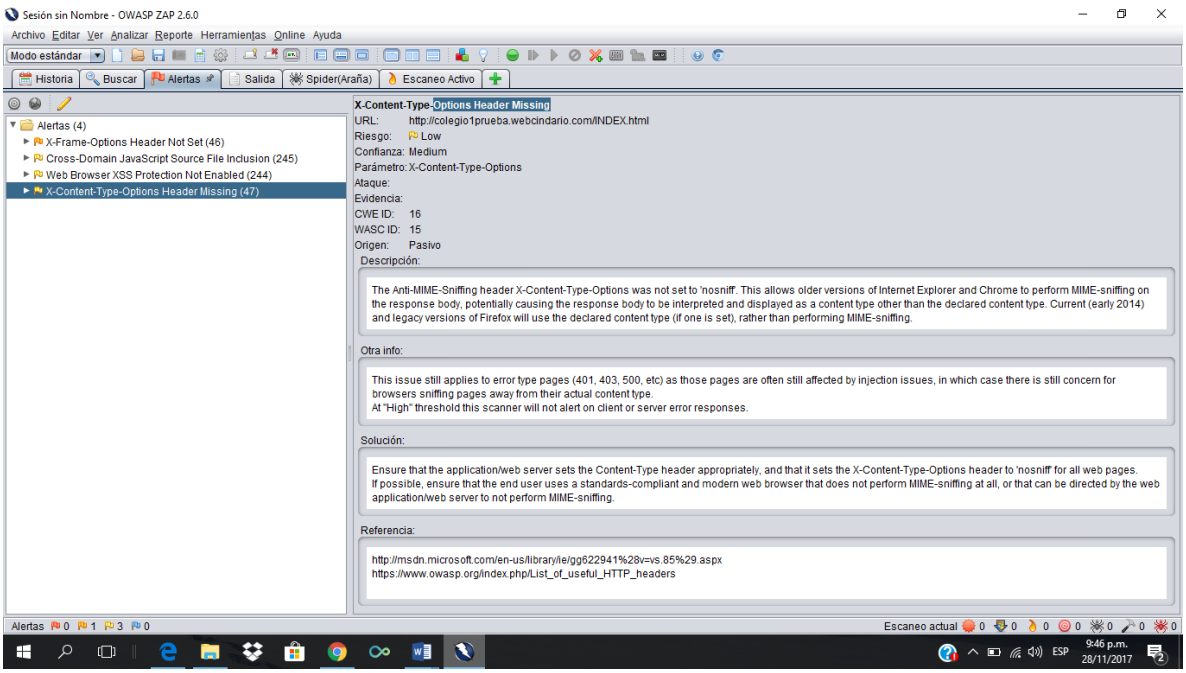
información mediante *phishing* "suplantación de identidad", hasta hacer que se descargue alguna amenaza y se ejecute en el sistema.

Es necesario asegurarse de que el filtro XSS del navegador web esté habilitado, configurando el encabezado de respuesta HTTP de X-XSS-Protection en '1'.

7.3.4. X-Content-Type-Options Header Missing

Tipo de contenido X: Encabezado de opciones desaparecido.

ILUSTRACIÓN 43: RESUMEN DE ALERTA OWASP4



Riesgo bajo, Confianza media.

El encabezado Anti-MIME-X-Content-Type-Options no se configuró en 'nosniff'. MIME-X o tipo de contenido es un mecanismo para decirle al cliente la variedad de documentos transmitidos, la extensión de un nombre de archivo no tiene significado en la web.Esto permite a las versiones anteriores de Internet Explorer y Chrome realizar el rastreo de MIME en el cuerpo de la respuesta, lo que puede causar que el cuerpo de la respuesta se interprete y se muestre como un tipo de contenido distinto del tipo de contenido

declarado. Las versiones actuales (principios de 2014) y heredadas de Firefox utilizarán el tipo de contenido declarado (si está configurado), en lugar de realizar el rastreo de MIME.

Este problema aún se aplica a las páginas de tipo de error (401, 403, 500, etc.), ya que esas páginas a menudo aún se ven afectadas por problemas de inyección, en cuyo caso los navegadores siguen preocupados por olfatear páginas de su tipo de contenido real.
En el umbral "Alto", este escáner no alertará sobre las respuestas de error del cliente o del servidor.
Si se envía la cabecera X-Content-Type-Options en la respuesta con el valor “nosniff”, los navegadores que soportan esta cabecera (IE y Chrome), no cargan las hojas de estilos, ni los scripts (Javascript), cuyo Myme-type no sea el adecuado.

El aspecto de la cabecera a utilizar seria la siguiente:

X-Content-Type-Options: nosniff

La mejor forma de añadir esta cabecera sería añadiendo unas líneas de código al archivos functions.php del tema de WordPress que se esté usando.

Se requiere Asegurarse de que la aplicación / servidor web configure el encabezado de tipo de contenido de manera adecuada y que establezca el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web. Si es posible, asegurarse de que el usuario final utilice un navegador web moderno y compatible con los estándares que no realice ningún tipo de detección MIME, o que la aplicación web / servidor web pueda indicarle que no realice el rastreo MIME.

7.4. SEGURIDAD EN LA INFORMACION

La página web de la IE actualmente se puede copiar tanto el código fuente como la información.

ILUSTRACIÓN 44: PÁGINA WEB I.E.

ILUSTRACIÓN 45: PÁGINA WEB I.E. OPCIÓN COPIAR

Es necesario insertarle el código de protección script para inactivar el acceso de copia por medio del clic derecho.

TABLA 1: CODIGO PROTECCIÓN SCRIPT

```
<script language="Javascript">
<!-- Begin
document.oncontextmenu = function(){return false}
// End -->
</script>
```

Para no copiar el contenido por medio del teclado es necesario agregar el siguiente código:

TABLA 2: CODIGO PROTECCIÓN SCRIPT TECLADO1

```
<script language="JavaScript">
function click() {
if (event.button==2) {
alert('RatónDeshabilitado');
}
}
function keypresed() {
alert('Teclado Desabilitado');
}

document.onkeydown=keypresed;
document.onmousedown=click;

</script>
```

Tabla 3: CODIGO PROTECCIÓN SCRIPT TECLADO2

```
<SCRIPT language=JavaScript1.2>

//Disable select-text script (IE4+, NS6+)- By Andy Scott
//Exclusive permission granted to Dynamic Drive to feature script
//Visit http://www.dynamicdrive.com for this script

function disableselect(e){
return false
}

function reEnable(){
return true
}

//if IE4+
document.onselectstart=new Function ("return false")
```

```
//if NS6
if (window.sidebar){
document.onmousedown=disableselect
document.onclick=reEnable
}
</SCRIPT>

<SCRIPT language=JavaScript>
statuss();
function statuss()
{
window.status = "... | w o l f s p i r i t | ...";
setTimeout("statuss()", 1);
}
</SCRIPT>
```

7.5. RESULTADO DE RIESGOS Y VULNERABILIDADES ENCONTRADAS

A continuación se resumen los ataques realizados a la página web y sus respectivas recomendaciones:

TABLA 4. RESULTADO DE RIESGOS Y VULNERABILIDADES ENCONTRADAS EN LA PAGINA WEB

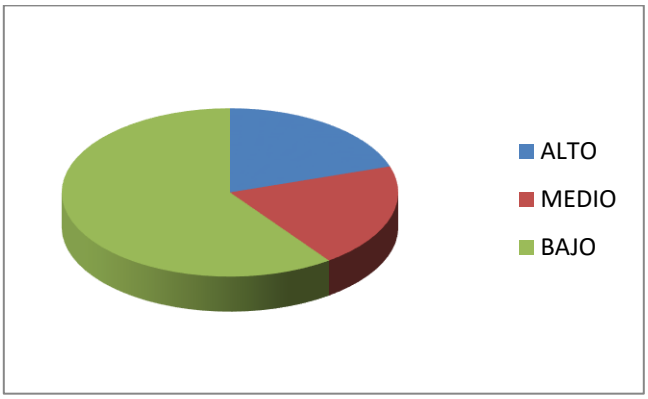
ATAQUE REALIZADO.	NIVEL DE RIESGO.	CONFIANZA.	DESCRIPCIÓN DEL ATAQUE ENCONTRADO.	RECOMENDACIONES.
X-Frame-Options Header Not Set: El encabezado de opciones no está configurado	Medio	Media.	Encabezado no establecido: el encabezado no está incluido en la respuesta HTTP (protocolo de transferencia de hipertextos) para proteger contra los ataques de 'ClickJacking'. El atacante "disfraza" un enlace no deseado, volviéndolo atractivo para la víctima. Para conseguirlo, se basa en el juego de capas que se puede conseguir con HTML e "iframe". Iframe es una (anticuada en cierta forma) técnica para cargar una web dentro de otra. **Clickjacking** está basado normalmente en el iframe. Desviando el direccionamiento de una página a otra abriendo una página o enlace diferente. La mayoría de los navegadores web modernos admiten el encabezado HTTP X-Frame-Options.	Es necesario que el encabezado HTTP X-Frame-Options. esté configurado en todas las páginas web devueltas por su sitio (si espera que la página esté enmarcada solo por páginas en su servidor (por ejemplo, es parte de un FRAMESET), entonces querrá usar SAMEORIGIN, de lo contrario, si nunca espera la página para enmarcar, debe usar DENY. ALLOW-FROM permite que sitios web específicos marquen la página web en navegadores web compatibles). En uno de los muchos navegadores web o plataformas con alguna vulnerabilidad, un ataque de clickjacking puede tomar la forma de código embebido o script que se ejecuta sin el conocimiento del usuario.
Cross-Domain JavaScript Source File Inclusion: Cruzar dominio: Inclusión de archivo de código JavaScript	Bajo	Media.	La página incluye uno o más archivos de script de un dominio de terceros.	Es necesario asegurarse de que los archivos fuente de JavaScript se carguen solo de fuentes confiables y que los orígenes de las aplicaciones no puedan controlarlas.
Web Browser XSS Protection Not Enabled: Navegador web Protección XSS no habilitada.	Bajo	Media.	La vulnerabilidad conocida como **Cross Site Scripting** (XSS) o ejecución de comandos en sitios cruzados es una de las más habituales donde los atacantes **explotan la confianza que un usuario tiene en un sitio en particular**, Si un sitio web contiene esta vulnerabilidad, un atacante puede realizar diversos tipos de ataques basándose en la **confianza** que inspira la plataforma en el usuario. Desde redirigir a otro sitio para robar información mediante *phishing* "suplantación de identidad", hasta hacer que se descargue alguna amenaza y se ejecute en el sistema.	Es necesario asegurarse de que el filtro XSS del navegador web esté habilitado, configurando el encabezado de respuesta HTTP de X-XSS-Protection en '1'.
X-Content-Type-Options Header Missing. Tipo de contenido X: Encabezado de opciones desaparecido.	Bajo	Media.	El encabezado Anti-MIME-X-Content-Type-Options no se configuró en 'nosniff'. MIME-X o tipo de contenido es un mecanismo para decirle al cliente la variedad de documentos transmitidos, la extensión de un nombre de archivo no tiene significado en la web. Esto permite a las versiones anteriores de Internet Explorer y Chrome realizar el rastreo de MIME en el cuerpo de la respuesta, lo que puede causar que el cuerpo de la respuesta se interprete y se muestre como un tipo de contenido distinto del tipo de contenido declarado. Las versiones actuales (principios de 2014) y heredadas de Firefox utilizarán el tipo de contenido declarado (si está configurado), en lugar de realizar el rastreo de MIME. Este problema aún se aplica a las páginas de tipo de error (401, 403, 500, etc.), ya que esas páginas a menudo aún se ven afectadas por problemas de inyección, en cuyo caso los navegadores siguen preocupados por olfatear páginas de su tipo de contenido real. En el umbral "Alto", este escáner no alertará sobre las respuestas de error del cliente o del servidor. Si se envía la cabecera X-Content-Type-Options en la respuesta con el valor "nosniff", los navegadores que soportan esta cabecera (IE y Chrome), no cargan las hojas de estilos, ni los scripts (Javascript), cuyo Myme-type no sea el adecuado. El aspecto de la cabecera a utilizar seria la siguiente: X-Content-Type-Options: nosniff.	La mejor forma de añadir esta cabecera sería añadiendo unas líneas de código al archivos functions.php del tema de WordPress que se esté usando. Se requiere Asegurarse de que la aplicación / servidor web configure el encabezado de tipo de contenido de manera adecuada y que establezca el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web. Si es posible, asegurarse de que el usuario final utilice un navegador web moderno y compatible con los estándares que no realice ningún tipo de detección MIME, o que la aplicación web / servidor web pueda indicarle que no realice el rastreo MIME.
Seguridad en el código fuente	Alto	Baja	Al realizar pruebas de copia de código fuente se observa que el usuario que tiene acceso al respectivo código de inserción, logrando de esta manera usurpar la información e interfaz gráfica de la página web, utilizando este código para el diseño de una aplicación similar.	Es necesario insertarle el código de protección script para inactivar el acceso de copia por medio del clic derecho y por medio de las telas de función del teclado.

Matriz de riesgo:

TABLA 5: MATRIZ DE RIESGO

Nivel de Riesgo	Total
ALTO	1
MEDIO	1
BAJO	3
TOTALES	**5**

ILUSTRACIÓN 46: MATRIZ DE RIESGO



Se concluye que según el grafico anterior que el nivel de riesgo que predomina en las 5 vulnerabilidades encontradas al escanear la página web es bajo.

7.6. ENTREGA DE REPORTE O INFORME A LA I.E.

Teniendo en cuenta el escaneo realzado a la página web de la institución educativa y detectando las diferentes amenazas relacionadas con respecto a su seguridad, se procede a redactar el informe final el cual es presentado a la Institución educativa técnica de Firavitoba con el fin de que tomen medidas de seguridad en el manejo de la información de la página web.

Firavitoba: XX de XXXX del 2017

Especialista:

HILDEBRANDO BONILLA BONIILLA
Rector I.E. Técnica de Firavitoba.

Asunto: Informe diagnostico seguridad página web.

Respetado rector, a continuación relatamos el proceso llevado a cabo a la página web de la I.E. con el fin de detectar amenazas en la seguridad de la información y dar soluciones para garantizar la confidencialidad, integridad y disponibilidad de la información que se maneja.

1. Se verifican los enlaces de las páginas a la página principal, algunos enlaces se encuentran bien direccionados y otros se evaden.
2. Se evidencia que de la página web de la IE actualmente se puede copiar tanto el código fuente como la información.
3. Se ejecuta la herramienta diagnostica Owasp con el fin de detectar posibles amenazas a la página web, encontrando los siguientes resultados y recomendaciones:

Dentro de los problemas detectados se encontró:

- Al ejecutar la herramienta Owasp dentro de sus amenazar arroja que un ataque de clickjacking puede tomar la forma de código embebido o script que se ejecuta sin el conocimiento del usuario y puede atacar a la página web. Desviando el direccionamiento de una página a otra abriendo una página diferente.

- La página incluye uno o más archivos de script de un dominio de terceros. Es necesario asegurarse de que los archivos fuente de JavaScript se carguen solo de fuentes confiables y que los orígenes de las aplicaciones no puedan controlarlas.

- El Navegador web Protección XSS no se encuentra habilitado, la vulnerabilidad **Cross Site Scripting** (XSS) o ejecución de comandos en sitios cruzados, permite que un atacante puede realizar diversos tipos de ataques basándose en la **confianza** que inspira la plataforma en el usuario. Desde redirigir a otro sitio para robar información mediante ***phishing*** *"*suplantación de identidad", hasta hacer que se descargue alguna amenaza y se ejecute en el sistema. Es recomendable asegurarse de que el filtro XSS del navegador web esté habilitado, configurando el encabezado de respuesta HTTP de X-XSS-Protection en '1'.

- El encabezado Anti-MIME-X-Content-Type-Options no se configuró en 'nosniff'. Si se envía la cabecera X-Content-Type-Options en la respuesta con el valor "nosniff", los navegadores que soportan esta cabecera (IE y Chrome), no cargan las hojas de

estilos, ni los scripts (Javascript), cuyo Myme-type no sea el adecuado. La mejor forma de añadir esta cabecera sería añadiendo unas líneas de código al archivos functions.php del tema de WordPress que se esté usando. Se requiere Asegurarse de que la aplicación / servidor web configure el encabezado de tipo de contenido de manera adecuada y que establezca el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web. Si es posible, asegurarse de que el usuario final utilice un navegador web moderno y compatible con los estándares que no realice ningún tipo de detección MIME, o que la aplicación web / servidor web pueda indicarle que no realice el rastreo MIME.

En la siguiente tabla se resumen los ataques realizados a la página web y sus respectivas recomendaciones:

TABLA 6 RESULTADO DE RIESGOS Y VULNERABILIDADES ENCONTRADAS EN LA PAGINA WEB1

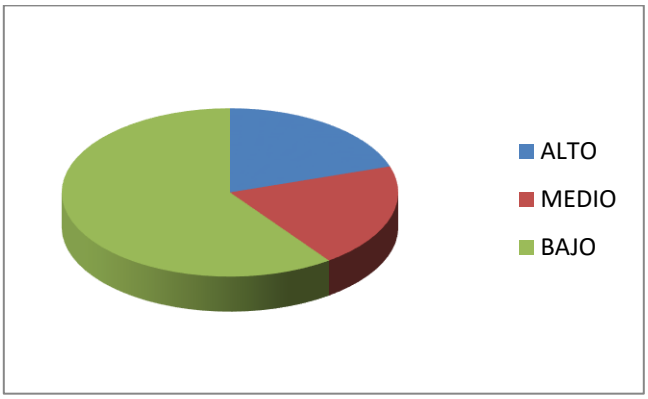
ATAQUE REALIZADO.	NIVEL DE RIESGO.	CONFIANZA.	DESCRIPCIÓN DEL ATAQUE ENCONTRADO.	RECOMENDACIONES.
X-Frame-Options Header Not Set: El encabezado de opciones no está configurado	Medio	Media.	Encabezado no establecido: el encabezado no está incluido en la respuesta HTTP (protocolo de transferencia de hipertextos) para proteger contra los ataques de 'ClickJacking'. El atacante "disfraza" un enlace no deseado, volviéndolo atractivo para la víctima. Para conseguirlo, se basa en el juego de capas que se puede conseguir con HTML e "iframe". Iframe es una (anticuada en cierta forma) técnica para cargar una web dentro de otra. **Clickjacking** está basado normalmente en el iframe. Desviando el direccionamiento de una página a otra abriendo una página o enlace diferente. La mayoría de los navegadores web modernos admiten el encabezado HTTP X-Frame-Options.	Es necesario que el encabezado HTTP X-Frame-Options. esté configurado en todas las páginas web devueltas por su sitio (si espera que la página esté enmarcada solo por páginas en su servidor (por ejemplo, es parte de un FRAMESET), entonces querrá usar SAMEORIGIN, de lo contrario, si nunca espera la página para enmarcar, debe usar DENY. ALLOW-FROM permite que sitios web específicos marquen la página web en navegadores web compatibles). En uno de los muchos navegadores web o plataformas con alguna vulnerabilidad, un ataque de clickjacking puede tomar la forma de código embebido o script que se ejecuta sin el conocimiento del usuario.
Cross-Domain JavaScript Source File Inclusion: Cruzar dominio: Inclusión de archivo de código JavaScript	Bajo	Media.	La página incluye uno o más archivos de script de un dominio de terceros.	Es necesario asegurarse de que los archivos fuente de JavaScript se carguen solo de fuentes confiables y que los orígenes de las aplicaciones no puedan controlarlas.
Web Browser XSS Protection Not Enabled: Navegador web Protección XSS no habilitada.	Bajo	Media.	La vulnerabilidad conocida como **Cross Site Scripting** (XSS) o ejecución de comandos en sitios cruzados es una de las más habituales donde los atacantes **explotan la confianza que un usuario tiene en un sitio en particular**, Si un sitio web contiene esta vulnerabilidad, un atacante puede realizar diversos tipos de ataques basándose en la **confianza** que inspira la plataforma en el usuario. Desde redirigir a otro sitio para robar información mediante *phishing* "suplantación de identidad", hasta hacer que se descargue alguna amenaza y se ejecute en el sistema.	Es necesario asegurarse de que el filtro XSS del navegador web esté habilitado, configurando el encabezado de respuesta HTTP de X-XSS-Protection en '1'.
X-Content-Type-Options Header Missing. Tipo de contenido X: Encabezado de opciones desaparecido.	Bajo	Media.	El encabezado Anti-MIME-X-Content-Type-Options no se configuró en 'nosniff'. MIME-X o tipo de contenido es un mecanismo para decirle al cliente la variedad de documentos transmitidos, la extensión de un nombre de archivo no tiene significado en la web. Esto permite a las versiones anteriores de Internet Explorer y Chrome realizar el rastreo de MIME en el cuerpo de la respuesta, lo que puede causar que el cuerpo de la respuesta se interprete y se muestre como un tipo de contenido distinto del tipo de contenido declarado. Las versiones actuales (principios de 2014) y heredadas de Firefox utilizarán el tipo de contenido declarado (si está configurado), en lugar de realizar el rastreo de MIME. Este problema aún se aplica a las páginas de tipo de error (401, 403, 500, etc.), ya que esas páginas a menudo aún se ven afectadas por problemas de inyección, en cuyo caso los navegadores siguen preocupados por olfatear páginas de su tipo de contenido real. En el umbral "Alto", este escáner no alertará sobre las respuestas de error del cliente o del servidor. Si se envía la cabecera X-Content-Type-Options en la respuesta con el valor "nosniff", los navegadores que soportan esta cabecera (IE y Chrome), no cargan las hojas de estilos, ni los scripts (Javascript), cuyo Myme-type no sea el adecuado. El aspecto de la cabecera a utilizar seria la siguiente: X-Content-Type-Options: nosniff.	La mejor forma de añadir esta cabecera sería añadiendo unas líneas de código al archivos functions.php del tema de WordPress que se esté usando. Se requiere Asegurarse de que la aplicación / servidor web configure el encabezado de tipo de contenido de manera adecuada y que establezca el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web. Si es posible, asegurarse de que el usuario final utilice un navegador web moderno y compatible con los estándares que no realice ningún tipo de detección MIME, o que la aplicación web / servidor web pueda indicarle que no realice el rastreo MIME.
Seguridad en el código fuente	Alto	Baja	Al realizar pruebas de copia de código fuente se observa que el usuario que tiene acceso al respectivo código de inserción, logrando de esta manera usurpar la información e interfaz gráfica de la página web, utilizando este código para el diseño de una aplicación similar.	Es necesario insertarle el código de protección script para inactivar el acceso de copia por medio del clic derecho y por medio de las telas de función del teclado.

Teniendo en cuenta la tabla anterior se observan los siguientes resultados:

TABLA 7: MATRIZ DE RIESGO

Nivel de Riesgo	Total
ALTO	1
MEDIO	1
BAJO	3
TOTALES	**5**

ILUSTRACIÓN: 47 MATRIZ DE RIESGO



Se concluye que según el grafico anterior que el nivel de riesgo que predomina en las 5 vulnerabilidades encontradas al escanear la página web es bajo.

Se recomienda a la institución educativa comprar el servicio de un hosting donde se pueda alojar su página web, con el fin de garantizar la seguridad de la información que en la página se maneja, ya que en este momento se encuentran alojada en un servidor gratuito lo cual genera riesgos y amenazas en el manejo de la información. Existen diferentes servidores que prestan el servicio de alojamiento, se aconseja realizar la gestión con Hosting Colombia por seguridad, responsabilidad y costos. El paquete que ofrece corresponde a un valor de 150.000 a 200.000 durante un año de servicio.

Las características recomendadas del servidor para alojar la página web de la I.E. son las siguientes:

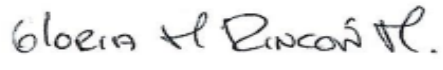
* 20.000MB (20GB) de espacio
* 20 cuentas de Correo Electrónico Corporativas
* Alojamiento para Sitio Web con soporte Flash/PHP/MySQL

* Soporte Técnico y asesoría durante todo el año de servicio.
* Constructor de sitios.
* Email Marketing.

Nos encontramos en la capacidad de apoyar el proceso de la seguridad de sus activos informáticos ya que es indispensable que toda Institución se encuentre protegida no solo en la parte de infraestructura sino también en el uso de su información física y digital.

Agradecemos la atención prestada.

Cordialmente,

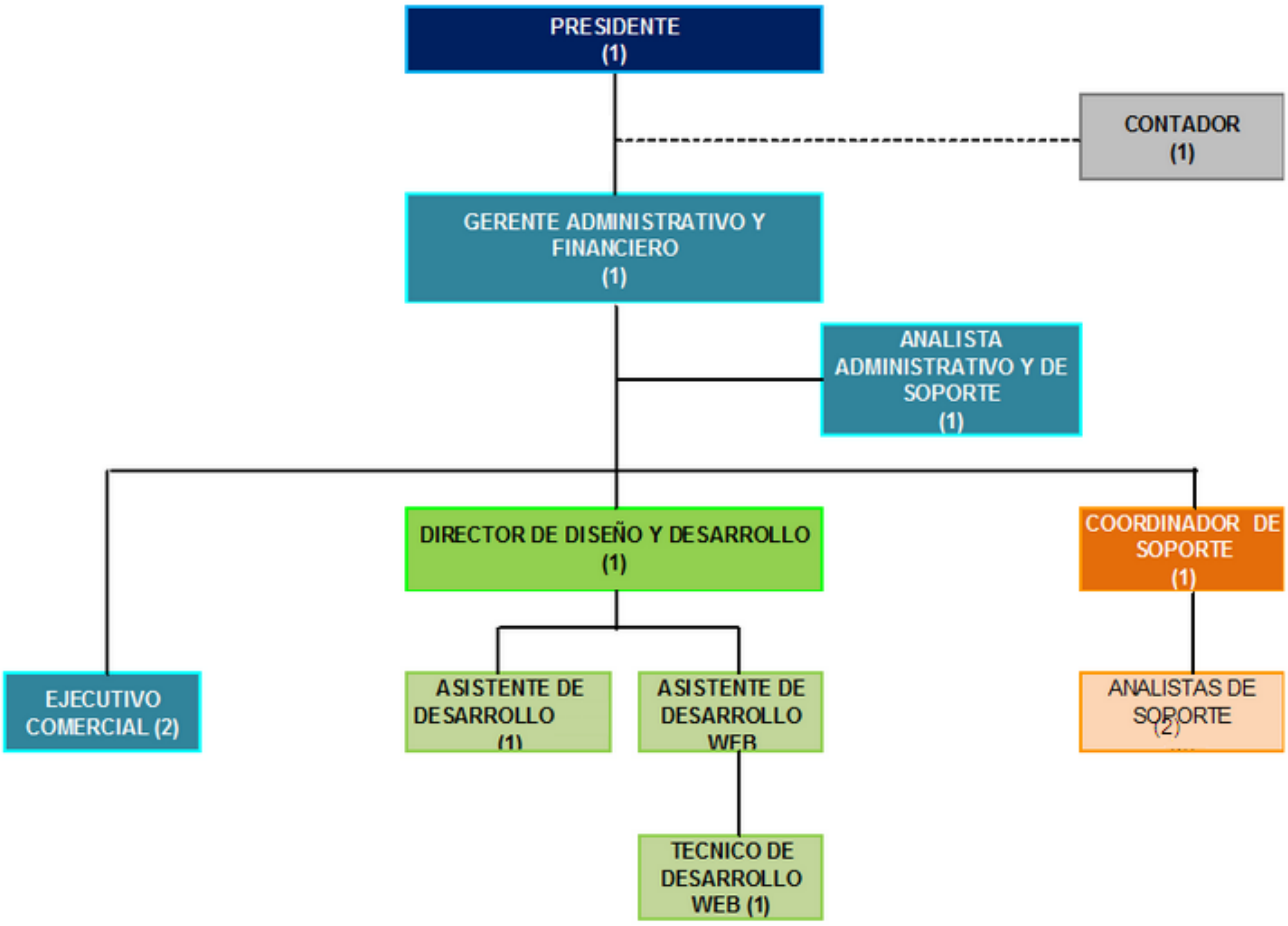


GLORIA MIREYA RINCON
Ing Sistemas.

FLORALBA ALBARRACIN
Ing Sistemas.

8. ESTRUCTURA ORGANIZACIONAL

ILUSTRACIÓN 48: ESRUCTURA ORGANIZACIONAL



9. PERSONAS QUE PARTICIPAN EN EL PROYECTO.

Proponentes primarios,

Gloria Mireya Rincón, Ingeniera de Sistemas. Egresada de la Universidad Nacional Abierta y a Distancia (2002). Actualmente estudiante en la misma Universidad en la Especialización en Seguridad Informática. Labora en el Servicio Nacional de aprendizaje SENA, Regional Boyacá como instructora en el área de Sistemas.

Floralba Albarracin Cristancho, nacida en Sogamoso- Boyacá. Ingeniera de sistemas de la Universidad San Buenaventura- Bogotá. Actualmente estudiante en la Universidad Nacional Abierta y a Distancia en la Especialización en Seguridad Informática. Labora en el Servicio Nacional de aprendizaje SENA, Regional Boyacá como instructora en el área de Sistemas.

Proponentes Secundarios

JUAN JOSE CRUZ GARZON, Ingeniero de Sistemas. Especialista en Seguridad Informática, Docente OCACIONAL de Postgrado del programa en Seguridad Informática (UNAD),

Especialista HILDEBRANDO BONILLA BONIILLA RECTOR de la Institución educativa Técnica de Firavitoba.

Tutor de asignatura de Proyecto:

Ing. ARTURO ERAZO, Ingeniero de Sistemas. ESPECIALISTA N SEG INFORMATICA

Y demás personas que coadyuvaron en la realización del proyecto.

10. RECURSOS DISPONIBLES

Materiales:

Escritorio, silla, resma de papel, bolígrafos, marcadores, borrador, lápiz.

Institucionales:

Biblioteca de la Universidad Abierta y a Distancia UNAD

Biblioteca de la Institución Educativa Técnica de Firavitoba

Financieros:

Los gastos los asumen los integrantes que están generando el proyecto, ya que es un requisito para optar al título de Especialistas en Seguridad Informática, estos costos disminuyen porque cada uno de ellos cuenta con su propio portátil para el desarrollo del proyecto. Los costos se discriminan a continuación:

TABLA 8: RECURSOS FINANCIEROS

RECURSO	DESCRIPCIÓN	PRESUPUESTO
Equipo Humano	Gloria Mireya Rincón Floralba Albarracín Cristancho	300000 300000
Equipos y Software	2 Equipos portátiles	2000000
Viajes y Salidas de Campo	Desplazamientos a la Institución Educativa de Firavitoba a recolectar información, realizar diagnóstico e implementar la página y realizar las pruebas pertinentes	220.000
Materiales y suministros	Escritorio, silla, resma de papel, bolígrafos, marcadores, borrador, lápiz.	100.000
Bibliografía	Referencias bibliográficas	150.000
TOTAL		**$ 3.070.000**

Humano:

El recurso humano para el desarrollo de la presente propuesta de proyecto de grado está conformado por los estudiantes Gloria Mireya Rincón y Floralba Albarracín Cristancho estudiantes de la especialidad "Seguridad Informática" de la Universidad Nacional Abierta y a Distancia - Unad, junto con la asesoría del Ingeniero Juan José Cruz Garzón.

TABLA 9: RECURSO HUMANO

Personal	Función
Gloria Mireya Rincón	Encargada de la investigación sobre la seguridad en páginas web, buscando procedimientos estrategias y herramientas que permitan garantizar la integridad, la disponibilidad y la confidencialidad de la información. Realizadora de las encuestas y proyecto investigativo
Floralba Albarracín	Encargada de la investigación sobre la seguridad en páginas web, buscando procedimientos estrategias y herramientas que permitan garantizar la integridad, la disponibilidad y la confidencialidad de la información. Realizadora de las encuestas y proyecto investigativo
ING. JUAN JOSE CRUZ GARZON	Encargado de guiar y orientar a las estudiantes en el proceso de la investigación sobre la seguridad en página web

Técnicos:

Para el desarrollo del proyecto de grado, el estudiante contará con los siguientes recursos

- Talleres de sistemas con elementos de equipos de cómputo.
- Plataforma virtual
- Biblioteca Unad
- 2 equipos portátiles para utilizarlos los diseñadores de la aplicación
- 1 Cámara Web
- 1 Impresora

Tecnológicos:

2 computadores, horas de internet, impresora, USB, etc.

11. RESULTADOS E IMPACTO ESPERADOS

El presente proyecto intenta, por una parte, concientizar a todos los integrantes de la comunidad educativa de la Institución Técnica de Firavitoba, de la importancia de la seguridad de las aplicaciones web que se manejan y conseguir que estas aplicaciones estén completamente protegidas.

Por otra parte se busca proteger en un porcentaje alto las aplicaciones web y evitar de esta forma el robo de información. Cuando se conoce y se evalúan los daños que pueden hacer, se decide actuar para combatir y protegerse ante este tipo de intrusiones.

Dentro de los problemas detectados se encontró:

- Al ejecutar la herramienta Owasp dentro de sus amenazar arroja que un ataque de clickjacking puede tomar la forma de código embebido o script que se ejecuta sin el conocimiento del usuario y puede atacar a la página web. Desviando el direccionamiento de una página a otra abriendo una página diferente.

- La página incluye uno o más archivos de script de un dominio de terceros. Es necesario asegurarse de que los archivos fuente de JavaScript se carguen solo de fuentes confiables y que los orígenes de las aplicaciones no puedan controlarlas.

- El Navegador web Protección XSS no se encuentra habilitado, la vulnerabilidad **Cross Site Scripting** (XSS) o ejecución de comandos en sitios cruzados, permite que un atacante puede realizar diversos tipos de ataques basándose en la **confianza** que inspira la plataforma en el usuario. Desde redirigir a otro sitio para robar información mediante ***phishing*** *"*suplantación de identidad", hasta hacer que se descargue alguna amenaza y se ejecute en el sistema. Es recomendable asegurarse de que el filtro XSS del navegador web esté habilitado, configurando el encabezado de respuesta HTTP de X-XSS-Protection en '1'.

- El encabezado Anti-MIME-X-Content-Type-Options no se configuró en 'nosniff'. Si se envía la cabecera X-Content-Type-Options en la respuesta con el valor "nosniff", los navegadores que soportan esta cabecera (IE y Chrome), no cargan las hojas de estilos, ni los scripts (Javascript), cuyo Myme-type no sea el adecuado. La mejor forma de añadir esta cabecera sería añadiendo unas líneas de código al archivos functions.php del tema de WordPress que se esté usando. Se requiere Asegurarse de que la aplicación / servidor web configure el encabezado de tipo de contenido de manera adecuada y que establezca el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web. Si es posible, asegurarse de que el usuario final utilice un navegador web moderno y compatible con los estándares que

no realice ningún tipo de detección MIME, o que la aplicación web / servidor web pueda indicarle que no realice el rastreo MIME.

- Se recomienda a la institución educativa comprar el servicio de un hosting donde se pueda alojar su página web, con el fin de garantizar la seguridad de la información que en la página se maneja, ya que en este momento se encuentran alojada en un servidor gratuito lo cual genera riesgos y amenazas en el manejo de la información. Existen diferentes servidores que prestan el servicio de alojamiento, se aconseja realizar la gestión con Hosting Colombia por seguridad, responsabilidad y costos. El paquete que ofrece corresponde a un valor de 150.000 a 200.000 durante un año de servicio.

12. CRONOGRAMA

El proyecto de investigación se desarrollará en un tiempo de 6 meses como lo ilustra el cronograma.

TABLA 10: CRONOGRAMA

1. CRONOGRAMA DE ACTIVIDADES												
ACTIVIDAD	**MES 1**	**MES 2**	**MES 3**	**MES 4**	**MES 5**	**MES 6**	**MES 7**	**MES 8**	**MES 9**	**MES 10**	**MES 11**	**MES 12**
Recolección de información												
Diagnóstico												
Organización y distribución de tareas												
Aplicar , tabular y analizar encuestas												
Aplicación herramienta diagnostica.												
Verificación amenazas en la página WEB.												
Establecer soluciones de seguridad a la aplicación web.												
Recomendaciones y entrega informe final.												

13. CONCLUSIONES

1. El proyecto desarrollado mejora los procesos académicos-administrativos en la Institución Educativa Técnica de Firavitoba ya que cuenta con una seguridad en todas las aplicaciones web que se manejan.

2. Después de realizar el análisis del manejo de la información de aplicaciones web de la Comunidad Educativa pudo observarse que ésta no constituye una forma segura y efectiva de administrarla, de tal manera se considera necesario el desarrollo de una aplicación que apoye los procesos de las aplicaciones web de forma segura con el fin de proteger la información.

3. Con el sistema propuesto será posible incrementar la seguridad de la información en las aplicaciones web, ya que la información se manejará de manera segura de tal forma se reduce el riesgo de pérdida de datos y la manipulación de los mismos por parte de los usuarios.

4. Las aplicaciones no se deben diseñar solo para cumplir un objetivo, sino que a la vez se deben diseñar de tal manera que se comprometa la seguridad de la información en la Institución Educativa.

BIBLIOGRAFIA

[1] Ristic, I. “Apache Security”. ISBN 10-0-596-00724-8. O’Reilly Media Inc. Estados Unidos de América. 2005. [1] AMÓRTEGUI T. Diego J., Ciberseguridad y Ciberterrorismo [en línea], <http://www.acis.org.co/fileadmin/Revista_119/informe_Diego_Amortegui.pdf>, [citado el 02 de Septiembre de 2011]

[2] ASOCIACION DE INGENIEROS DE SISTEMAS. Seguridad de la información en Latinoamérica, Tendencias en 2011 [en línea], Tomado de: <http://www.acis.org.co/fileadmin/Revista_119/informe_Latinoamerica 2011.pdf>, [citado el 02 de Septiembre de 2011]

[3] ASOCIACION DE INGENIEROS DE SISTEMAS. Seguridad de la información en Latinoamérica, Tendencias en 2011 [en línea], Tomado de: <http://www.acis.org.co/fileadmin/Revista_119/informe_Latinoamerica 2011.pdf>, [citado el 02 de Septiembre de 2011]

[4] CODEBOX, Glosario [en línea],<http://www.codebox.es/glosario>, [citado el 05 de Septiembre de 2011]

[5] New Web Star. Los diferentes lenguajes de programación para la web [en línea],<http://www.newwebstar.com/ebooks/133193-los-diferentes-programas- de-programación-para-la-html>, [citado el 06 de Septiembre de 2011]

[6] Guía de pruebas OWASP V 3.0 [En línea], disponible en: https://www.owasp.org/images/8/80/Gu%C3%ADa_de_pruebas_de_OWASP_ver_3.0.pdf >, [Citado 2008]

[7] Metodología y Frameworks de testeo de la seguridad en aplicaciones, [En línea], disponible en: http://www.juntadeandalucia.es/servicios/madeja/sites/default/files/historico/1.3.0/contenido-recurso-216.html#OSSTMM

[8] Metodología y Frameworks de testeo de la seguridad en aplicaciones, [En línea], disponible en: http://www.juntadeandalucia.es/servicios/madeja/sites/default/files/historico/1.3.0/contenido-recurso-216.html#OSSTMM

[9] VELAZCO, Ruben., OWASP ZAP, herramienta para auditar la seguridad de una página web, [En línea], disponible en: https://www.redeszone.net/2015/04/25/seguridad-web-owasp-zap/ , [citado el 25 de Abril de 2015]

[10] MELON, Luis, 10 herramientas para escanear vulnerabilidades web, [En línea], disponible en: https://ciberseguridad.blog/10-herramientas-para-escanear-

vulnerabilidades-web/10 herramientas para escanear vulnerabilidades web, [citado el 17 de Febrero de 2017]

[11] CACERES, Jesus., 12 herramientas gratuitas en línea para analizar vulnerabilidades de seguridad y malware en sitios web, [En línea], disponible en: http://www.xn--apaados-6za.es/tenemos-que-apanar/internet-tutoriales-y-trucos/71269-herramientas-gratuitas-en-linea-analizar-vulnerabilidades-seguridad-malware-sitios-web.html, [citado el 28 de Diciembre de 2016]

[12] Secretaría del Senado, Ley1273 de 2009 [En línea], <http://www.secretariasenado.gov.co/senado/basedoc/ley/2009/ley_1273_2009.html>, [Citado el 3 de Octubre de 2011]

[13] Ley Estatutaria 1581 de 2012, [En línea], http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4998 [Citado por Diario Oficial 48587 de octubre 18 de 2012]

[14] VIEIRA, Marco., ANTUNES, Nuno., MADEIRA, Henrique. “Using Web Security Scanners to in Web Services”. IEEECISUC, Departament of informatics Engineering Detect Vulnerabilities” University of Coimbra, Portugal, 2009.

[15] ASCENCIO, Martha., MORENO, Pedro., Desarrollo de una Propuesta Metodológica para Determinar la Seguridad en una Aplicación Web. [En línea], http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/2511/0058A811.pdf?sequence=1 >, [Citado el 15 de Octubre de 2011] Pereira, 2011.

ANEXOS

ANEXO A. LISTA DE CHEQUEO ANTEPROYECTO

Elemento	Criterio / elementos	cumple SI/NO	Argumento
Título	Abarca el qué, el cómo y el dónde del tema de investigación de forma clara y concisa.	SI	Se define claramente lo que se pretende hacer ya que en la mayoría de las empresas que trabajan con sistemas web se ven expuestos a riesgos informáticos por falta de seguridad.
	Mayúscula sostenida, en negrilla, sin punto al final	SI	
Delimitación del tema de estudio	Verificar limitaciones de tipo temporal, económico o de complejidad	SI	Se encuentra delimitado ya que se enfoca a la seguridad en aplicaciones Web.
	Pertinencia y relevancia del tema de estudio en el área en el que se desarrolla	SI	Se enfatiza en el tema de estudio que es la seguridad de la información.
	La realización de la investigación no implica riesgos para la seguridad del investigador, o el investigador es plenamente consciente de ellos y decide asumirlos.	SI	No existe riesgo alguno y si lo llegara a ser el investigador asumirá sus propios riesgos.
Disponibilidad de la información	Es posible encontrar la suficiente información y asesoría respecto al tema en cuestión	SI	Se cuenta con referencias bibliográficas y en línea para el desarrollo y puesta en marcha del proyecto.
Redacción	Adecuación textual	SI	Cada tema a tratar esta establecido según lo requerido.
	Coherencia textual	SI	Existe relación entre lo solicitado con lo que se pretende realizar.
	Cohesión textual	SI	Se encuentra bien especificado según los ítems sugeridos.
	Corrección gramatical	SI	Cumple con especificaciones gramaticales.
Ortografía	No se presentan errores ortográficos	SI	Cumple con parámetros ortográficos.
Formulación del problema	Se hace una formulación clara y sin ambigüedades	SI	Es clara ya que de ella depende lo que se pretende realizar.
	Evidencia la relación entre variables en un contexto temporal y espacial	NO	

Justificación	Argumenta las razones por las cuales se escogió el tema de estudio y evidencia su importancia	SI	Se ve necesaria esta investigación ya que la seguridad en la Web asume un papel importante en los sistemas informáticos.
	Describe y argumenta claramente los beneficios al realizar el proyecto	SI	Se ven evidenciados en la justificación.
	Grado de innovación del proyecto, su valor científico, académico o técnico.	NO	No se trata tema de innovación.
Objetivo general	El objetivo general es coherente con la pregunta de investigación	SI	El objetivo general define el proyecto a trabajar.
Objetivos específicos	Representan metas parciales que llevan al cumplimiento del objetivo general	SI	Se discrimina a lo que se quiere llegar con el desarrollo del proyecto.
	Son realistas, no deben ser muy difíciles de cumplir.	SI	Se especifica lo que se pretende realizar.
	Redactados en orden cronológico (orden de cumplimiento)	NO	No se evidencia el tiempo de cumplimiento de los objetivos, pero están redactados en orden de aplicación.
Marco referencial	Marco teórico	SI	Estudio de investigación y referencias Bibliográficas.
	Marco contextual	NO	
	Marco legal	NO	
	Otros marcos de referencia (si es necesario)	SI	Diseño metodológico Preliminar.
Diseño metodológico preliminar	Tipo de investigación	SI	Fases de elaboración del trabajo.
	Población, muestra, variables	SI	Se especifica a quien va dirigido.
	Técnicas de recolección de información	SI	Por medio de la Encuesta.
Recursos	Talento Humano	SI	Equipo de trabajo
	Materiales y equipos	SI	Se encuentran establecidos.
	Análisis de costos	SI	Recursos económicos necesarios básicos.
	Fuentes de financiación	NO	No se encuentran relacionados.
	Relación costo - beneficio	NO	No se encuentran relacionados.
Cronograma	Establece los plazos de ejecución de las fases y	SI	Detallados según la actividad respecto al tiempo.

	actividades más relevantes del proyecto.		
Bibliografía	Cantidad, calidad y relevancia de las fuentes	SI	Se ajustan con respecto a las consultas elaboradas para la realización del anteproyecto.
	Normatividad APA o ICONTEC	SI	Cumple con APA
	Organizada en orden alfabético	SI	Se encuentran organizadas alfabéticamente.
	Funcionalidad de los enlaces, si los hay.	NO	No existen enlaces.
glosario (* opcional)	Si es necesario, se sugiere incluir un glosario con mínimo 10 términos relacionados con el tema de estudio	NO	La terminología es aplicada en el Marco referencia.

Objetivos	Redactados en orden cronológico (orden de cumplimiento)	NO	No se evidencia el tiempo de cumplimiento de los objetivos, pero están redactados en orden de aplicación.

De la Lista de Chequeo original se eliminarían los siguientes aspectos:

Dentro del elemento Objetivos se podría eliminar este criterio ya que todo objetivo específico se enumera de acuerdo a su fecha de ejecución y se ejecutan en orden o secuencia.

Dentro del elemento Redacción se podría incluir los 3 primeros criterios ya que todos hacen referencia a la claridad de lo que se está especificando en el tema, en cuanto a claridad del texto, coherencia de lo que se habla y la lingüística manejada omitiendo de esta manera términos innecesarios (cohesión).

Redacción	Adecuación textual	SI	Cada tema a tratar esta establecido según lo requerido.
	Coherencia textual	SI	Existe relación entre lo solicitado con lo que se pretende realizar.
	Cohesión textual	SI	Se encuentra bien especificado según los ítems sugeridos.
	Corrección gramatical	SI	Cumple con especificaciones gramaticales.

Elemento modificado:

ANEXO B. NUEVA LISTA DE CHEQUEO MODIFICADA ANTEPROYECTO

Redacción	Adecuación, Coherencia y Cohesión textual	SI	Cada tema a tratar esta establecido según lo requerido, existe relación entre lo solicitado con lo que se pretende realizar y se encuentra bien especificado según los ítems sugeridos.
	Corrección gramatical	SI	Cumple con especificaciones gramaticales.

Elemento	Criterio / elementos	cumple SI/NO	Argumento
Título	Abarca el qué, el cómo y el dónde del tema de investigación de forma clara y concisa.	SI	Se define claramente lo que se pretende hacer ya que en la mayoría de las empresas que trabajan con sistemas web se ven expuestos a riesgos informáticos por falta de seguridad.
	Mayúscula sostenida, en negrilla, sin punto al final	SI	
Delimitación del tema de estudio	Verificar limitaciones de tipo temporal, económico o de complejidad	SI	Se encuentra delimitado ya que se enfoca a la seguridad en aplicaciones Web.
	Pertinencia y relevancia del tema de estudio en el área en el que se desarrolla	SI	Se enfatiza en el tema de estudio que es la seguridad de la información.
	La realización de la investigación no implica riesgos para la seguridad del investigador, o el investigador es plenamente consciente de ellos y decide asumirlos.	SI	No existe riesgo alguno y si lo llegara a ser el investigador asumirá sus propios riesgos.
Disponibilidad de la información	Es posible encontrar la suficiente información y asesoría respecto al tema en cuestión	SI	Se cuenta con referencias bibliográficas y en línea para el desarrollo y puesta en marcha del proyecto.
Redacción	Adecuación, Coherencia y Cohesión textual	SI	Cada tema a tratar esta establecido según lo requerido, existe relación entre lo solicitado con lo que se pretende realizar y se encuentra bien especificado según los ítems sugeridos.
	Corrección gramatical	SI	Cumple con especificaciones gramaticales.
Ortografía	No se presentan errores ortográficos	SI	Cumple con parámetros ortográficos.
Formulación del problema	Se hace una formulación clara y sin ambigüedades	SI	Es clara ya que de ella depende lo que se pretende realizar.

	Evidencia la relación entre variables en un contexto temporal y espacial	NO	
Justificación	Argumenta las razones por las cuales se escogió el tema de estudio y evidencia su importancia	SI	Se ve necesaria esta investigación ya que la seguridad en la Web asume un papel importante en los sistemas informáticos.
	Describe y argumenta claramente los beneficios al realizar el proyecto	SI	Se ven evidenciados en la justificación.
	Grado de innovación del proyecto, su valor científico, académico o técnico.	NO	No se trata tema de innovación.
Objetivo general	El objetivo general es coherente con la pregunta de investigación	SI	El objetivo general define el proyecto a trabajar.
Objetivos específicos	Representan metas parciales que llevan al cumplimiento del objetivo general	SI	Se discrimina a lo que se quiere llegar con el desarrollo del proyecto.
	Son realistas, no deben ser muy difíciles de cumplir.	SI	Se especifica lo que se pretende realizar.
Marco referencial	Marco teórico	SI	Estudio de investigación y referencias Bibliográficas.
	Marco contextual	NO	
	Marco legal	NO	
	Otros marcos de referencia (si es necesario)	SI	Diseño metodológico Preliminar.
Diseño metodológico preliminar	Tipo de investigación	SI	Fases de elaboración del trabajo.
	Población, muestra, variables	SI	Se especifica a quien va dirigido.
	Técnicas de recolección de información	SI	Por medio de la Encuesta.
Recursos	Talento Humano	SI	Equipo de trabajo
	Materiales y equipos	SI	Se encuentran establecidos.
	Análisis de costos	SI	Recursos económicos necesarios básicos.
	Fuentes de financiación	NO	No se encuentran relacionados.
	Relación costo - beneficio	NO	No se encuentran relacionados.
Cronograma	Establece los plazos de ejecución de las fases y actividades más relevantes del proyecto.	SI	Detallados según la actividad respecto al tiempo.

Bibliografía	Cantidad, calidad y relevancia de las fuentes	SI	Se ajustan con respecto a las consultas elaboradas para la realización del anteproyecto.
	Normatividad APA o ICONTEC	SI	Cumple con APA
	Organizada en orden alfabético	SI	Se encuentran organizadas alfabéticamente.
	Funcionalidad de los enlaces, si los hay.	NO	No existen enlaces.
glosario (* opcional)	Si es necesario, se sugiere incluir un glosario con mínimo 10 términos relacionados con el tema de estudio	NO	La terminología es aplicada en el Marco referencia.