ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN Y VINCULACIÓN CON LA COLECTIVIDAD

PROGRAMA DE MAESTRIA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

TESIS DE GRADO PREVIO A LA OBTENCION DEL TITULO DE MAGISTER.

TEMA: EVALUACIÓN TÉCNICA DE SEGURIDAD DE LA APLICACIÓN WEB DEL "SISTEMA INFORMATICO INTEGRADO DE SERVICIOS MUNICIPALES" DEL GADIC CAÑAR

AUTORES: FLORES URGILES CRISTINA MARIUXI
FLORES URGILES CRISTHIAN HUMBERTO

DIRECTOR: ING. RON GAVI MARIO MSc.

SANGOLQUÍ

2015

UNIVERSIDAD DE LAS FUERZAS ARMADAS – ESPE
MAESTRIA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

CERTIFICADO

ING. MARIO RON GAVI
DIRECTOR

ING. CARLOS PROCEL SILVA
OPONENTE

CERTIFICAN

Que el trabajo de tesis, titulado: "EVALUACIÓN TÉCNICA DE SEGURIDAD DE LA APLICACIÓN WEB DEL SISTEMA INFORMATICO INTEGRADO DE SERVICIOS MUNICIPALES DEL GADIC CAÑAR", presentado por la Ing. CRISTINA MARIUXI FLORES URGILES y el Ing. CRISTHIAN HUMBERTO FLORES URGILES, requisito previo para la obtención del título de MAGÍSTER en Evaluación y Auditoría de Sistemas Tecnológicos, ha sido guiado y revisado periódicamente y cumple normas estatuarias establecidas por la ESPE, en el reglamento de Estudiantes de la Universidad de las Fuerzas Armadas.

Revisado el contenido del presente trabajo, y tomando en consideración que entrega un valioso aporte a la entidad receptora del mismo, se recomienda su publicación.

Autorizan a Flores Urgilés Cristina Mariuxi y Flores Urgilés Cristhian Humberto, entregar el mismo a la Unidad de gestión de Postgrados.

En la ciudad de Sangolquí, a los 7 días del mes de mayo del 2015.

ING. MARIO RON GAVI
DIRECTOR

ING. CARLOS PROCEL SILVA
OPONENTE

UNIVERSIDAD DE LAS FUERZAS ARMADAS – ESPE
MAESTRIA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

ACTA DE RESPONSABILIDAD

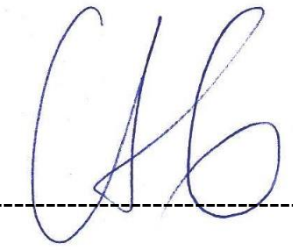
ING. CRISTINA MARIUXI FLORES URGILES

ING. CRISTHIAN HUMBERTO FLORES URGILES

El contenido e información que se encuentra en ésta Tesis denominada "EVALUACIÓN TÉCNICA DE SEGURIDAD DE LA APLICACIÓN WEB DEL SISTEMA INFORMATICO INTEGRADO DE SERVICIOS MUNICIPALES DEL GADIC CAÑAR" es responsabilidad exclusiva del autor y ha respetado derechos intelectuales de terceros, conforme a las fuentes que se incorporan en la bibliografía.

En la ciudad de Sangolquí, a los 7 días del mes de mayo del 2015.

Ing. Cristina Flores Urgiles



Ing. Cristhian Flores Urgiles

UNIVERSIDAD DE LAS FUERZAS ARMADAS – ESPE

MAESTRIA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

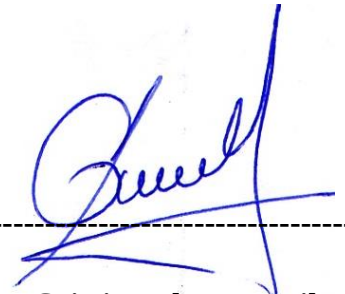
AUTORIZACIÓN PUBLICACIÓN BIBLIOTECA

ING. CRISTINA MARIUXI FLORES URGILES

ING. CRISTHIAN HUMBERTO FLORES URGILES

Autorizo a la Universidad de las Fuerzas Armadas- ESPE, la publicación, en la biblioteca virtual de la Institución del trabajo de grado denominado "EVALUACIÓN TÉCNICA DE SEGURIDAD DE LA APLICACIÓN WEB DEL SISTEMA INFORMATICO INTEGRADO DE SERVICIOS MUNICIPALES DEL GADIC CAÑAR", cuyo contenido, ideas y criterios son de nuestra responsabilidad y autoría.

En la ciudad de Sangolquí, a los 7 días del mes de mayo del 2015.



---------- ----------

Ing. Cristina Flores Urgiles **Ing. Cristhian Flores Urgiles**

DEDICATORIA.

"…A Marcos y Diego Andrés, por ser la razón de mi vida y la consecuencia de todo mi esfuerzo, a Papi Humbico por su apoyo y amor incondicional…y a mami Charito consiente de que a través de los recuerdos le mantengo viva, a través de mis logros le honraré eternamente…"

Ing. Cristina Flores Urgiles

"… A Elita y Matías que son mi inspiración para siempre conseguir mis metas, a Papi Humbico, Jonathan y Cristina por la fortaleza demostrada en los momentos difíciles, que me permitió culminar con mis objetivos, a Mami Charo que su fortaleza, decisión y amor vivirá siempre en mi corazón .. ″

Ing. Cristhian Flores Urgiles

AGRADECIMIENTO

A Dios por la fortaleza que nos ha brindado para culminar con este proyecto y que día a día nos bendice para salir siempre adelante.

A nuestro hermano Jonathan quien con sus palabras de aliento nos han motivado a culminar con éxito esta meta que nos hemos trazado

Al MSig. Danny Andrade Cárdenas responsable del departamento informático del Gobierno Autónomo Descentralizado Intercultural de Cañar, por permitirnos desarrollar nuestro tema de tesis con el cual damos cumplimiento a una etapa más de nuestra educación .

Agradecemos de manera especial el apoyo incondicional y dedicación del Msc. Mario Ron Gabi por su acertada dirección en este trabajo de investigación y por habernos brindando a más de conocimientos, su amistad.

Al director y docentes de la Maestría En Evaluación Y Auditoría De Sistemas Tecnológicos, quienes nos han brindado valiosos conocimientos y con sus acertadas gestiones nos han permitido cumplir esta meta.

A todos ellos, muchas gracias.

Cristina Mariuxi Flores Urgiles

Cristhian Humberto Flores Urgiles

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

INDICE DE TABLAS

RESUMEN

En el presente proyecto se pretende realizar un análisis de las vulnerabilidades del aplicativo Web del "SISTEMA INFORMATICO INTEGRADO DE SERVICIOS MUNICIPALES" del GADIC CAÑAR con el fin de detectar y prevenir las amenazas más comunes que ponen en peligro la estabilidad de los sistemas informáticos en la WEB, partiendo de un análisis comparativo entre diferentes metodologías de aseguramiento como son OWASP top 10, WASC Tc v2.0 Y CWE/SANS Top 25, los cuales presentan los riesgos más relevantes, sus vectores de ataque y los posibles controles de mitigación. Una vez determinada la metodología de aseguramiento a ser utilizada, se establece la metodología de auditoria con sus respectivos entregables por cada fase; luego se establece las herramientas que pueden ser utilizadas para la detección de las vulnerabilidades según los puntos de control establecidos por OWASP top 10, metodología seleccionada en un proceso anteriores. Las pruebas fueron diseñadas dentro de las pruebas sustantivas de auditoria, así también se tomó como referencia la ISO 27002 para realizar el análisis de los controles existentes y el diseño de las pruebas de cumplimiento. De los resultados obtenidos se emitió un informe detallado de los hallazgos con sus conclusiones y recomendaciones que fueron diseñados con el objetivo de brindar soporte al mejoramiento continuo de los servicios informáticos que brinda a la ciudadana el GADIC Cañar.

PALABRAS CLAVES:

- **EVALUACIÓN TÉCNICA INFORMÁTICA**
- **SEGURIDAD**
- **VULNERABIILIDADES**
- **APLICACIONES WEB**
- **OWASP TOP 10**

ABSTRACT

In the presente In this project it is to perform an analysis of the vulnerabilities of Web application of " SISTEMA INFORMATICO INTEGRADO DE SERVICIOS MUNICIPALES " of GADIC CAÑAR in order to detect and prevent the most common threats that endanger the stability of computer systems in the WEB, based on a comparative analysis of different assurance methodologies such as OWASP Top 10 and WASC Tc v2.0 CWE / SANS Top 25, which have the most significant risks, their means of attack and possible mitigating controls. After determining the assurance methodology to be used, the audit methodology with their respective deliverables for each phase is set; then the tools that can be used to detect vulnerabilities as checkpoints established by OWASP top 10, methodology selected on a previous process is established. The tests were designed within the substantive audit tests, so it was taken as reference the ISO 27002 for the analysis of existing controls and the design of compliance testing. The results obtained a detailed report of findings with conclusions and recommendations that were designed with the aim of providing support to the continuous improvement of IT services provided to the public the GADIC Cañar was issued.

KEY WORDS:

- **TECHNICAL ASSESSMENT INFORMATION**
- **SECURITY**
- **VULNERABIILIDADES**
- **WEB APPLICATIONS**
- **OWASP TOP 10.**

CAPÍTULO I

1.1. Título

Evaluación técnica de seguridad de la aplicación web del "SISTEMA INFORMATICO INTEGRADO DE SERVICIOS MUNICIPALES" del GADIC CAÑAR

1.2. Resumen

La seguridad informática se ha convertido en uno de los aspectos más importantes dentro de la administración efectiva de los sistemas de información, con la adopción de nuevas metodologías y herramientas informáticas, que en la actualidad proveen de servicios eficientes para las organizaciones, se han incrementado el riesgos de ataques informáticos, perdida de información sensible de los usuarios, no disponibilidad de los servicios entre otros que pueden afectar la continuidad de las operaciones del negocio.

En el caso puntual de las aplicaciones web, herramientas informáticas a las que se accede a través de internet u otras redes similares como intranet, el riesgo es superior ya que al encontrarse alojado en la web esta se vuelve más vulnerable, y más aún cuando su estructura no se encuentra correctamente diseñada al no contemplar aspectos de seguridad en su construcción.

El caso de estudio es el GADIC Cañar, Municipio que ha experimentado una transformación importante en el ámbito tecnológico, mediante la implementación de sistemas de información que han automatizado las tareas de las diferentes dependencias, de manera puntual el cabildo cuenta con el " SISTEMA INFORMATICO INTEGRADO DE SERVICIOS MUNICIPALES ", el mismo que cuenta con una aplicación web que permite la gestión de la siguientes información: Agua potable, alcantarillado y basura, predio rustico y predio urbano, patentes municipales, cobro del rodaje, control de mercados, plazas y andenes, cartera, transferencia de dominios, cementerios , alcabalas, plusvalía y certificados de solvencia municipal . Este sistema es desarrollado bajo la plataforma de .NET y

como motor de base de datos Oracle, sin embargo al momento de su construcción no se aplicó ningún estándar de aseguramiento de la aplicación.

El proceso de investigación será desarrollado mediante el método científico, haciendo una combinación de los procesos de inducción y deducción. La investigación teórica utilizará el método documental permitiéndonos obtener un texto formal. El método experimental será utilizado para la realización de pruebas controladas que nos permitirán el entendimiento de los procesos causales.

1.3. Justificación e Importancia

1.3.1. Estado del arte a nivel mundial y local.

Al constituirse como necesaria e indispensable la utilización de aplicaciones web para algunas organizaciones, se torna importante el estudio del aseguramiento de mencionadas aplicaciones, por ello se han desarrollado diversos estándares que permiten analizar qué tan seguro es la estructura de la aplicación. Por lo expuesto anteriormente varios autores han desarrollado diversos estudios de investigación sobre el tema, cuyos resultados han proveído una guía de las mejores prácticas a tomarse en consideración. A continuación detallamos los más destacados:

La investigación desarrollada por Dharmesh M Mehta, que titula "Effective Software Security Management".

"Estudio De Metodologías Para Pruebas De Penetración A Sistemas Informáticos" desarrollado por el Ing. Agustín López del Instituto Técnico Nacional de la Ciudad de México, realiza el análisis de tres metodologías de pruebas de penetración a aplicaciones Web.

El estudio realizado por: Carmen Torrano-Gimenez, Alejandro Perez-Villegasy Gonzalo Alvarez que titula " WASAT- A New Web Authorization Security Analysis Tool", presenta un análisis realizado sobre la aplicación WASAT,EL estudio realizado por Fu Quanlin del departamento de Ciencias Computacionales e Ingeniería de la Universidad Shanghai Jiao Tong, habla acerca de la "Web Application Security Detection and Measure Based on OWASP ".

Efectividad de OWASP Para Proteger Applicaciones Web Contra Inyección de SQL, Manuel López Arredondo, Guadalajara; es un estudio del nivel de riesgo al que se encuentran expuestas las aplicaciones web.

En el Ecuador el tema planteado también ha sido analizado en trabajos similares, debido a la importancia que ha tomado el tema de seguridad de la información y al creciente porcentaje de empresas que trabajan con aplicaciones web para soportar sus servicios, los trabajos generados se han enfocado en determinar los niveles de riesgos que poseen las aplicaciones web cuando no han sido construidos en base a estándares de seguridad, además de analizar los diversos marcos de referencia que pueden ser utilizados para la construcción de una aplicación web segura.

Entre los trabajos de investigación más destacados tenemos los siguientes:

"Seguridad en Entornos Web para Sistemas de Gestión Académica desarrollado por René Guamán Quinche".

"Estrategias de Seguridad para aplicaciones web desarrolladas en asp.net para el Instituto Tecnológico Sudamericano a nivel de autenticación y privilegios de usuario", desarrollado por Diego Armando Morocho Herrera.

"Análisis de las aplicaciones web de la Superintendencia de Bancos y Seguros, utilizando las recomendaciones Top Ten de OWASP para determinar los riesgos más críticos de seguridad e implementar buenas prácticas de seguridad para el desarrollo de sus aplicativos." desarrollado por Salgado Yánez, Ángel Lenin. (Salgado Yanez, 2014)

1.4. Planteamiento del problema

El GADIC Cañar, Municipio que ha experimentado una transformación importante en el ámbito tecnológico, mediante la implementación de sistemas de información que han automatizado las tareas de las diferentes dependencias que componen esta ilustre institución, al igual que el creciente porcentaje de organizaciones que han adoptado los servicios web como cartera de servicios hacia sus usuarios, posee una aplicación web que permite a la ciudadanía consultar información relevante se sus diligencias municipales.

Actualmente el creciente porcentaje de ataques informáticos a páginas web gubernamentales en el Ecuador, genera la preocupación por parte de los directivos GADIC Cañar, que desean conocer las vulnerabilidades que ponen en riesgo la información que gestiona la municipalidad, ya que corresponde a información sensible de la ciudadanía del cantón, por lo expuesto se torna imperiosa la ejecución de la evaluación técnica de seguridad que permitirá identificar las vulnerabilidades que generan mayor riesgo a los sistemas de información; así también como brindar recomendaciones que permitirá implementar controles de seguridad al entorno web diseñado por la Institución

Por lo expuesto se torna imperiosa esta evaluación que permitirá determinar cuáles son las vulnerabilidades que generan mayor riesgo, así como brindar recomendaciones que permitirá implementar controles de seguridad basados en estándares reconocidos.

1.5. Formulación del problema a resolver

-¿Qué modelo de evaluación de seguridad informática tiene que ser aplicado para evaluar la seguridad de aplicaciones WEB?

-¿Cuál es el nivel de riesgo informático al que se encuentra expuesto la aplicación WEB del GADIC Cañar?

-¿Se realizan pruebas que garanticen el cumplimiento de estándares de seguridad en el desarrollo de los aplicativos?

-¿El personal de desarrollo de los aplicativos se encuentra consciente de los riesgos de seguridad que poseen sus aplicativos WEB?

1.6. Hipótesis

No Aplica

1.7. Objetivo General

Realizar una evaluación a la seguridad del aplicativo web del “SISTEMA INFORMATICO INTEGRADO DE SERVICIOS MUNICIPALES” del GADIC Cañar, utilizando estándares de aseguramiento de aplicaciones web, a fin de encontrar vulnerabilidades y emitir recomendaciones dentro del ambiente informático, que permitirá minimizar los riesgos seguridad.

1.8. Objetivos Específicos

- Realizar un estudio comparativo entre los diferentes estándares de aseguramiento de aplicaciones web, para identificar cuál de ellas abarca los aspectos más relevantes de seguridad.
- Diseñar un modelo de evaluación de seguridad informática para las aplicaciones WEB de la institución.
- Identificar, vulnerabilidades y riesgos relacionados con la seguridad en los aplicativos web de la institución.
- Diseñar un manual de buenas prácticas de seguridad para el desarrollo de aplicaciones WEB, dentro de la institución.

CAPITULO II

MARCO TEÓRICO Y ANÁLISIS CONCEPTUAL DEL ESTADO DEL ARTE

2.1. Antecedentes del estado del arte

Al constituirse como necesaria e indispensable la utilización de aplicaciones web para algunas organizaciones, se torna importante el estudio del aseguramiento de mencionadas aplicaciones, por ello se ha desarrollado diversos estándares que permiten analizar qué tan seguro es la estructura de la aplicación. Por lo expuesto anteriormente varios autores han desarrollado diversos estudios de investigación sobre el tema, cuyos resultados han proveído una guía de las mejores prácticas a tomarse en consideración. A continuación detallamos cada uno de la investigación y que han aportado a la comunidad informática.

En la investigación desarrollada por Dharmesh M Mehta, que titula "Effective Software Security Management", se analiza la importancia del aseguramiento de cualquier aplicación, considerando que las empresas que entiendan a la seguridad de aplicaciones como un problema multidimensional necesitan reconocer de que el desarrollo del ciclo de vida del software requiere una transformación en diferentes fases para apoyar la seguridad de aplicaciones.

Así también el "Estudio De Metodologías Para Pruebas De Penetración A Sistemas Informáticos" desarrollado por el Ing. Agustín López del Instituto Técnico Nacional de la Ciudad de México, realiza el análisis de tres metodologías de pruebas de penetración a aplicaciones (NIST SP800-115, EC-Council LPT y OSSTMM), evaluando semejanzas y diferencias entre cada una de ellas, teniendo como resultado criterios para la aplicación de cada una de las metodologías para el aseguramiento de aplicaciones.

Por otro lado el estudio realizado por: Carmen Torrano-Gimenez, Alejandro Perez-Villegasy Gonzalo Alvarez que titula " WASAT- A New Web Authorization Security Analysis Tool", presenta un análisis realizado sobre la aplicación WASAT, la misma que ha sido diseñada para la evaluación de la seguridad de los diferentes esquemas de autenticación relacionados con la web.

EL estudio realizado por Fu Quanlin del departamento de Ciencias Computacionales e Ingeniería de la Universidad Shanghai Jiao Tong, habla acerca de la "Web Application Security Detection and Measure Based on OWASP "; este trabajo se presenta el método de detección de la seguridad de aplicaciones web y medida basada en las estadísticas y documentos de OWASP, el mismo que disminuye el riesgo de la seguridad de aplicaciones web, y el proyecto real en el que se basan indica que este método puede aumentar la conciencia de la seguridad al tiempo que mejora la seguridad de aplicación web.

Efectividad de OWASP Para Proteger Aplicaciones Web Contra Inyección de SQL, Manuel López Arredondo, Guadalajara; es un estudio del nivel de riesgo al que se encuentran expuestas las aplicaciones web , mediante la explotación de las vulnerabilidades de inyección de SQL, así como del nivel de efectividad de las técnicas de OWASP (Open Web Application Security Project) para mitigar ésas vulnerabilidades.

En el Ecuador el tema planteado también ha sido analizado en trabajos similares, debido a la importancia que ha tomado el tema de seguridad de la información y al creciente porcentaje de empresas que trabajan con aplicaciones web para soportar sus servicios, los trabajos generados se han enfocado en determinar los niveles de riesgos que poseen las aplicaciones web cuando no han sido construidos en base a estándares de seguridad, además de analizar los diversos marcos de referencia que pueden ser utilizados para la construcción de una aplicación web segura:

Entre los trabajos de investigación más destacados tenemos los siguientes:

"Seguridad en Entornos Web para Sistemas de Gestión Académica desarrollado por René Guamán Quinche", en cuyo trabajo estudia los ataques más comunes que afectan a los sistemas Web, como son los diferentes ataques como son la Inyección SQL y XSS. Además se ha revisado ampliamente la literatura sobre políticas de seguridad con el fin de tener una visión general de las principales normas, reglamentos y protocolos a seguir para proteger los sistemas Web.

Como aporte de este proyecto se puede destacar el modelo de prevención generado en base a las vulnerabilidades detectadas por los métodos de inyección además de las vulnerabilidades detalladas por OWASP.

"Estrategias de Seguridad para aplicaciones web desarrolladas en asp.net para el Instituto Tecnológico Sudamericano a nivel de autenticación y privilegios de usuario", desarrollado por Diego Armando Morocho Herrera, este estudio nos muestra la importancia de generar mecanismo de seguridad para las aplicaciones web, identificando cuales son las vulnerabilidad de los sistemas informáticos generados (Morocho Herrera, 2011).

"Análisis de las aplicaciones web de la Superintendencia de Bancos y Seguros, utilizando las recomendaciones Top Ten de OWASP para determinar los riesgos más críticos de seguridad e implementar buenas prácticas de seguridad para el desarrollo de sus aplicativos." desarrollado por Salgado Yánez, Ángel Lenin (Salgado Yanez, 2014), quien en su investigación no provee los beneficios de utilizar el estándar de seguridad en aplicativos web, OWASP al momento de identificar las vulnerabilidades que posee nuestras aplicaciones.

2.2. Marco teórico

2.2.1. Aplicaciones Web.

En Ingeniería de software una aplicación Web es una aplicación a la cual se accede través de una red como Internet o una intranet, generalmente haciendo uso de un navegador web. En los últimos tiempos las aplicaciones web se han convertido en las más populares en el ámbito de desarrollo de aplicaciones, debido a que utilizan menos recursos que una aplicación normal de escritorio, utilizando navegadores web para su ejecución, los mismos que son considerados clientes livianos, puesto que no se requiere instalar grandes paquetes de software en cada cliente y se puede actualizar y mantener las aplicaciones de manera eficiente sin comprometer el estado de los sistemas.

Las páginas web utilizan protocolos de comunicación que permiten la comunicación entre procesos, En el entorno de Internet, lo protocolos utilizados

forman parte de un conjunto de protocolos que trabajan y se relación entre sí, denominado TCP/IP. Los protocolos más utilizados son: HTTP, HTTPS, FTP, SMTP.

En la actualidad las aplicaciones Web utilizan una estructura de tres niveles, en el cual en su forma más común, el navegador Web ofrece la primera capa que constituye la interfaz para el usuario, una capa intermedia lógica y de servicios en donde se encuentra la lógica del negocio, constituida como un motor capaz de usar alguna tecnología Web dinámica (PHP, ASP, ASP.NET, CGI, etc.) y por último, la capa de datos que constituye la base de datos. (Luján Mora, 2001)

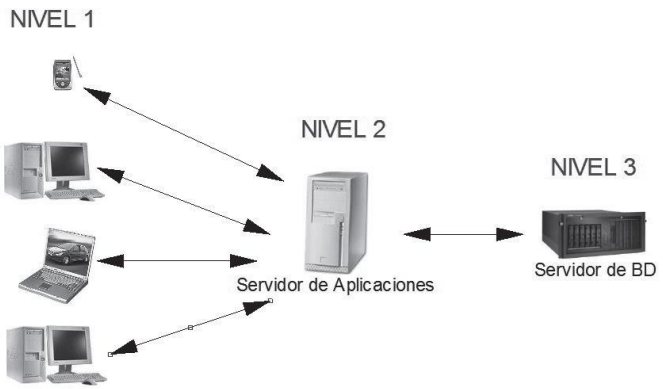


Figura 1 *:* Arquitectura de tres niveles, la arquitectura en tres niveles las aplicaciones al nivel del servidor son descentralizadas de uno a otro, es decir, cada servidor se especializa en una determinada tarea, (por ejemplo, servidor web/servidor de bases de datos).

Fuente:(Ferrer Martinez, 2012)

2.2.1.1. Servicios Web.

Los Servicios Web son aplicaciones modulares auto descriptivas. La arquitectura se describe como el envoltorio del código de aplicación. Este envoltorio proporciona medios estandarizados para la descripción de los Servicios Web y su función. El aspecto más interesante de los Servicios Web es que cualquier usuario de XML puede acceder a ellos independientemente de la plataforma, lenguaje o modelo de objetos que utilice. (Patrick Cauldwell, 2002, pág. 19)

La infraestructura sobre la que se construyen los servicios Web está formada por los siguientes elementos:

- *Servicio de directorio*: Provee de la localización centralizada de un servicio Web específico, utilizando para aquello el servicio UDDI.
- *Servicio de localización:* "Localizan uno o más documentos que describen un servicio Web mediante el WSDL" (Gallegos Varela , pág. 99).
- *Descripción de los servicios Web*: Describe los métodos y acciones que puede ser llevados a cabo por un servicio Web.
- *Formatos de transmisión:* "Para permitir una comunicación lo más universal posible, se utilizan protocolos estándares tales como HTTP-GET, HTTP-POST y SOAP" (Gallegos Varela , pág. 100).

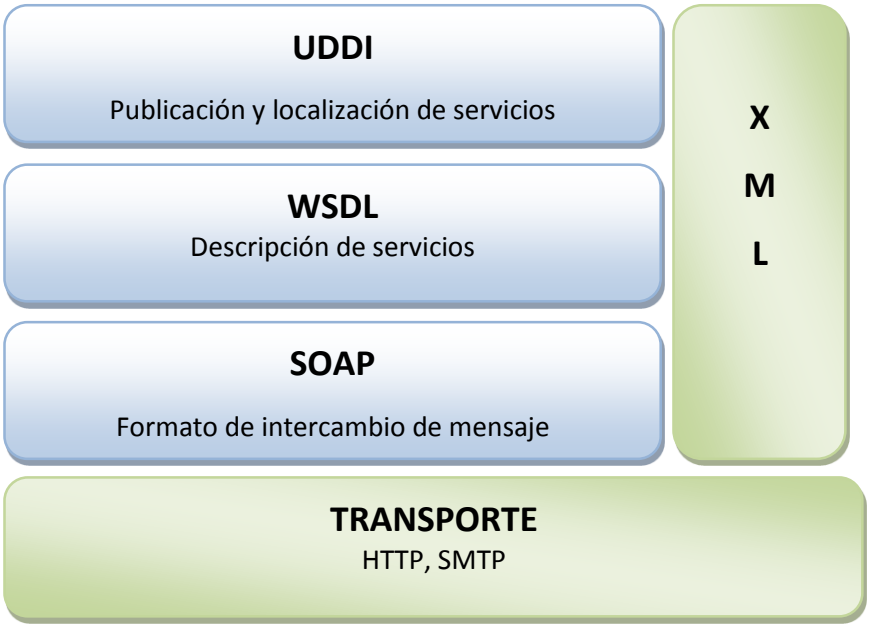


Figura 2 *:* Infraestructura de un Servicio WEB

2.2.1.2. Seguridad en las aplicaciones WEB.

Las organizaciones necesitan adoptar una serie de estándares, normas y reglas, así como controles que brinden un alto grado de seguridad sobre la información que se maneja dentro de la organización; se vuelve indispensable asegurar que los recursos del sistema de información sean utilizados de forma correcta y de acuerdo al personal autorizado.

Al aplicar medidas de seguridad sobre la información se pretende garantizar la intimidad y confidencialidad de la información a usuarios o clientes de una organización; por lo cual las organizaciones deben plantearse medidas que aseguren que la información y los recursos se encuentren protegidos siempre que se encuentren expuestos sus servicios a la red de datos.

Las aplicaciones Web frente a las aplicaciones de escritorio permiten utilizar de manera eficiente los recursos, pero al mismo tiempo se encuentran expuestos a una serie de amenazas y un notorio riesgo de acceso y mal uso de los aplicativos e información existentes, por lo cual se les clasifica como los sistemas más críticos donde la seguridad es significativa, es así que todas las aplicaciones web deben contar con mecanismos de protección (Serrao, Aguilera Díaz, & Cerullo, 2010).

Los aspectos más críticos que se deben asegurar en una aplicación Web son los siguientes:

- **Disponibilidad***:* La disponibilidad hace referencia a la condición de la información de encontrarse a disposición y accesible a personal autorizado, sin interrupciones no autorizadas de los recursos informáticos
- **Integridad**: Propiedad de la información en la cual ninguna persona no autorizada a de poder modificar la información transmitida o almacenada.
- **Confidencialidad**: Es la propiedad de la información que imposibilita su divulgación, además de evitar el acceso a sistemas no autorizados. Asegurando que a la información solo se accedida por quien es autorizado para ello.
- **Autenticidad:** Es la propiedad que determina que el origen de un mensaje pueda ser perfectamente identificado, confirmando la identidad del generador de la información.

2.2.1.2.1. Seguridad de la información.

En términos generales es probable que se llegue a confundir el término de seguridad informática con la de seguridad en la información, pero al hablar de

seguridad de la información se hace referencia a todo lo que puede contener información y no necesariamente en un medio informático.

"La seguridad de la información se define como un conjunto de medidas preventivas, técnicas y organizativas de una institución que permiten asegurar y proteger la confidencialidad, integridad y disponibilidad de la información" (Salgado Yanez, 2014, pág. 28).

2.2.1.2.2. Ataques más comunes a las aplicaciones web.

En términos informáticos un ataque es la acción o método utilizado por un individuo, mediante un sistema informático, que intenta explotar las debilidades de seguridad de los sistemas informáticos (servidor, un equipo de cómputo, una red) tomando el control, desestabilizándolos o causando daños permanentes, los ataque informático siempre son efectuados mediante el Internet. Este se realiza con la finalidad de:

- Obtener accesos a una aplicación
- Robar información de la empresa, de los procesos de esta, clientes (cuentas bancarias, dirección, teléfono)
- Afectar el funcionamiento normal del servicio que presta la organización
- Utilizar el sistema de un usuario como un "rebote" para un ataque.
  (Cabrera García, García Castro, Salinas Romero, Montalvo Gonzales, & Rodríguez Arce, 2009)

Las aplicaciones Web al encontrarse alojadas en el Internet y en la Intranet son las más vulnerables a los ataques que pueden comprometer a la información que se administra, corriendo un alto riesgo si es que no se ejecutan las medidas de protección adecuadas, por lo cual , el desarrollador de aplicaciones no sólo debe concentrarse en los requerimientos del usuario, sino además en los eventos que puedan interferir con la integridad del software y la información que éste maneja (Steve, Cross, Kapinos, Meer, & Muttik, 2011).

Entre los ataques más comunes podemos citar a continuación los más relevantes:

Code Injection*:* Es el término general que se le da a todos los tipos de ataques que consisten en la inyección de código que luego es interpretado / ejecutada por la aplicación. Por lo general se hacen posibles estos tipos de ataques debido a la falta de validación de datos de entrada / salida adecuado (OWASP FOUNDATION, 2013).

Remote Code-Inclusion: El atacante fuerza una aplicación para cargar los archivos de código arbitrario desde una ubicación remota. El atacante podría usar esto para tratar de cargar las versiones antiguas de los archivos de la biblioteca de los cuales ya se tienen conocido las vulnerabilidades, para cargar archivos que el atacante coloca en la máquina remota durante un ataque previo, así como a modificar la funcionalidad de la aplicación específica de forma inesperada (CAPEC, 2014).

Sql Injection: Es una técnica utilizada para la manipulación de los servicios Web que envían a un sistema administrador de base de datos para alterar, insertar o eliminar datos de una base de datos.

Cross-Site Scripting*:* Es una técnica conocida también como XSS"HTML Injection", Según el documento (OWASP FOUNDATION, 2013) manifiesta que Cross-Site Scripting es un ataque común que:

> Intenta manipular los parámetros de entrada que recibe la aplicación para que genere una salida maliciosa. Se puede encontrar un XSS cuando la aplicación no valida nuestra entrada y genera la salida que se encuentra bajo nuestro control. Esta vulnerabilidad genera varios tipos de ataques, por ejemplo, robar información confidencial (tales como cookies de sesión) o tomando control del navegador de una victima. (pág. 201)

Web Spoofing*:* Es un tipo de ataque en el que el atacante crea una convincente copia falsa de todo un sitio web. El falso sitio se parece al real: tiene todas las mismas páginas y enlaces. Sin embargo, el atacante controla la Web falsa, para que todo el tráfico de red entre el navegador de la víctima y la Web pase por el atacante. Para poder llevar a cabo este ataque es necesario contar con tres; el atacante, atacado y un sistema suplantado.

Denegación De Servicios: Es un ataque que afecta directamente a la disponibilidad del sistema, Su principal objetivo es el de impedir al proveedor de servicios el recibir o responder a mensajes.

2.2.2. ISO 27000.

La ISO 27000 es un conjunto de estándares emitidos por la Organización Internacional para la Estandarización y la Comisión Electrotécnica Internacional que incluye las normas para la Seguridad de la Información, elaborada para dar un modelo de establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un Sistema de Gestión de la Seguridad de la Información (SGSI) (ISO/IEC 27000:2005, 2014).

Las diferentes normas incluidas en la serie ISO 27000; explican los pasos a seguir por una organización para lograr la implantación un sistema de gestión de seguridad de la información (SGSI).

2.2.2.1. Familias de las Normas ISO 27000.

ISO 27000: Contiene la descripción general y vocabulario a ser empleado en toda la serie 27000. Se puede hacer uso para entender con claridad tanto la serie como la relación entre los distintos documentos que la constituyen.

UNE-ISO/IEC 27001: Es el estándar más conocido de la familia que proporciona requisitos para un sistema de gestión de seguridad de la información (SGSI). Siendo esta la norma certificable por auditores externos los SGSI de las organizaciones (El portal de ISO 27001 en Español, 2013).

ISO 27002: Es una guía de buenas prácticas. Realiza una descripción de los objetivos de control y controles en cuanto a seguridad de la información. Está constituida por 11 dominios, 39 objetivos de control y 133 controles.

ISO 27003: Provee de una guía para la planificación y ejecución de un SGSI e información que hace referencia tanto al uso del modelo PDCA como de los requisitos de sus diferentes etapas de implementación.

ISO 27004: Detalla en forma específica las métricas y las técnicas de medida que se aplican para determinar la efectividad de la implantación de un SGSI y de los controles vinculados.

ISO 27005: Es una guía de Gestión del Riesgo de la Seguridad de la Información y sirve de apoyo a la ISO 27001 y a la implantación de un SGSI.

2.2.2.2. ISO 27001.

ISO / IEC 27001: 2013 especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un SGSI en el contexto de la organización. Además de especificar los requisitos para la evaluación y el tratamiento de los riesgos de seguridad de información adaptados a las necesidades de la organización (ISO/IEC 27000:2005, 2014).

Los requisitos para la implementación de controles de seguridad son genéricos y adaptados a las necesidades de las organizaciones sin importar tipo, tamaño y naturaleza. La Norma ISO 27001 adopta el modelo del proceso Planear-Hacer-Chequear- Actuar (PDCA), el cual se puede aplicar a todos los procesos SGSI

2.2.2.3. ISO 27002.

El estándar ISO/IEC 27002:2005 fue creado con el objetivo de proporcionar la debida información a los responsables de la implementación de seguridad de la información. Es considerado como una buena práctica para desarrollar y mantener normas de seguridad en una organización y así mejorar la confiabilidad de la seguridad de la información. En él se definen las estrategias de 133 controles de seguridad organizados bajo 11 dominios. (Hardy & Heschl, 2008)

A continuación se detalla los 11 dominios que pertenecen al marco de trabajo para el desarrollo de un Sistema de Gestión de Seguridad de Información, que deberían ser implementados en la organización:

- La política de seguridad.
- Organización para la seguridad.
- Clasificación de activos y su control.
- Seguridad del personal.
- Seguridad física y del entono.

- Comunicaciones y gestión de operaciones.
- Control de acceso.
- Adquisición, desarrollo y mantenimiento de sistemas.
- Gestión de incidentes en la seguridad de la información.
- Gestión de la continuidad del negocio.
- Cumplimiento.

Controles y Objetivos de Control: Cada uno de los dominios que pertenecen al marco de trabajo de la ISO 27002, se encuentra conformada por objetivos de control y a su vez por controles que deben ser implementados en la organización para asegurar la información.

La norma ISO 27002 se encuentra conformada por once dominios los mismos que detallaremos a continuación:

1. **Política de Seguridad.**

   Está conformada por un único objetivo de control que es el contar con directrices de la dirección que tomará la seguridad de la información.

2. **Aspectos Organizativos relacionados con la seguridad de la información.**

   Los Objetivos de Control que componen este dominio son la Organización Interna para la gestión de seguridad de la información y Dispositivos para movilidad y teletrabajo

3. **Seguridad ligada a los Recursos Humanos.**

   Este dominio abarca como objetivos de control a la seguridad en la definición del trabajo y los recursos, seguridad en el desempeño de las funciones del empleo y cese o cambio del puesto de trabajo.

4. **Gestión de Activos.**

   Los Objetivos de Control que componen este dominio son: responsabilidad sobre activos, clasificación de la información y manejo de los soportes de almacenamiento.

5. **Control de accesos.**

   Para cumplir con este dominio, es necesario toman en consideración los siguientes objetivos de control: Requerimientos de negocio para el control de

acceso a sistemas y aplicaciones, Gestión de acceso de usuario y sus responsabilidades.

6. **Cifrado.**

   Se debe tomar en consideración contar con controles criptográficos, como objetivos de control.

7. **Seguridad Física y Ambiental.**

   Poseer áreas seguras y la debida seguridad de los equipos, son los objetivos de control, que contemplan este dominio.

8. **Seguridad en la Operativa.**

   Los objetivos de control que componen a este dominio son contar con procedimientos y responsabilidades de manejo, protección contra código malicioso, respaldo de información, registro de actividad y supervisión, control de software en explotación, gestión de vulnerabilidades técnicas y consideraciones de las auditorias de los sistemas de información.

9. **Seguridad de las Telecomunicaciones.**

   La gestión de la seguridad, en las redes y el intercambio de información con partes externas son objetivos de control clave para cumplir con este dominio.

10. **Adquisición, desarrollo y mantenimiento de sistemas.**

    Las necesidades de seguridad de los sistemas, seguridad de los procesos vinculados al desarrollo y soporte y la seguridad de los datos de prueba, son aspectos de control que se los considera en este dominio.

11. **Relaciones con los Suministradores.**

    Los objetivos de control enmarcados en este dominio son: Seguridad de la información en las relaciones con los suministradores y gestión de la prestación del servicio por suministradores.

12. **Gestión de incidentes en la seguridad de la información.**

    La Gestión de incidentes en la seguridad de la información y mejoras es el único objetivo de control incluido en este dominio.

13. **Seguridad de la información en la gestión de la continuidad del negocio.**

    La continuidad de la seguridad de la información y las redundancias son los objetivos de control contemplados en el dominio.

14. **Cumplimiento.** Los dos objetivos de control que forman parte de este dominio son: Cumplimiento de los requisitos legales contractuales y revisión de la seguridad de la información.

2.2.3. OWASP

Es un proyecto de código abierto destinada a la de seguridad en aplicaciones Web, esta comunidad está dedicada a habilitar a las organizaciones para desarrollar, comprar y mantener aplicaciones confiables.

OWASP es reconocido en el mercado de seguridad informática, con un nuevo tipo de entidad. Al ser una corporación libre proporciona información imparcial, práctica y redituable sobre seguridad de aplicaciones informáticas. Una de las principales recomendaciones de OWASP es la de enfocar la seguridad de aplicaciones informáticas tomando en cuenta todas las dimensiones empresariales es decir: personas, procesos y tecnologías.

2.2.3.1. Proyectos OWASP.

OWASP mantiene dos categorías de proyectos: Los de desarrollo y los de documentación. Dentro de la línea de los proyectos de desarrollo de (OWASP FOUNDATION, 2013) podemos destacar los siguientes:

- *Guía OWASP:* Guía detallada sobre la seguridad de las aplicaciones web.
- *Guía de autoevaluación OWASP Top 10*: Documento que se centra en las vulnerabilidades más críticas de los aplicativos web.
- *Métricas:* Proyecto para definir métricas aplicables de seguridad de aplicaciones web.
- *Guía de pruebas:* Es una guía especializada en la prueba de la seguridad de aplicaciones web.
- *ISO 27002:* Documentos de apoyo para organizaciones que realicen revisiones.
- *AppSec FAQ :* Preguntas y respuestas frecuentes sobre seguridad de aplicaciones web.

Por otra parte los proyectos de desarrollo de OWASP son los siguientes:

- *WebScarab:* Aplicación diseñada para el control de vulnerabilidades en las aplicaciones web incluyendo las herramientas proxy.
- *Filtros de validación:* Filtros genéricos de seguridad perimetral que los desarrolladores pueden usar en sus propias aplicaciones.
- *WebGoat* : Herramienta de formación en aspectos de seguridad de aplicaciones web.
- *DotNet*: Herramientas para asegurar los entornos .NET.

2.2.3.1.1. Guía OWASP.

La Guía OWASP ha sido re-escrita completamente, ya que se han ocupado de todas las cuestiones de seguridad en aplicaciones web, desde las más antiguas, como la inyección SQL, hasta las modernas tales como la suplantación de identidad, manipulación de tarjetas de crédito, fijación del período de sesiones, falsificaciones de petición en sitios cruzados, el cumplimiento de las reglas cuestiones de privacidad. (Van Der Stock, 2005)

La mayoría de los controles que se encuentran incluidos en la Guía OWASP 2.0 se encuentran influenciados por algunos requerimientos de estándares nacionales o marcos de control como lo son COBIT Y LA ISO 27002.

La Posición de OWASP dentro del marco legislativo: El siguiente diagrama muestra donde se ubica OWASP.

Figura 3: La posición de OWASP dentro del marco legislativo.- Las organizaciones necesitan establecer una política de seguridad de la información fundada en

legislación nacional relevante, regulación industrial, acuerdos de comercio, y guías de mejores prácticas complementarias, tales como OWASP

Fuente: (OWASP FOUNDATION, 2013)

Modelado De Riesgo De Amenaza: Es recomendable que el modelado de riesgo sea elaborado durante el diseño de la aplicación, utilizando controles que permitan evaluar el riesgo de amenaza, de otra forma las organizaciones tendrán que enfrentarse a controles inútiles y no suficientes.

OWASP utiliza el proceso de modelado de amenaza de Microsoft, la misma que proporciona una herramienta desarrollado en .NET para permite dar seguimiento y visualización de árboles de amenazas.

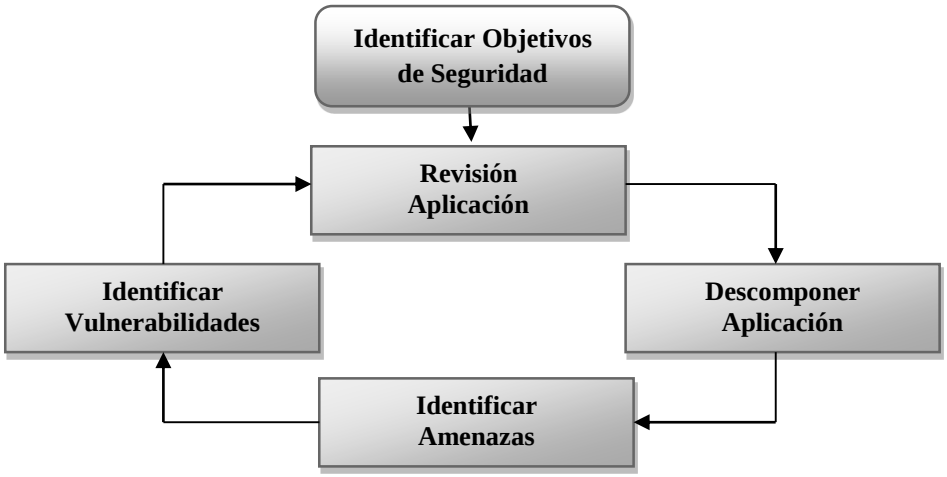


Figura 4: Flujo del Modelo de Amenazas.

Identificar objetivos de seguridad.- Los objetivos de seguridad en aplicaciones necesitan ser divididos en:

- Identidad
- Reputación
- Financiero
- Privacidad y regulaciones

Visión general de la aplicación.- Una vez que los objetivos han sido definidos, la aplicación debería ser analizada, de manera primordial los diagramas de componentes UML, los mismos que permitirán determinar:

- Componentes
- Flujos de datos
- Límites de confianza

La mejor manera de hacer esto es obtener la documentación de arquitectura y diseño de la aplicación.

Descomponer la aplicación.- Una vez que la arquitectura de la aplicación ha sido entendida, la aplicación necesita ser desplegada, esto significa que las características y módulos que tienen un impacto de seguridad necesitan llegar al más bajo nivel

Documentar las amenazas conocidas.- Una vez que la aplicación haya sido disgregada, se debe iniciar con la identificación de vulnerabilidades y a su vez de las amenazas consecuentes. Es así que se debe concentrar en los riesgos que son conocidos y que pueden ser fácilmente demostrados utilizando herramientas o el seguimiento de errores.

Metodologías de Pruebas.- La metodología de pruebas de intrusión de aplicación web OWASP se encuentra basada en el enfoque de caja negra. El auditor que realizará las pruebas tiene poca, o ninguna, información sobre la aplicación que va a ser comprobada. El modelo de pruebas consta de**:**

- **Auditor:** Persona encargada de realizar las actividades de comprobación de la aplicación Web.
- **Herramientas y metodología**: El núcleo de este proyecto de guía de pruebas
- **Aplicación:** La caja negra sobre la que realizar las pruebas

Las pruebas se dividen en 2 fases:

- Modo pasivo: En esta fase el encargado de la auditoría estudia y comprende la lógica de la aplicación y recopila información. Al final de esta fase esta persona debería comprender cuales son todos los puntos de acceso (puertas) de la aplicación (p.e. cabeceras HTTP, parámetros, cookies).
- Modo activo: En esta fase el auditor a cargo de la comprobación empieza a realizar las pruebas usando la metodología descrita en los siguientes apartados.

OWASP Top 10.- Es un documento que se enfoca en lograr la conciencia de gran alcance para la seguridad de aplicaciones web, identificando los riesgos de seguridad más relevantes. La lista representa un amplio consenso acerca de cuáles son los defectos más críticos de seguridad de aplicaciones web.

"El objetivo principal del Top 10 es educar a los desarrolladores, diseñadores, arquitectos, gerentes, y organizaciones; sobre la consecuencias de las vulnerabilidades de seguridad más importantes en aplicaciones web". El Top 10 provee técnicas básicas sobre cómo protegerse en estas áreas de alto riesgo y también provee orientación sobre los pasos a seguir. (OWASP FOUNDATION, 2013)

Auditoría OWASP TOP 10: El enfoque de un trabajo de estas características es revisar una aplicación en busca de las debilidades más habituales y que tienen un impacto mayor en la seguridad de un sistema.

Los calificativos de los riesgos en el Top 10 proceden del tipo de ataque al que se está expuesto, el tipo de debilidad o el tipo de impacto que causan. Por lo cual se ha optado tomar los nombres que reflejan con precisión los riesgos al que se encuentran expuestos las aplicaciones Web.

A continuación de detalla el Top 10 de Riesgos de Seguridad de aplicaciones:

A1: Inyección: Se produce cuando datos no confiables o maliciosos son enviados mediante una aplicación como parte de una consulta hacia un intérprete, mediante las consultas SQL, LDAP, Xpath o NoSQL.

A2: Autenticación y Gestión de Sesiones: Cuando las funciones de autenticación y gestión de sesiones son vulnerables a ataques, estos pueden ser aprovechadas por atacantes quienes obtienen explotar otras fallas de implementación.

A3: Cross-Site Scripting (XSS): Ocurren cuando una aplicación web permite tomar información no confiable y los envía al navegador web sin haber realizado previamente una validación y codificación apropiada.

A4: Referencias inseguras a objetos directos: Una aplicación web es vulnerable a ataques, cuando ha sido programada de manera que las referencias a objetos de

implementación interna son expuestas. Sin un debido control de acceso, estas referencias pueden ser manipuladas por los atacantes y a la vez pueden acceder a datos no autorizados.

A5: Configuración errónea de Seguridad: Para referirnos a una aplicación segura, esta requiere que se encuentre definidos, implementados y mantenidos los siguientes aspectos de seguridad: Marcos de trabajo, servidore de aplicación y web, base de datos, y plataforma. Esto incluye mantener todo el software actualizado, incluidas las librerías de código utilizadas por la aplicación.

A6: Exposición de datos sensibles: Una aplicación se encuentra vulnerable a ataques cuando los datos sensibles no son cifrados de manera adecuada, es así cuando son utilizadas algoritmos débiles, y particularmente técnicas débiles de hashing de contraseñas.

A7– Ausencia de control de acceso a funciones: Para mantener una aplicación web segura se necesita implementar la verificación de control de acceso en el servidor cuando se solicita el acceso a cada función.

A8: Cross-Site Request Forgery (CSRF): CSRF aprovecha la situación en el cual un alto porcentaje de aplicaciones web permiten predecir los detalles de una actividad en particular a los atacantes.

Este tipo de ataque obliga al navegador de una víctima autenticada a enviar una petición HTTP falsificado, incluyendo la sesión del usuario y cualquier otra información de autenticación incluida automáticamente, a una aplicación web vulnerable. (OWASP TOP 10 -2013, 2013)

A9: Insuficiente protección de la capa de transporte: En la mayoría de las aplicaciones web, la configuración para algunos componentes tales como las librerías, los *frameworks* y otros módulos de software casi siempre funcionan con todos los privilegios. Si uno de estos componentes vulnerables es atacado este error de seguridad podría facilitar la intrusión en el servidor o una perdida seria de datos.

A10: Redirecciones y reenvíos no validados Las aplicaciones web habitualmente tiene que redirigir y reenviar a los a los usuarios hacia otras páginas o sitios web para culminar sus transacciones, y a la vez utilizan datos que no son no confiables para poder identificar la página de destino. Si la aplicación web no posee una validación apropiada, permite al atacante redirigir a las víctimas hacia sitios que contengan *phishing* o malware.

2.2.4. *CWE/SANS Top 25.*

CWE con apoyo del SANS (CWE/SANS) presentan su posicionamiento de los errores de programación más comunes y críticos que pueden conducir a graves vulnerabilidades de software. Son comunes de encontrar y fácil de explotar. El peligro consiste en frecuencia que permitirá a los atacantes tomar por completo el software, robar datos, o evitan que el software funcione en absoluto. Ranking y descripción sobre los veinticinco errores más peligrosos de software, es decir, los riesgos más críticos de seguridad, donde se observa cierta similitud entre los primeros descritos por el OWASP, como se observa a continuación, presentados de mayor a menor severidad.

La lista Top 25 es una herramienta para educar a los desarrolladores sobre los mecanismos que permiten prevenir los tipos de vulnerabilidades que pueden afectar a la seguridad de las organizaciones, que cuentan con aplicativos para mejorar la eficiencia de sus procesos, identificando y evitando los errores más comunes de seguridad.

Los investigadores de seguridad de software pueden utilizar el Top 25 para centrarse en un estrecho pero importante subconjunto de todos los fallos de seguridad conocidos. Por último, los administradores de software y los directores de TI pueden utilizar la lista de Top 25 como una vara de medir el progreso en sus esfuerzos por asegurar su software.

2.2.4.1. Top 25 Errores de Software.

El listado los errores de software se dividen en tres categorías, según su grado de severidad y vulnerabilidades del sistema:

1. Interacción insegura entre componentes.

2. Gestión de Recursos de Riesgos
3. Defensa porosa

Interacción insegura entre componentes: Esta vulnerabilidad esta relacionadas con formas de inseguridad en que se envían y reciben datos entre distintos componentes, módulos, programas, procesos, hilos o sistemas.

1. CWE-89: Inyección SQL
2. CWE-78: Inyección de Comandos al Sistema Operativo
3. CWE-79: Cross-Site Scripting
4. CWE-434: Carga NO Restringida de Archivos con Código Malicioso
5. CWE-352: Falsificación de Petición en Sitios Cruzados (CSRF)
6. CWE-601: Redirección de URL a Sitios NO Confiables

Gestión de Recursos de riesgos: Los puntos débiles de esta categoría son ocasionadas cuando el software no administra correctamente la creación, uso, transferencia, o la destrucción de los recursos del sistema.

1. CWE-120: Desbordamiento de Buffer
2. CWE-22: Directorio Transversal
3. CWE-494: Descarga de Código sin Verificación de Integridad
4. CWE-131: Calculo Incorrecto del tamaño del Buffer
5. CWE-190: Integrador de Desbordamiento
6. CWE-829: Inclusión de funcionalidad desde esferas de control.
7. CWE-676: Uso de funciones potencialmente peligrosas.
8. CWE-134: Formato String sin control.

Defensa Porosa: Estas deficiencias están relacionadas con las técnicas defensivas que a menudo han sido usadas, abusadas, o simplemente ignoradas.

1. CWE-306: Falta de autenticación para funciones críticas
2. CWE-798: Uso de credenciales codificadas
3. CWE-311: Falta de cifrado sobre datos sensibles
4. CWE-807: Dependencia sobre entradas no confiables.
5. CWE-732: Asignación incorrecta de permisos a recursos críticos
6. CWE-327: Utilización de un algoritmo de cifrado revelado

7. CWE-868: Falta de autorización
8. CWE-250: Ejecución con permisos innecesarios.
9. CWE-863: Autorización Incorrecta
10. CWE-307: Restricción inadecuado de intentos de autenticación.
11. CWE-759: Uso de un HASH de una sola dirección

2.2.5. WASC (WEB APPLICACTION SECURITY CONSORTIUM)

Los miembros de Web Application Security Consortium, han unido esfuerzos de cooperación para desarrollar y promover un estándar de organización y clasificación de amenazas de seguridad web. Lo cual provee de un lenguaje común a desarrolladores, fabricantes de software, personal de seguridad y auditores, para tratar aspectos afines con la seguridad.

> El documento generado por WASC proporciona un entendimiento y comprensión más profunda de los riesgos de seguridad que amenazan los sitios web, mejora las prácticas de programación segura para prevenir problemas de seguridad durante el desarrollo de aplicaciones además sirve como guía para determinar si los sitios web han sido correctamente diseñados, desarrollados, y revisados contra todas las amenazas conocidas. (Web Application Security Consortium, 2014, pág. 1)

2.2.5.1. WASC Clasificación de amenazas.

Las amenazas son divididas de acuerdo a 6 criterios de seguridad, las mismas que se detallaran a continuación.

1. Autenticación
2. Autorización
3. Ataques en la parte cliente
4. Ejecución de comandos
5. Revelación de información
6. Ataques Lóg

Autenticación: Cubre ataques cuyo objetivo es el método utilizado por un sitio web para validar la identidad de un usuario, servicio o aplicación**.**

1. Fuerza bruta

2. Autenticación insuficiente
3. Débil validación en la recuperación de contraseñas.

Autorización*:* Cubre los ataques que tienen como objetivo un método de los sitios web para determinar si un usuario, servicio o aplicación tiene los permisos necesarios para ejecutar una acción solicitada (Web Application Security Consortium, 2014).

1. Predicción de Credenciales/Sesión
2. Autorización Insuficiente
3. Expiración de Sesión Insuficiente
4. Fijación de Sesión

Ataques en la parte cliente*:* Se centra en el abuso o aprovechamiento de los usuarios de los sitios web. Cuando un usuario visita un sitio web, se establece una relación de confianza entre las dos partes, tecnológica y psicológicamente.

1. Suplantación de Contenido
2. Cross-site Scripting

Ejecución de comandos: Abarca los ataques diseñados para ejecutar comandos remotos en el sitio web. Todos los sitios web utilizan datos suministrados por el usuario para satisfacer peticiones (Web Application Security Consortium, 2014).

1. Desbordamiento de Buffer
2. Ataques de Formato de Cadena
3. Inyección LDAP
4. Comandos de Sistema Operativo
5. Inyección de código SQL
6. Inyección de código SSI
7. Inyección XPath

Revelación de información: Aborda los ataques diseñados para adquirir información específica del sistema sobre un sitio web. La información específica del sistema incluye la distribución de software, números de versión y niveles de parcheado. La información puede contener la ubicación de ficheros de backup y ficheros temporales.

1. Indexación de Directorio

2. Fuga de Información
3. Path Traversal
4. Localización de Recursos Predecibles

Ataques lógicos: Se centra en el abuso o explotación del flujo lógico de una aplicación web. La lógica de la aplicación es el flujo de procedimientos esperados para realizar una cierta acción (Web Application Security Consortium, 2014).

1. Abuso de Funcionalidad
2. Denegación de Servicio
3. Anti-automatización Insuficiente
4. Validación de Proceso Insuficiente

2.2.6. Auditoria Informática

2.2.6.1. Concepto.

> Consiste en el examen objetivo, crítico, sistemático y selectivo de las políticas, normas, prácticas, procedimientos y procesos, para dictaminar respecto a la economía, eficiencia y eficacia de la utilización de los recursos de tecnologías de la información, la oportunidad, confiabilidad, validez de la información y la efectividad del sistema de control interno asociado a las tecnologías de la información y a la entidad en general. (General, 2009, pág. 3)

2.2.6.2. Objetivos.

Debido a la importancia que ha tomado los sistemas de información automatizados dentro de las organizaciones, la auditoria en el ambiente informático se ha tornado de vital importancia para mejorar el desempeño de los sistemas y así incrementar la seguridad y confiabilidad dela información que produce. La evaluación a estos sistemas devuelve importantes hallazgos que permiten establecer controles que disminuyen amenazas que pueden comprometer la integridad de la información.

2.2.6.3. Proceso de Auditoría Informática.

La metodología de auditoría establecida por los autores (Yañez de la Melena & Ibsen Muñoz, 2011), determinan dentro del proceso de auditoria tres fases de

ejecución denominadas: planeación, ejecución y comunicación de resultados; en cada una de ellas se establecen y ejecutan un conjunto de actividades y tareas específicas.

1. Planeación de la auditoría: La fase de planeación de la auditoria incluirá los siguientes puntos:
   - Plan de auditoría preliminar.
   - Comprensión de la organización, procesos de negocio y sistemas
   - Definición del programa y alcance de la auditoría
2. Ejecución del plan*:* La fase de ejecución de la auditoria incluirá los siguientes puntos:
   - Evaluación del control interno:
   - Diseño de las pruebas de auditoría
   - Ejecución de las pruebas de auditoría
   - Evaluación del resultado de las pruebas de auditoría
3. Conclusión y preparación de informe: Esta es la última fase del proceso de auditoría, en la cual se resume los resultados obtenidos en las fases anteriores, incluyendo los siguientes puntos:
   - Elaboración del informe con los resultados de la auditoría:
   - Seguimiento a las observaciones de la auditoría

2.2.6.4. Auditoria Basada en Riesgos.

La auditoría basada en riesgos se refiere a la identificación y análisis de los riesgos relevantes que existen dentro del ambiente tecnológico que pueden interrumpir la consecución de los objetivos, la auditoria con enfoque basado a riesgos permite determinar las actividades de control.

Los objetivos contemplados dentro de la auditoria basada en riesgos son: Valorar los riesgos tecnológicos de la organización, diseñar y ejecutar procedimientos de auditoría adicionales que respondan a los riesgos valorados y reduzcan a un nivel aceptablemente bajo los riesgos y emitir un reporte de auditoria.

Para cumplir con los objetivos planteados, se requiere tomar en consideración el apetito de riesgos de la organización, que se refiere al nivel de riesgo que una organización está preparada para tolerar, así mismo el riesgo inherente que hacer

referencia al nivel de riesgo propio de la actividad sin tomar en consideración el efecto de los controles, el riesgo residual que permite determinar el nivel resultante de riesgo después de aplicar los controles.

2.3. Marco Conceptual

Amenaza de Seguridad: "Es un evento que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos" (Gutiérrez & Tena, 2003, pág. 35).

Ataque: Evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.

Autenticación: Es el acto de establecimiento o confirmación de algo como auténtico.

Autorización: La determinación de los recursos de un usuario, servicio o aplicación al que tiene permiso de acceso. Recursos accesibles pueden ser URL de, archivos, directorios, servlets, bases de datos, rutas de ejecución (OWASP FOUNDATION, 2013).

*Buenas prácticas***:** Es un conjunto análogo de actividades que devuelven execelentes resultado en un determinado contexto y que se espera que, en contextos similares, rindan similares resultados.

CWE/SANS Top 25 Most Dngerous Software: es una lista de los errores más comunes y críticos que llevan a vulnerabilidades graves de software que son fáciles de encontrar y explotar.

Control: Mecanismo que permite atenuar el riesgo inherente, con el fin de disminuir la probabilidad de ocurrencia y/o impacto.

*Denegación de servicio***:** Técnica de ataque que consume todos los recursos disponibles de un sitio web con la intención de hacer uso legítimo imposible.

Impacto: Es la consecuencia sobre un activo de la materialización de una amenaza (Grupo IWI., 2009).

*Fuerza bruta***:** Es un proceso automático de prueba y error que se utiliza para adivinar el "secreto" la protección de un sistema. Ejemplos de estos secretos incluyen nombres de usuario, contraseñas o claves criptográficas (Amaya Tarazona, 2014).

Servicios Web: Un servicio web es una tecnología que utiliza un conjunto de protocolos y estándares que sirven para intercambiar datos entre aplicaciones.

OWASP :(Open Web Application Security Project - Proyecto de seguridad de aplicaciones web abiertas) es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro (OWASP FOUNDATION, 2013).

Protocolo HTTP: Protocolo de transferencia de hipertexto.

Protocolo HTTPS: Protocolo seguro de Transferencia de hipertexto.

Protocolo FTP: Protocolo de transferencia de archivos.

Protocolo SMTP: Protocolo simple de transferencia de correo.

Riesgo: Posibilidad de materialización de una amenaza. Proximidad o posibilidad de un daño (Grupo IWI., 2009).

SOAP: Es un protocolo de comunicación desarrollado por la W3C, que se encuentra basado en XML y que permite el intercambio de mensajes entre sistemas mediante la representación de los mensajes de invocación (argumentos) y respuesta (valor retorno) como documentos XML.

UDDI: Es el directorio de servicios que almacena la descripción de los servicios disponibles, es almacenado en un lenguaje estándar basado en XML, el mismo que admite describir, publicar y encontrar los servicios.

Web Application Security: Ciencia de la seguridad de la información relacionada con el mundo del software Wide Web, HTTP y de aplicaciones web.

Vulnerabilidad: Exposición latente de un riesgo.

WASC Threat Classification: La Clasificación de Amenazas es un esfuerzo para clasificar las debilidades y ataques que pueden llevar a la divulgación de un sitio web, sus datos o sus usuarios.

WSDL: Es un formato estándar basado en XML para describir servicios web y sus interfaces de forma estándar mediante lenguaje XML.

XML-RPC: Es un protocolo basado en XML, estándar para la definición de lenguajes de marcas, para el intercambio de información entre sistemas, es independiente de la plataforma.

CAPITULO III

MARCO METODOLÓGICO

3.1. Metodología de Investigación

El proceso de investigación será desarrollado mediante el método científico, haciendo una combinación de los procesos de inducción y deducción. La investigación teórica utilizará el método documental permitiéndonos obtener un texto formal. El método experimental será utilizado para la realización de pruebas controladas que nos permitirán el entendimiento de los procesos causales.

3.1.1. Método Inductivo.

Estudia los fenómenos o problemas desde las partes hacia el todo, es decir analiza los elementos del todo para llegar a un concepto o ley.

3.1.2. Método Deductivo.

Estudia un fenómeno o problema desde el todo hacia las partes, es decir analiza el concepto para llegar a los elementos de las partes del todo.

3.1.3. Inductivo – Deductivo.

Este método estudia el fenómeno desde la descomposición hasta la construcción, es decir del menor al mayor.

3.1.4. Método Documental.

La investigación de tipo documental, seleccionar y analiza datos que están en forma de documentos producidos por la sociedad para estudiar un fenómeno determinado.

3.1.5. El método experimental.

Este método utiliza procesos sistemáticos y una aproximación científica a la investigación en la cual el investigador manipula una o más variables y controla y mide cualquier cambio en otras variables.

3.2. Enfoque metodológico de la auditoria

El enfoque metodológico propuesto integra el conocimiento aportado por las organizaciones que lideran el desarrollo de los estándares y mejores prácticas en el ámbito de las tecnologías de la información reconocidas a nivel internacional, entregando un marco referencial para realizar auditorías a las tecnologías de

información centradas en los procesos del negocio, los sistemas de información que los soportan y sus actividades de control (Melena Yanez & Muñoz Ibsen, 2015).

3.3. Metodología

Esta constituye una herramienta basado estándar COBIT y la norma técnica ISO/IEC 27002 a los programas de auditorías a las tecnologías de información y comunicaciones.

A continuación, se presentan las etapas que componen la metodología:

a) FASE I. Planificación de la auditoría

1. Plan de auditoria preliminar
2. Comprensión de la organización, procesos de negocio y sistemas
3. Definición del programa y alcance de la auditoría

b) FASE II. Ejecución de la auditoría

1. Evaluación del control interno
2. Diseño de las pruebas de auditoría
3. Ejecución de las pruebas de auditoría
4. Evaluación del resultado de las pruebas de auditoría

c) FASE III. Comunicación de los resultados

1. Elaboración del informe con los resultados de la auditoría
2. Seguimiento a las observaciones de la auditoría (Melena Yanez & Muñoz Ibsen, 2015).

3.4. Síntesis de actividades y productos entregables por etapas

A continuación, se propone las actividades y productos que componen las etapas a cumplir para realizar una auditoría (Melena Yanez & Muñoz Ibsen, 2015).

Tabla 1

Actividades y productos de la fase de planificación de la auditoría

ETAPAS DE LA METODOLOGÍA		ACTIVIDADES QUE SE EJECUTAN	PRODUCTOS DE LA ETAPA
Nº	**DESCRIPCION**		
1	**Plan de auditoría preliminar**	- Elaborar un plan de auditoría con objetivos generales. - Conformar el grupo de trabajo que realizará la auditoría. - Estimar tiempo necesario para realizar la auditoría.	- Plan de auditoría preliminar. - Definición del perfil del personal requerido y asignación de auditores. - Lista con horas estimadas por etapa para realizar la auditoría.
2	**Comprensión de la organización, procesos de negocio y sistemas**	- Levantamiento de información sobre el estado actual y características de la organización, infraestructura, procesos de negocios y sistemas de información que los soportan. - Realizar ficha técnica de los sistemas de información que soportan los procesos de negocio.	- Archivos de trabajo de la auditoría. - Documento con definición de los procesos de negocio y diagramas descriptivos. - Ficha técnica de los sistemas de información que soportan los procesos de negocio.
3	**Definición del programa y alcance de la auditoría**	- Seleccionar los objetivos de control aplicables a los procesos de negocio y sistemas de información. - Elaborar el programa de auditoría detallado. - Confeccionar Carta Gantt del programa de auditoría.	- Lista de objetivos de control que deben ser satisfechos por los procesos de negocio y sistemas de información. - Programa de auditoría detallado. - Carta Gantt del programa de auditoría.

Tabla 2

Actividades y productos de la fase de Ejecución de la auditoría

ETAPAS DE LA METODOLOGÍA		ACTIVIDADES QUE SE EJECUTAN	PRODUCTOS DE LA ETAPA
Nº	**DESCRIPCIÓN**		
4	**Evaluación del sistema de control interno**	- Identificar y documentar los controles existentes en los procesos de negocio y sistemas de información. - Evaluar el diseño y grado de protección que ofrecen los controles existentes. - Identificar y documentar los controles deficientes.	- Lista de controles existentes para los procesos de negocio y sistemas de información. - Lista con el grado de protección de controles existentes para los procesos de negocio y los sistemas. - Lista de deficiencias y debilidades de control interno.
5	**Definición y diseño de las pruebas de auditoría**	- Definir y diseñar pruebas de cumplimiento para los controles claves de los procesos de negocio y sistemas agrupados por técnicas de verificación. - Definir el diseño y alcance de las pruebas sustantivas para datos clave de los procesos y sistemas.	- Definición del alcance de las pruebas de cumplimiento. - Diseño detallado de las pruebas de cumplimiento según técnicas de verificación. - Definición del alcance de las pruebas sustantivas. - Diseño detallado de las pruebas sustantivas.
6	**Ejecución de las pruebas de auditoría**	- Ejecutar pruebas de cumplimiento y sustantivas utilizando técnicas de verificación manuales o asistidas por computador.	- Lista de controles verificados por el auditor. - Soportes de las pruebas de auditoría realizadas.
7	**Evaluación de los resultados obtenidos en las pruebas de auditoría**	- Evaluar los resultados de las pruebas efectuadas. - Desarrollar el análisis de las observaciones de auditoría y puntos mejorables. - Diseñar las conclusiones de auditoría para los resultados no satisfactorios.	- Listado con análisis de observaciones de auditoría para pruebas de cumplimiento y sustantivas. - Conclusiones de los resultados obtenidos.

Tabla 3

Actividades y productos de la fase de comunicación de los resultados

ETAPAS DE LA METODOLOGÍA		ACTIVIDADES QUE SE EJECUTAN	PRODUCTOS DE LA ETAPA
Nº	**DESCRIPCIÓN**		
8	**Elaboración del informe con los resultados de la auditoría**	- Elaborar resume de observaciones. - Desarrollar y aprobar informe preliminar. - Emitir informe preliminar. - Analizar respuesta del servicio al informe preliminar. - Diseñar conclusiones generales y específicas de la auditoría. - Elaborar y aprobar informe final de auditoría. - Emitir informe final de auditoría. - Organizar y cerrar expediente y archivo con hojas de trabajo.	- Resumen de observaciones obtenidas. - Informe preliminar de auditoría. - Documento con el análisis de las respuestas emitidas por el servicio auditado al informe preliminar. - Informe final de auditoría. - Expediente de auditoría con observaciones organizadas y referenciadas adecuadamente.
9	**Seguimiento a las observaciones de auditoría**	- Planificar seguimiento al cumplimiento de las observaciones de auditoría. - Efectuar seguimiento en fechas programadas. - Analizar y evaluar resultados del seguimiento. - Elaborar y aprobar informe de seguimiento. - Emitir informe de seguimiento.	- Programa de seguimiento. - Listado con el resultado del cumplimiento de las observaciones. - Informe de seguimiento.

3.5. FASE I. Planificación de la auditoría

En la primera fase de la auditoría se realizará plan de auditoría preliminar, la cual no se realizará en vista de que no existen auditorias anteriores, pero en cambio se determinará el grupo de trabajo que realizará la auditoría el cual estará integrado por los tesistas, además se estimará el tiempo necesario para realizar la auditoría.

A continuación se pasará a la etapa de comprensión de la organización, procesos de negocio y sistemas e fundamental, se realizará el levantamiento de información sobre el estado actual y características de la organización, infraestructura, recursos humanos y técnicos, procesos de negocios y sistemas de información que los soportan., se elaborará un flujograma de los procesos de negocio que soporta la aplicación, para finalizar con una ficha técnica de los sistemas de información que soportan los procesos de negocio.

A continuación se seleccionarán los objetivos de control aplicables a los procesos de negocio y sistemas de información y se elaborará el programa de auditoría detallado incluyendo su carta Gantt.

3.6. FASE II. Ejecución de la auditoría

La segunda fase de la auditoría comprende un análisis del sistema de control interno de la organización con el objetivo de planificar y realizar las pruebas de cumplimiento y sustantivas que evaluarán si los controles operan de forma adecuada y cumplen con resguardan el cumplimiento de los objetivos y requisitos del negocio.

Iniciaremos con la evaluación de control interno, en el cual se identifica y documenta los controles existentes en los procesos de negocio y son soportado por los sistemas de información, para luego pasar a evaluar el diseño y grado de protección que ofrecen los controles existentes, toda esta información debe encontrarse en una lista que posteriormente nos permita identificar y documentar los controles deficientes.

La siguiente etapa consiste en definir y diseñar las pruebas de auditoria tanto las de cumplimiento para los controles claves de los procesos de negocio y sistemas agrupados por técnicas de verificación como las sustantivas para datos clave de los procesos y sistemas. Para luego pasar a la ejecución de las pruebas de auditoria tanto de cumplimiento como sustantivas utilizando técnicas de verificación manuales o

asistidas por el computador. De lo cual deberán existir la respectiva lista y soportes de las pruebas de auditoria realizadas.

Para finalizar esta fase se evalúan los resultados obtenidos en las pruebas de auditoria, realizando un análisis de las observaciones de auditoría y puntos mejorables para los controles y datos deficientes, identificando las causas, el impacto y las implicaciones de las observaciones para la organización y verificar los estándares y mejores prácticas que no se cumplen. Como fin de esta fase se elaboran las conclusiones de auditoría para los resultados no satisfactorios.

3.7. FASE III. Comunicación de los resultados

Esta es la última fase de la auditoría, en ella se resumen los resultados más significativos obtenidos en las etapas anteriores.

Estos son los insumos para elaborar el informe de auditoría con el cual se comunicará a la alta dirección y a los demás interesados, las observaciones y conclusiones sobre las características de seguridad, calidad y confiabilidad de la información y de los recursos tecnológicos y humanos que intervienen en las actividades de control de los procesos de negocio y sistemas de información.

Organizar y cerrar expediente y archivo con hojas de trabajo. Se elabora el resumen de observaciones que servirá de base para desarrollar y aprobar informe preliminar; luego se analizará respuesta del servicio al informe preliminar para diseñar las conclusiones generales y específicas de la auditoría. Para finalizar con la elaboración y aprobación y emisión del informe final de auditoría, para organizar y cerrar expediente y archivo de trabajo

La etapa de seguimiento a las observaciones de auditoría ya no será realizada ya que se encuentra fuera del alcance del proyecto.

3.8. Estudio Comparativo entre Marcos de Aseguramiento de Aplicativos Web

La existencia de varios marcos de aseguramiento de aplicativos web con amplio reconocimiento en el mercado crea un dilema sobre cuál de todas es la más adecuada para la realización del presente proyecto. Por lo cual se realizará un análisis

comparativo en base a tabla de entre los tres marcos más reconocidos en el medio: **OWASP Top 10-2013, WASC Tc v2.0, CWE/SANS Top 25.** Tomando como medida de comparación los siguientes indicadores: Versión vigente (VV), Tiempo desde su primera versión (PV) , Metodología basada en Riesgos (MR), Documentación al Español (DE), Recomendaciones de Seguridad (RS), Basada en MITRE VULNERABILITY (MV) ; Metodología de Pruebas (MP)

Tabla 4

Tabla comparativa entre Marcos de Aseguramiento de Aplicativos Web

	VV	**PV**	**MR**	**DE**	**RS**	**MV**	**MP**
OWASP Top ten 2013	2013	12 años	Si	Si	Si	Si	Si
WASC Tc v2.0	2010	11 años	No	No	Si	Si	Si
CWE/SANS Top 25	2011	6 años	No	No	Si	Si	Si

Cumplimiento de los indicadores por parte de cada una de las metodologías seleccionadas.

3.8.1. Selección de Marcos de Aseguramiento de Aplicativos Web

Tomando en cuenta que **OWASP Top 10-2013, WASC Tc v2.0, CWE/SANS Top 25** son marcos de amplio reconocimiento, la decisión por **OWASP Top 10-2013** se tomó en base fortalezas que representaron ventajas para la realización del presente proyecto, las cuales se detallan a continuación.

- Mantiene la versión más actual de las tres 2013, además que el tiempo de lanzamiento desde la primera versión garantiza un nivel madurez de la norma mayor.
- Utiliza metodología basada en riesgos, en vista que el presente proyecto se enfoca en determinar las vulnerabilidades del aplicativo web, el contar con una metodología de referencia se torna una fortaleza para el desempeño de las actividades.
- La existencia de la última versión en idioma español, garantiza el fácil acceso a la información por parte de la entidad receptora del proyecto.

Tabla 5
Mapeo entre marco de aseguramiento de aplicativos web seleccionado ISO 27002.

DOMINIO ISO 27002	OBJETIVO DE CONTROL	CONTROLES	OWASP TOP 10-2013
Política de Seguridad	- Directrices de la Dirección en la Seguridad de la Información.	- Conjunto de políticas para la seguridad de la información. - Revisión de las políticas para la seguridad de la información	A1- Inyección A2– Pérdida de Autenticación y Gestión de Sesiones
Adquisición, desarrollo y mantenimiento de sistemas	- Requisitos de seguridad de los sistemas de información. - Seguridad en los procesos de desarrollo y soporte. - Datos Prueba	- Análisis y especificación de los requisitos de seguridad. - Protección de las transacciones por redes telemáticas. - Política de desarrollo seguro de software. - Uso de principios de ingeniería en protección de sistemas. - Seguridad en entornos de desarrollo. - Protección de los datos utilizados en pruebas.	A3– Secuencia de Comandos en Sitios Cruzados (XSS) A4– Referencia Directa Insegura a Objetos A5– Configuración de Seguridad Incorrecta. A6 – Exposición de datos sensibles
Cifrado	- Controles criptográficos	- Política de uso de los controles criptográficos. - Gestión de claves.	A7– Ausencia de Control de Acceso a Funciones.
Gestión de incidentes en la seguridad de la información	- Gestión de incidentes en la seguridad de la información y mejoras.	- Notificación de los eventos de seguridad de la información. - Notificación de puntos débiles de la seguridad. - Valoración de eventos de seguridad de la información y toma de decisiones. - Respuesta a los incidentes de seguridad. - Aprendizaje de los incidentes de seguridad de la información.	A8– Falsificación de Peticiones en Sitios Cruzados (CSRF) A9– Utilización de componentes con vulnerabilidades conocidas. A10– Redirecciones y reenvíos no validados

Al ser la ISO 27002 un estándar de referencia de seguridad de la información en general a nivel mundial, realizar un mapeo de **OWASP Top 10-2013** con la citada norma nos permite obtener una visión clara sobre sus alcances y limitaciones.

CAPITULO IV
EVALUACIÓN TÉCNICA DE LAS SEGURIDAD DE LA APLICACIÓN WEB

En base a la metodología antes especificada en el capítulo 3, se detalla a continuación las actividades realizadas durante el proceso de auditoría, así también como los productos de cada etapa.

4.1. FASE I. Planificación de la auditoría

4.1.1. Plan de Auditoría preliminar

Al no existir auditorias previas no existe plan de auditoria preliminar pero documentos obtenidos en esta etapa son:

Tabla 6

Anexos de cada una de las actividades desarrolladas en la etapa actual.

PRODUCTOS DE LA ETAPA	ANEXOS
Definición del perfil del personal requerido y asignación de auditores.	S-01.01 Auditores
Lista con horas estimadas por etapa para realizar la auditoría.	S-01.02 Tiempo estimado en horas
Carta de Confidencialidad	S-01.03 Carta de Confidencialidad

	GOBIERNO AUTONOMO DESCENTRALIZADO INTERCULTURAL CANTÓN CAÑAR S-01 PLAN DE ADUITORIA PRELIMINAR Asignación de auditores	S-01.01 26/03/2015

1.1 Nombre de la Organización:

ANEXO 1

DEFINICIÓN DEL PERFIL DEL PERSONAL REQUERIDO Y ASIGNACIÓN DE AUDITORES.

DATOS PERSONALES 1

NOMBRES: Cristhian Humberto
APELLIDOS: Flores Urgilés
FECHA NACIMIENTO: 17-06-1980
CÉDULA DE IDENTIDAD: 030163837-5
TÍTULO PROFESIONAL: Ingeniero Electrónico
CUARTO NIVEL:

- Diploma Superior en Docencia con el Empleo de las Tecnologías de la Información y La Comunicación
- Especialista en Docencia Universitaria
- Egresado Maestría en Evaluación y Auditoria de Sistemas Tecnológicos

EXPERIENCIA: Catedrático Universitario
TELÉFONO CONVENCIONAL: 072235572
TELÉFONO CELULAR: 0998156996
DIRECCIÓN (DOMICILIO): José Peralta y Rudecindo Inga Vélez CAÑAR
EMAIL PERSONAL: criss_flo@msn.com
EMAIL INSTITUCIONAL: chfloresu@ucacue.edu.ec

DATOS PERSONALES 2

NOMBRES: Cristina Mariuxi
APELLIDOS: Flores Urgilés
FECHA NACIMIENTO: 27-08-1985
CÉDULA DE IDENTIDAD: 0302090535
TÍTULO PROFESIONAL: INGENIERA DE SISTEMAS
CUARTO NIVEL:

- Egresada Maestría en Evaluación y Auditoria de Sistemas Tecnológicos

EXPERIENCIA: Catedrática Universitario
DIRECCIÓN DOMICILIARÍA:
TELÉFONO CONVENCIONAL: 072235572
TELÉFONO CELULAR: 0987974395
DIRECCIÓN (DOMICILIO): San Bruno y Rumiñahui CAÑAR
EMAIL PERSONAL: titis_flo@hotmail.es
EMAIL INSTITUCIONAL: cmfloresu@ucacue.edu.ec

FUENTE: AUDITORES

	Ing. Cristina Flores Urgiles Ing. Cristhian Flores Urgilés

Figura 5. Definición del perfil del personal requerido y asignación de auditores.

	GOBIERNO AUTONOMO DESCENTRALIZADO INTERCULTURAL CANTÓN CAÑAR S-01 CARTA DE CONFIDENCIALIDAD	S-01.01 12/03/2015

CARTA DE CONFIDENCIALIDAD

FECHA: 12-03-2015

Ing. Danny Andrade Cárdenas
RESPONSABLE DEL DEPARTAMENTO INFORMÁTICO GADIC CAÑAR
Presente

Señor Asesor:

Los que suscribimos, en virtud del desarrollo de la EVALUACIÓN TECNICA DE SEGURIDAD DE LA APLICACIÓN WEB DEL "SISTEMA INFORMATICO INTEGRADO DE SERVICIOS MUNICIPALES" en el GADIC CAÑAR, para la, declaramos que nos obligamos a guardar absoluta reserva de la información confiada y a la que pueda tener acceso durante desarrollo y cumplimiento del presente trabajo. La inobservancia de lo manifestado dará lugar a que el GAD CAÑAR ejerza las acciones legales civiles y penales correspondientes y en especial las determinadas en los artículos 200 y 201 del Código Penal vigente.

Atentamente

Ing. Cristhian Flores Urgilés Ing. Cristina Flores Urgilés

AUDITORES

Figura 6. Carta de Confidencialidad

La presente auditoria tiene estimada 150 Horas distribuidas de la siguiente forma:

Tabla 7

Horas estimadas para el desarrollo de la Auditoría

FASE	**TIEMPO (Horas)**
Planificación de la auditoría	30
Ejecución de la auditoría	90
Comunicación de los resultados	30
TOTAL	180

Lista con horas estimadas por etapa para realizar la auditoría.

4.1.2. Comprensión de la organización, procesos de negocio y sistemas

Durante esta etapa de la auditoria se realizó el levantamiento de información sobre el estado actual y características de la organización, infraestructura, recursos humanos y técnicos, procesos de negocios y sistemas de información que los soportan, se elaboró un flujograma de los procesos de negocio que soporta la aplicación, finalizando con una ficha técnica de los sistemas de información que soportan los procesos de negocio.

Tabla 8

Anexos de cada una de las actividades desarrolladas en la etapa actual.

PRODUCTOS DE LA ETAPA	ANEXOS
Archivos de trabajo de la auditoría.	S-01.01 Misión, Visión Y Objeto Social S-01.02 Estructura Orgánica
Documento con definición de los procesos de negocio y diagramas descriptivos.	S-01.03 Arquitectura Tecnológica
Ficha técnica de los sistemas de información que soportan los procesos de negocio.	S-01.04 Flujograma de los procesos y subprocesos del negocio

4.1.2.1. Misión, Visión y Objeto social del GADIC Cañar.

4.1.2.1.1. *Misión.*

La misión del Gobierno Autónomo Descentralizado Intercultural del Cantón Cañar, se encuentra establecida en el estatuto orgánico de gestión organizacional que rige desde el año 2011 para la municipalidad, a continuación se enuncia el mismo:

> Promover el desarrollo equitativo, solidario, sustentable, económico y social del Cantón Cañar, que con la integración y participación ciudadana, se garantice el suministro adecuado de servicios básicos, de salud, de educación, de vialidad urbana e infraestructura complementaria; se ejecuten programas objetivos de seguridad y desarrollo social, y se brinde seguridad y saneamiento ambiental; haciendo así efectivos los derechos de la ciudadanía y el régimen del buen vivir, como acción local a la afirmación del carácter intercultural y plurinacional del Estado ecuatoriano. (Cañar, 2011, pág. 3)

4.1.2.1.2. Visión

De la misma manera dentro del estatuto orgánico de gestión organizacional del GADIC Cañar, se encuentra establecida la visión institucional la misma que es enunciada a continuación:

> Lograr que el Gobierno Autónomo Descentralizado Intercultural de Cantón Cañar transforme sus actuales condiciones físicas, sociales, culturales y ambientales en alternativas y modelos de desarrollo que reflejen el trabajo de gestión administrativa, de participación ciudadana y del esfuerzo del gobierno y las comunidades por el régimen del buen vivir. . (Cañar, 2011, pág. 3)

4.1.2.2. Estructura orgánica del GADIC Cañar.

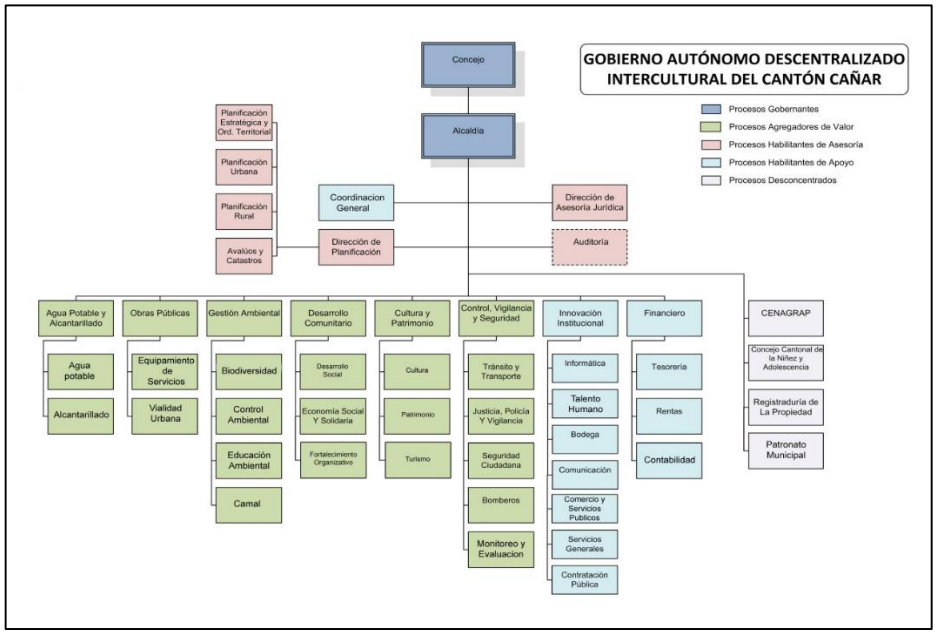


Figura 7. Organigrama estructural del GADIC Cañar

4.1.2.2.1. Departamentos del GADIC Cañar

Tabla 9

Departamentos del GADIC Cañar, con sus representantes.

DEPARTAMENTO	DIRECTIVOS
Agua Potable Y Alcantarillado	Ing. Edgar Urgilés
Obras Públicas	Ing. Mauricio Pacheco
Desarrollo Comunitario	Ing. Jesús Pichizaca
Cultura Y Patrimonio	Ing. Ranty Chuma
Control, Vigilancia Y Seguridad	Dr. Ezequiel Cárdenas
Innovación Institucional	Ing. Katty Herrera
Financiero	Ing. María Palchizaca

4.1.2.2.2. ***Innovación Institucional***

*Misión***.-** Administrar los bienes muebles e inmuebles, la tecnología, el sistema del talento humano, la difusión de la acción municipal y los servicios administrativos.

Responsable: Director de Innovación Institucional

Subprocesos:

- Talento Humano
- Informática
- Contratación Pública
- Comercio y Servicios Públicos

*Atribuciones***.-** Son atribuciones del Director de Innovación Institucional, las siguientes:

- Velar por el fiel cumplimiento de las leyes y normativas relacionadas con la administración de los bienes del sector público.
- Supervisar y controlar el correcto uso de las herramientas informáticas a disposición de los funcionarios de la municipalidad.
- Controlar la correcta difusión interna y externa respecto a las actividades que realiza la municipalidad.

- Coordinar e interactuar con las autoridades y demás directores de procesos los servicios internos que están a su cargo.
- Realizar estudios y presentar informes de los mismos, respecto a implementar cambios en la estructura administrativa de la municipalidad.
- Presentar proyectos y programas que simplifiquen procedimientos en pro de lograr una mejor productividad como institución.

Productos de Informática:

- Elaborar el plan informático institucional.
- Mantenimiento y desarrollo de sistemas informáticos.
- Informes de investigación tecnología de la información que sea útil a la Institución.
- Diseñar, desarrollar y mantener sistemas, redes y aplicaciones;
- Administrar la página Web de la Entidad; y,
- Asesorar a la entidad en esta materia.

4.1.2.2.3. Estructura Interna del Departamento Informático del GADIC Cañar.

Tabla 10

Personal que trabaja en el departamento informático.

PERSONAL	PUESTO
Ing. Danny Andrade Cárdenas	ANALISTA INFORMÁTICO
Wilson Lema Lema	TÉCNICO INFORMÁTICO.

4.1.2.3. Arquitectura Tecnológica.

4.1.2.3.1. Sistemas informáticos implementados en GADIC Cañar.

Los servicios informáticos con los que cuenta actualmente las diversas dependencias de la municipalidad, han sido implementados en base a los requerimientos y procedimientos propios de la gestión municipal. Para su implementación han tenido que pasar por la aprobación del consejo y alcaldía, para posteriormente iniciar su implementación. Actualmente el GADIC Cañar cuenta con

siete aplicaciones informáticas que son utilizadas por las diferentes dependencias del cabildo, las mismas que son detalladas a continuación:

Tabla 11

Sistemas informáticos implementados en GADIC Cañar, con las dependencias en las que son utilizadas.

NOMBRE DE LA APLICACIÓN	DEPENDENCIAS	DESARROLLADOR
SIG AME	Departamento Financiero Validación Predial	AME (Asociación de Municipalidades Ecuatorianas)
SNRP (Sistema Nacional de Registros de la Propiedad)	Registro de la Propiedad	DINARDAP (Dirección Nacional de Registro de Datos Públicos)
GPR (Gobierno por Resultados)	Directivos Departamentales	EcoConsulting
Correo Electrónico (Zimbra)	Todos los departamentos del cabildo	Analista Informático
Sistema de Turnos	Ciudadanía	Analista Informático
Sistema Informático Integrado De Servicios Municipales	Agua Potable Predio Urbano Locales Municipales Impuesto de Patente Municipal Turismo	Analista Informático Consultoría
Ushay	Financiero	SERCOP (Servicio Nacional de Contratación Pública)

Además de las aplicaciones mencionadas anteriormente, el GADIC Cañar cuenta con dos aplicativos Web que son utilizados por la ciudadanía del Cantón, para la consulta de información institucional, así también como para realizar trámites municipales.

Tabla 12

Aplicativos Web implementados en GADIC Cañar, con las dependencias en las que son utilizadas.

NOMBRE DE LA APLICACIÓN WEB	SERVICIOS	DESARROLLADOR
Sistema Informático Integrado De Servicios Municipales	Agua Potable Cartera Pendientes de Pago Impuesto Patentes Municipales Impuesto al Rodaje Impuestos Prediales	Analista Informático Consultoría
Página Web informativa http://www.canar.gob.ec/	Información General de la Municipalidad. Ley de Transparencia. Rendición de Cuentas de la Municipalidad.	Analista Informático

4.1.2.3.2. Catálogo de servicios del GADIC Cañar.

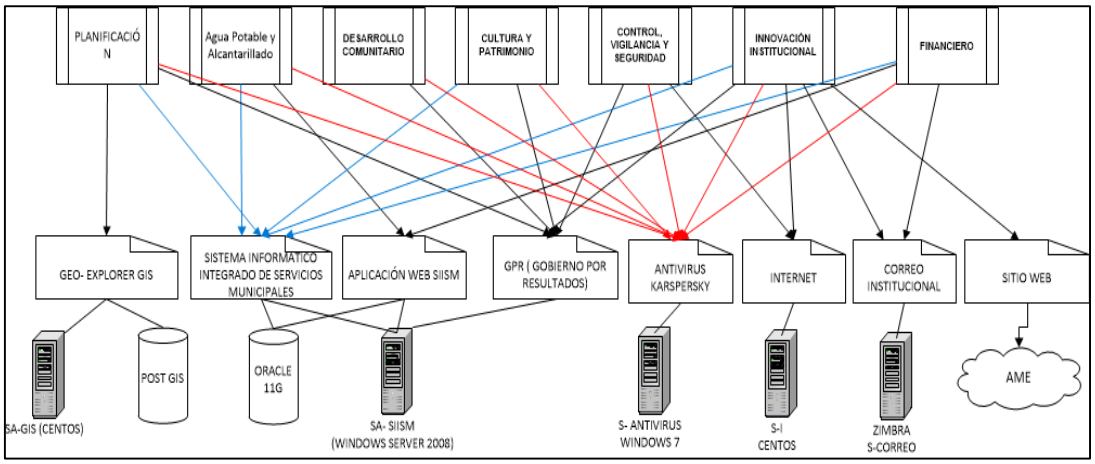


Figura 8. Estructura tecnológica del GADIC Cañar.

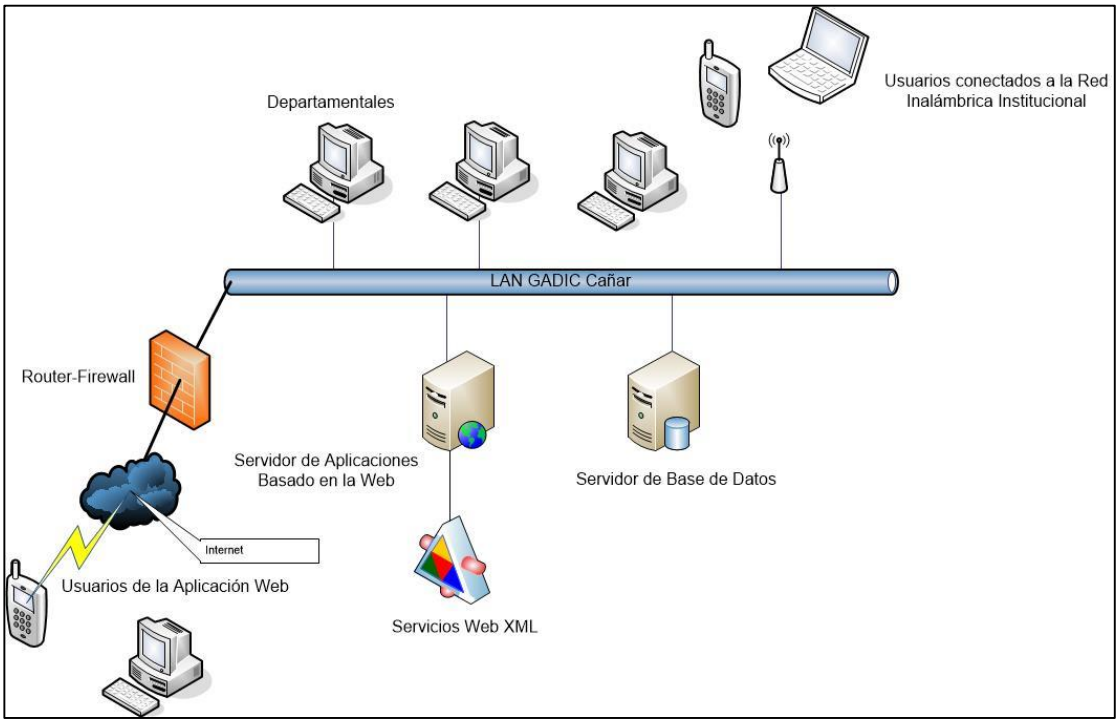


Figura 9. Diagrama aplicación WEB, Sistema Informático Integrado De Servicios Municipales

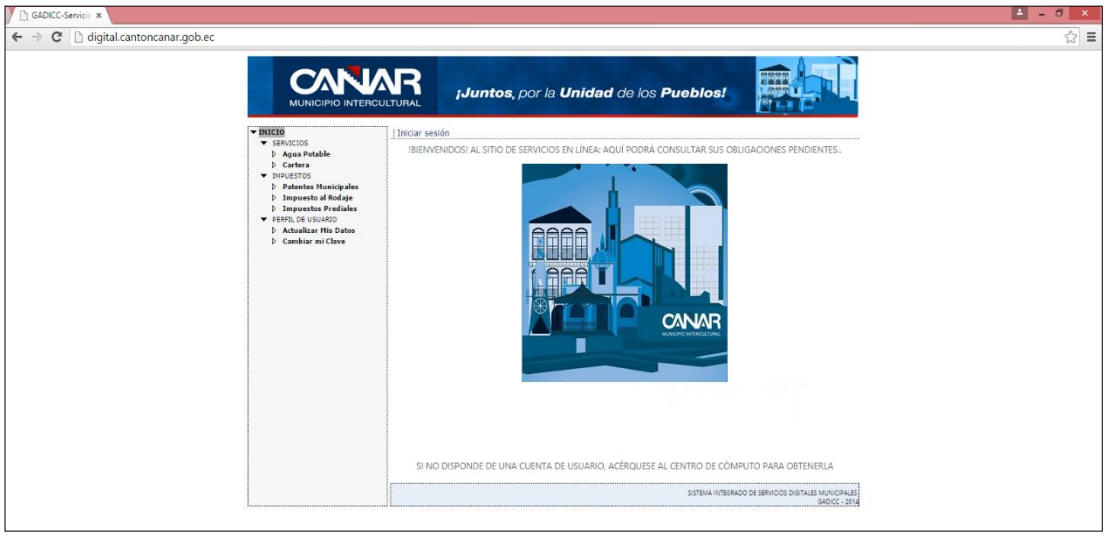


Figura 10. Aplicativo Web, Sistema Informático Integrado De Servicios Municipales

Figura 11. Aplicativo Web, Sitio Web Informativo del GADIC Cañar

Una vez realizado el análisis de la arquitectura tecnológica se ha llegado a determinar los siguientes puntos de referencia:

- La aplicación Web "Sistema Informático Integrado De Servicios Municipales", es utilizada por el departamento de Agua Potable y Financiero, en donde los usuarios pueden llegar a utilizar los siguientes servicios: Agua potable, cartera vencida, impuestos a las patentes municipales, Impuesto al rodaje e impuestos prediales.
- La aplicación Web "Sistema Informático Integrado De Servicios Municipales", se encuentra bajo el servidor web IIS (Internet Information Server), bajo un servidor de aplicaciones Windows Server 2008, además de trabajar con el gestor de base de datos Oracle 11 G.
- Lo servicios web se encuentran almacenados en el mismo servidor web en donde se localiza la aplicación Web.

- El aplicativo web fue desarrollado bajo la plataforma ASP. NET, utilizando una arquitectura de tres capas: capa de datos, capa de negocio y capa de presentación.
- El Sitio Web informativo del GADIC Cañar, La aplicación Web informativa del GADIC Cañar, fue desarrollado mediante el sistema de gestión de contenidos joomla, conjuntamente con el gestor de base de datos MySql.
- No se puede conocer el estructura de la aplicación WEB, ya que se encuentra alojada en los servidores de aplicaciones Web de AME (Asociación de Municipalidades del Ecuador), la municipalidad únicamente tiene acceso al servidor mediante una cuenta de usuario que le permite administrar su sitio web.

4.1.2.3.3. Procesos y subprocesos que soportan el negocio.

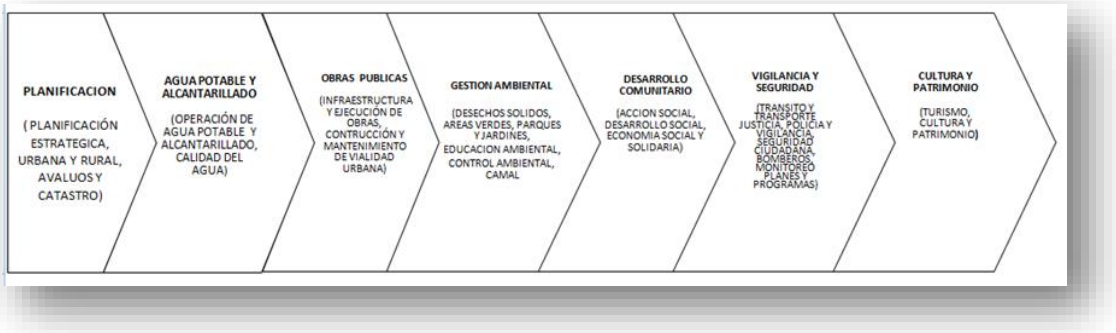


Figura 12. Cadena de valor Institucional GADIC Cañar.

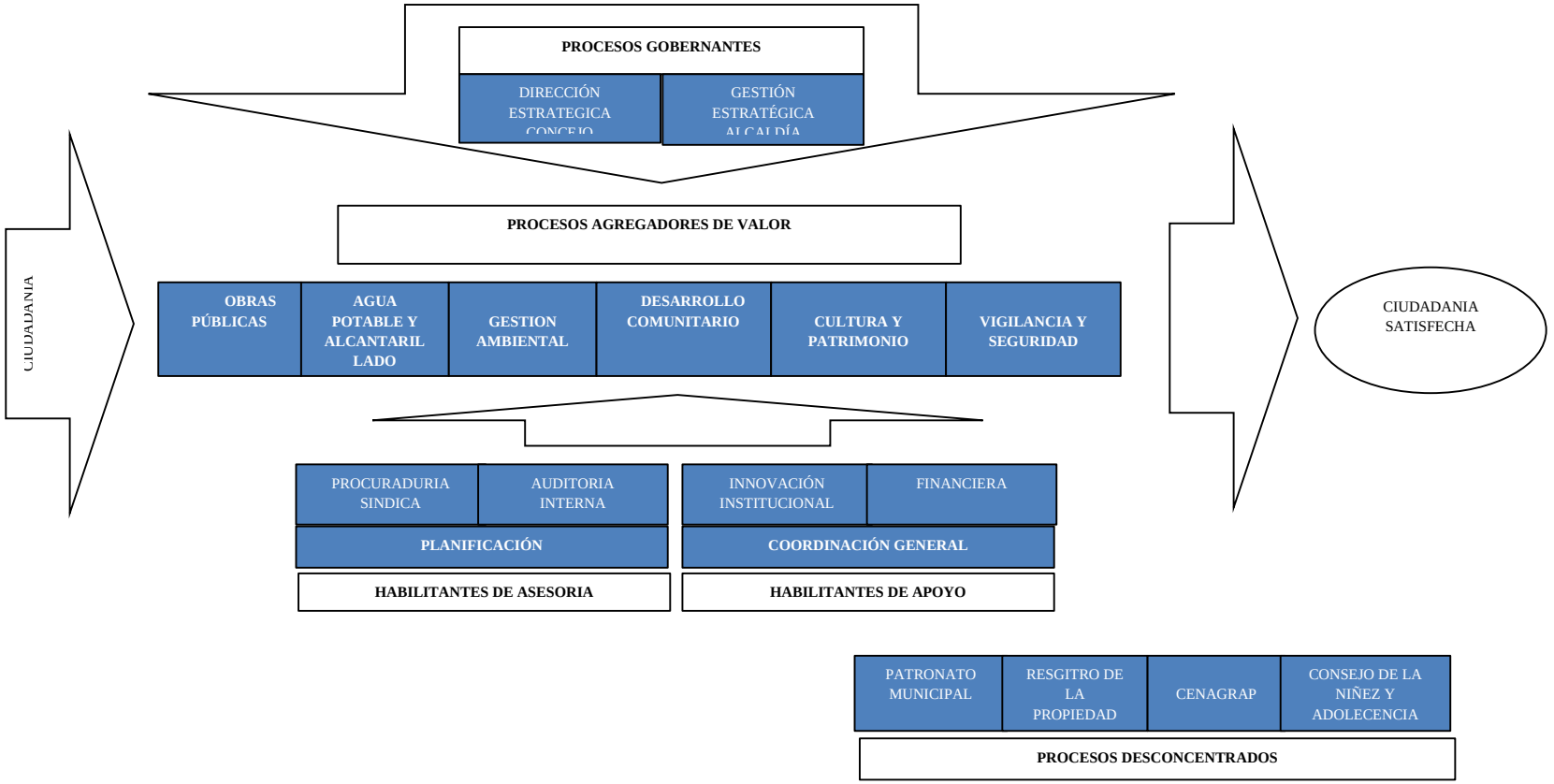


Figura 13. Flujo grama de procesos y subprocesos del GADIC Cañar.

4.1.3. Definición del programa y alcance de la auditoría

Para su cumplimiento se seleccionó los objetivos de control que se pueden aplicar a los procesos de negocio y son soportados por los sistemas de información y se elaboró el programa de auditoría detallado incluyendo su carta Gantt.

Tabla 13

Anexos de cada una de las actividades desarrolladas en la etapa actual.

PRODUCTOS DE LA ETAPA	ANEXOS
Lista de objetivos de control que deben ser satisfechos por los procesos de negocio y sistemas de información.	S-01.01 Listado de Objetivos de Control
Programa de auditoría detallado.	S-01.02 Programa de Auditoria Detallado
Carta Gantt del programa de auditoría.	S-03.03 Carta Gantt

4.1.3.1. Objetivos que deben ser satisfechos por el proceso del negocio.

A continuación se detalla la lista de objetivos de control que deben ser satisfechos por los procesos de negocio y sistemas de información, en base al resultado obtenido del mapeo entre la ISO 27002 Y OWASP.

Tabla 14

Listado de Objetivos que deben ser satisfechos por el proceso del negocio

OBJETIVO DE CONTROL	OWASP TOP 10-2013
Dominio ISO 27002: Política de Seguridad Directrices de la Dirección en la Seguridad de la Información.	
Dominio ISO 27002**:** Adquisición, desarrollo y mantenimiento de sistemas - Requisitos de seguridad de los sistemas de información. - Seguridad en los procesos de desarrollo y soporte. - Datos Prueba	A1- Inyección A2– Pérdida de Autenticación y Gestión de Sesiones A3– Secuencia de Comandos en Sitios Cruzados (XSS) A4– Referencia Directa Insegura a Objetos A5– Configuración de Seguridad Incorrecta A7– Ausencia de Control de Acceso a Funciones A8- Falsificación de Peticiones en Sitios Cruzados (CSRF) A9– Utilización de componentes con vulnerabilidades conocidas A10 – Redirecciones y reenvíos no validados
Dominio ISO 27002: Cifrado - Controles criptográficos	A6 – Exposición de datos sensibles
Dominio ISO 27002: Gestión de incidentes en la seguridad de la información Gestión de incidentes en la seguridad de la información y mejoras.	A5 – Configuración de Seguridad Incorrecta

4.1.3.2. Programa de auditoria detallado

Tabla 15

Papel de trabajo - programa de auditoria detallado

CAÑAR MUNICIPIO INTERCULTURAL	**PROGRAMA DE AUDITORIA DETALLADO**			**S-04.01**
	GADIC "Cañar"			
AUDITORIA:	Evaluación técnica de seguridad de la aplicación web del "SISTEMA INFORMATICO INTEGRADO DE SERVICIOS MUNICIPALES" del GADIC CAÑAR			
INICIO:	12-03-2015	**Fin:**	10-04-2015	
OBJETIVO:	Evaluar la seguridad del aplicativo web del "SISTEMA INFORMATICO INTEGRADO DE SERVICIOS MUNICIPALES" del GADIC Cañar, a fin de encontrar vulnerabilidades y emitir recomendaciones dentro del ambiente informático, que permitirá minimizar los riesgos seguridad.			
ALCANCE:	Evaluación sobre la seguridad del aplicativo web del "SIISM", además del sitio web del GADICC la misma que la contiene.			
N°	**PROCEDIMIENTOS**	**REF**	**PERSONAL**	**FECHA**
1.	**Aplicables etapa preliminar**			
1.01	Comprensión de la organización, procesos de negocio y sistemas		Auditores	12/03/2015
1.02	Seleccionar los objetivos de control aplicables a los procesos de negocio y sistemas de información.		Auditores	16/03/2015
2.	**Aplicables en las etapas intermedias y final**			
2.01	Identificar y evaluar los controles existentes dentro del dominio evaluado.		Auditores	17/03/2015
2.02	Definición y diseño de las pruebas de auditoría		Auditores	19/03/2015
2.03	Ejecución de las pruebas de auditoria		Auditores	23/03/2014
2.04	Evaluación de los resultados obtenidos en las pruebas de auditoría		Auditores	31/03/2014
2.05	Elaboración del informe con los resultados de la auditoría		Auditores	6/04/2015

4.2. FASE II. Ejecución De La Auditoría

La segunda fase de la auditoría comprendió un análisis del sistema de control interno de la organización, se planificó y aplicó las pruebas de cumplimiento y sustantivas que evaluaron si los controles operan de forma adecuada y cumplen con resguardan el cumplimiento de los objetivos y requisitos del negocio.

4.2.1. Evaluación del sistema de control interno

Iniciamos con la evaluación de control interno, identificando y documentando los controles existentes en los procesos de negocio y sistemas de información, para luego pasar a evaluar el diseño y grado de protección que ofrecen los controles existentes, toda esta información se encuentra en una lista que posteriormente nos permitió identificar y documentar los controles deficientes.

Tabla 16

Anexos de cada una de las actividades desarrolladas en la etapa actual.

PRODUCTOS DE LA ETAPA	ANEXOS
Lista de controles existentes para los procesos de negocio y sistemas de información.	S-04.01 Evaluación Del Control Interno
Lista con el grado de protección de controles existentes para los procesos de negocio y los sistemas.	S-04.01 Evaluación Del Control Interno
Lista de deficiencias y debilidades de control interno.	S-04.01 Evaluación Del Control Interno

Tabla 17

Evaluación Del Control Interno, utilizando como referencia los controles de la ISO 27002

ISO 27002	DESCRIPCION	EXISTE		OBSERVACIONES	CUMPLE	RIESGO EVALUADO	CRITICIDAD
		SI	NO				
5. POLÍTICA DE SEGURIDAD 5.1 DIRECTRICES DE LA DIRECCIÓN EN LA SEGURIDAD DE LA INFORMACIÓN							
5.1.1 Conjunto de Políticas para la seguridad de la información	Cuenta el Departamento Informático con políticas de seguridad de la información debidamente documentadas y legalizadas por las autoridades del GADICC?		NO	No cuentan con políticas de seguridad de la información.	NO	Construcción de software sin aspectos de seguridad alineadas con la organización.	**MEDIO**
5.1.2 Revisión de Políticas para la seguridad de la información	Se realizan periódicamente revisiones y actualizaciones de las políticas de seguridad de la información?		NO	No cuentan con políticas de seguridad de la información.	NO	Construcción de software sin aspectos de seguridad alineadas con la organización.	**MEDIO**
10. CIFRADO 10.1 CONTROLES CRIPTOGRAFICOS							
10.1.1 Política de uso de controles criptográficos	Las aplicaciones desarrolladas internamente cuentan con controles criptográficos?		NO	Las aplicaciones web desarrolladas por el departamento informático no cuentan con controles criptográficos.	NO		

Tabla 18

Evaluación Del Control Interno, utilizando como referencia los controles de la ISO 27002

ISO 27002	DESCRIPCION	EXISTE		OBSERVACIONES	CUMPLE	RIESGO EVALUADO	CRITICIDAD
		SI	NO				
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS 14. 1 REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN							
14.1.1 Análisis y Especificación de requisitos de seguridad.	Antes de iniciar un proyecto de software, los requisitos de seguridad son evaluados. ?	SI		Los requisitos de seguridad son evaluados antes de iniciar el proyecto, pero no cuentan con documentación que apoye su cumplimiento.	NO	Aplicaciones informáticas inseguras.	**ALTO**
14.2 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE							
	Cuenta el departamento informático con políticas de desarrollo seguro de software, debidamente documentado y versionado?		NO	No cuentan con políticas de desarrollo seguro de software.	NO	Construcción de software inseguro	**ALTO**
14.2.1 Política de desarrollo seguro de software	Los desarrolladores siguen un estándar establecido para generar software seguro?		NO	Los desarrolladores no siguen ningún estándar de software seguro.	NO	Los requerimientos funcionales y no funcionales de software no son cubiertos de manera eficiente.	**MEDIO**
14.2.2 Procedimientos de control de cambios en los sistemas	Existe un procedimiento establecido para control de cambios de las aplicaciones informáticas desarrollados por el departamento. ?		NO	No cuentan con ningún procedimiento establecido para control de cambios.	NO	Cambios de software no autorizados.	**BAJO**

Tabla 19

Resultados de la Evaluación de Control Interno

CALIFICACIÓN TOTAL:	CT=	2
PONDERACIÓN TOTAL:	PT=	12
NIVEL DE CONFIANZA: NC= CT/PT x 100	NC=	0.1667
NIVEL DE RIESGO INHERENTE: RI= 100% - NC%	RI=	0.8333

4.2.2. Definición y diseño de las pruebas de auditoría

La siguiente etapa consistió en definir y diseñar las pruebas de auditoria tanto las de cumplimiento para los controles claves de los procesos de negocio y sistemas agrupados por técnicas de verificación como las sustantivas para datos clave de los procesos y sistemas.

Tabla 20

Anexos de cada una de las actividades desarrolladas en la etapa actual.

PRODUCTOS DE LA ETAPA	ANEXOS
Definición del alcance de las pruebas de cumplimiento.	S-05.01 DISEÑO PRUEBAS SUSTANTIVAS
Diseño detallado de las pruebas de cumplimiento según técnicas de verificación.	S-05.01 DISEÑO PRUEBAS SUSTANTIVAS
Definición del alcance de las pruebas sustantivas.	S-05.02 DISEÑO PRUEBAS DE CUMPLIMIENTO
Diseño detallado de las pruebas sustantivas.	S-05.02 DISEÑO PRUEBAS DE CUMPLIMIENTO

4.2.2.1. Diseño de pruebas sustantivas.

Luego de realizar la evaluación de los controles existentes en el área de desarrollo del GADIC Cañar, y al encontrar ciertas deficiencias que podrían afectar la seguridad de las aplicaciones. Se pretende realizar las siguientes pruebas que permitirán corroborar si las aplicaciones web implementadas son vulnerables a ataques externos, que pueden afectar la integridad de la información de la municipalidad.

Tabla 21

Pruebas sustantivas diseñadas para la ejecución de la auditoría

OWASP TOP 10 RIESGOS	PRUEBAS	HERRAMIENTAS	RESPONSABLE
	Análisis general de vulnerabilidades **Alcance:** Escaneo de las aplicaciones web.	**VEGA** **KALI LINUX**	Auditores
A1- Inyección	Pruebas de Inyección SQL **Alcance:** Se realizará el escaneo con el fin de determinar las vulnerabilidades que permitan el ataque con SQL Injection.	**SQLMAP** **ACCUNETIX** **VEGA**	Auditores
A2 – Pérdida de Autenticación y Gestión de Sesiones.	Pruebas de acceso a Fuerza bruta. **Alcance:** Realizar introducción a sesión mediante fuerza bruta.	**XHYDRA**	Auditores
	Pruebas de Expiración de sesión. **Alcance:** Revisar configuración de las cookies de los aplicativos web.	**NAVEGADOR CHROME**	Auditores
A3 – Secuencia de Comandos en Sitios Cruzados (XSS)	Pruebas de Cross-site scripting **Alcance:** Escanear la existencia de vulnerabilidades utilizando las herramientas citadas.	**ACCUNETIX** **XSSER** **VEGA**	Auditores
A4 – Referencia Directa Insegura a Objetos	Pruebas para referencias a inseguras de referencias a objetos directos **Alcance:** Identificar la probabilidad de acceder a referencias a objetos directos.	**ACCUNETIX**	Auditores
A5 – Configuración de Seguridad Incorrecta	Pruebas de Indexación Directorio **Alcance:** Identificar la existencia de vulnerabilidad en la configuración de directorio.	**ACCUNETIX**	Auditores

Tabla 22

Pruebas sustantivas diseñadas para la ejecución de la auditoría

OWASP TOP 10	PRUEBAS	HERRAMIENTAS	RESPONSABLE
A7 – Ausencia de Control de Acceso a Funciones	Pruebas de control de acceso a Funciones. **Alcance:** Identificar la ausencia de control de acceso a funciones.	**ACCUNETIX** **PRUEBAS MANUALES**	Auditores
A8 - Falsificación de Peticiones en Sitios Cruzados (CSRF)	Pruebas de Cross-site Request Forgery.	**SCRIPT**	Auditores
A9 – Utilización de componentes con vulnerabilidades conocidas	Pruebas de vulnerabilidades de joomla **Alcance**: Escanear vulnerabilidades propias del entorno de desarrollo joomla.	**JOOMSCAN**	Auditores
A9 – Utilización de componentes con vulnerabilidades conocidas	Análisis de vulnerabilidad propios de ASP.NET **Alcance**: Escanear las vulnerabilidades propias del entorno de desarrollo ASP.NET.	**ACCUNETIX**	Auditores
A10 – Redirecciones y reenvíos no validados	Pruebas de configuración de redirecciones. **Alcance:** Identificar la existencia de Redirecciones y reenvíos en las aplicaciones, y si existieran determinar si se encuentran correctamente diseñados.	**PRUEBAS MANUALES**	Auditores

4.2.2.2. Diseño de pruebas de cumplimiento.

Luego de realizar la evaluación de los controles existentes en el área de desarrollo del GADIC Cañar, y al encontrar ciertas deficiencias que podrían afectar la seguridad de las aplicaciones. Se realiza un cuestionario que permitirá definir si se cumple con ciertas directivas que aseguran la estabilidad de los aplicativos web evaluados. Mencionada herramienta va dirigida al Analista de Sistemas quien es el principal responsable de departamento informático y todos los procesos relacionados, dentro del GADIC Cañar.

Tabla 23

Pruebas de Cumplimiento - Cuestionario dirigido al Analista de Sistemas del GADIC Cañar.

CUESTIONARIO	SI	NO	MEDIO DE VERIFICACIÓN
A1- INYECCIÓN			
El departamento informático cuenta con una política de pruebas de desarrollo seguro, estableciendo procedimientos en contra de los posibles ataques de Inyección. ?			Política documentada y autorizada
A2 – PÉRDIDA DE AUTENTICACIÓN Y GESTIÓN DE SESIONES.			
Se encuentra establecido el cumplimiento de los requisitos de autenticación y gestión de sesiones definidos en el Application Security Verification Standard de OWASP, o de alguna otra normativa. ?			Política documentada y autorizada
A3 – SECUENCIA DE COMANDOS EN SITIOS CRUZADOS (XSS)			
Cuenta con políticas de seguridad de contenido para defenderse contra XSS. ?			Política documentada y autorizada
A5 – CONFIGURACIÓN DE SEGURIDAD INCORRECTA			
¿Tiene algún software sin actualizar? Esto incluye el SO, Servidor Web/Aplicación, DBMS, aplicaciones.			Observación Versión SO, Servidor Web, Joomla, IIS, Asp.Net
¿El manejo de errores revela rastros de las capas de aplicación u otros mensajes de error demasiado informativos a los usuarios?			Observación en aplicación WEB
A6 – EXPOSICIÓN DE DATOS SENSIBLES			
¿Se utiliza algún algoritmo criptográfico. ?			Algoritmo documentado y certificado,
A8 - FALSIFICACIÓN DE PETICIONES EN SITIOS CRUZADOS (CSRF)			
La aplicación WEB cuenta con mecanismos de re-autenticación (CAPTCHA). ?			Observación aplicaciones WEB
La aplicación web desarrollada aplica la propiedad anti-forgery tokens para evitar ataques CRSF?			Observación código fuente de implementación.

4.2.3. Ejecución de las pruebas de auditoría

Luego pasamos a la ejecución de las pruebas de auditoria tanto de cumplimiento como sustantivas utilizando técnicas de verificación manuales o asistidas por el

computador. De lo cual existe la respectiva lista y soportes de las pruebas de auditoria realizadas.

Tabla 24

Anexos de cada una de las actividades desarrolladas en la etapa actual.

PRODUCTOS DE LA ETAPA	ANEXOS
Lista de controles verificados por el auditor.	S-06.01 Lista De Controles Verificados
Soportes de las pruebas de auditoría realizadas.	S-06.02 Pruebas Sustantivas Ejecutadas S-06.03 Pruebas De Cumplimiento

4.2.4. Pruebas Sustantivas Ejecutadas

Como se mencionó anteriormente la pruebas sustantivas diseñadas fueron realizadas en base a OWASP Top 10, además para cada una de los puntos se seleccionó una serie de herramientas, con las cuales se estableció si las aplicaciones WEB auditadas son o no vulnerables a las Amenazas que hace referencia OWASP.

A continuación se puede observar un informe ejecutivo de las pruebas que fueron realizadas a cada uno de los aplicativos WEB.

4.2.4.1. Análisis General De Vulnerabilidades

4.2.4.1.1. Análisis de los aplicativos

El análisis generado en este punto establece de manera general cuales son las vulnerabilidades de seguridad de las aplicaciones evaluadas, identificando el lugar exacto en donde la aplicación es vulnerable a ataques. Las herramientas utilizadas para este análisis fueron: VEGA de KALI LINUX y ACCUNETIX, siendo versiones libres y pagadas respectivamente. El Informe detallado que emite cada una de las herramientas se puede encontrar en el ANEXO 1, archivo corriente de la auditoria.

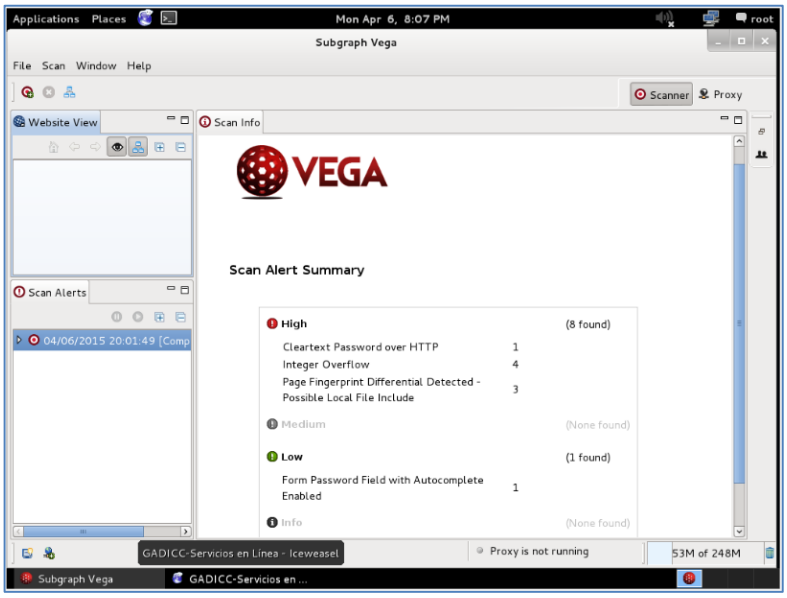


Figura 14. Herramienta Vega (Análisis de vulnerabilidades de las aplicaciones Web)

Figura 15. Herramienta ACCUNETIX (Análisis de vulnerabilidades de las aplicaciones Web)

Tabla 25

Resumen del análisis efectuado a los aplicativos web, utilizando las herramientas anteriormente citadas.

	digital.cantoncanar.gob.ec		www.canar.gob.ec	
HERRAMIENTAS	**DESCRIPCIÓN VULNERABILIDADES**	**CRITICIDAD**	**DESCRIPCIÓN VULNERABILIDADES**	**CRITICIDAD**
VEGA - KALI LINUX	Contraseña sin cifrar a través de HTTP	ALTA	Cross Site Scripting	ALTA
	Desbordamiento de enteros	ALTA	Page fingerprint differential, Possible Xpath Injection	ALTA
	Page fingerprint differential detectado,	ALTA	SQL Injection	ALTA
	Campo de contraseña con Autocomplete permitido	BAJA	Possible Http Put File Upload	MEDIO
ACCUNETIX	Parámetros no encriptados	MEDIO	Cross Site Scripting	ALTA
	Credenciales de usuario son enviados en clear text	MEDIO	JQUERY Cross Site Scripting	ALTA
	Depuración de ASP.NET permitido.	BAJA	Configuración de directorio	MEDIO
	Opciones de cabecera X-Frame perdidos	BAJA	Posibles directories sensibles	BAJA
	Página de login de usuario vulnerable a ataque	BAJA	Posibles archivos sensibles	BAJA
	Sesión de Cookie sin configuración secure	BAJA	Posible host virtual encontrado	BAJA

4.2.4.2. Pruebas de Inyección SQL

Para las pruebas de inyección SQL, se tomó como referencia los resultados obtenidos en el análisis general de vulnerabilidades, además de utilizar la herramienta SQLMAP de KALI LINUX.

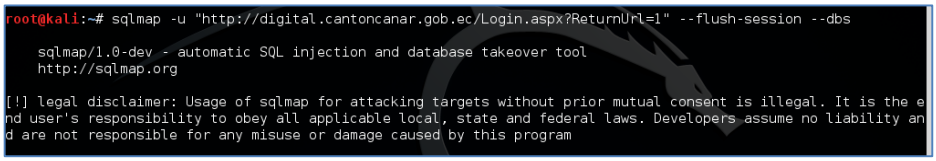


Figura 16. Pruebas de Inyección SQL utilizando la herramienta SQLMAP

Tabla 26

Resumen de los resultados obtenidos en cada una de las herramientas utilizadas.

	APLICACIONES WEB AUDITADAS	
HERRAMIENTAS	digital.cantoncanar.gob.ec	www.canar.gob.ec
VEGA KALI LINUX	NO	SI
ACCUNETIX	NO	NO
SQL MAP	NO	NO

4.2.4.3. Pérdida De Autenticación Y Gestión De Sesiones.

4.2.4.3.1. Análisis De Acceso A Fuerza Bruta

Para las pruebas de acceso a fuerza bruta, se utilizó la herramienta XHYDRA de KALI LINUX, la misma que permite establecer la posibilidad de predecir las posibles credenciales de los usuarios del aplicativo WEB.

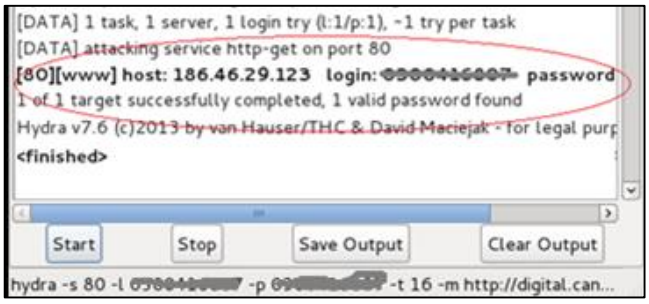
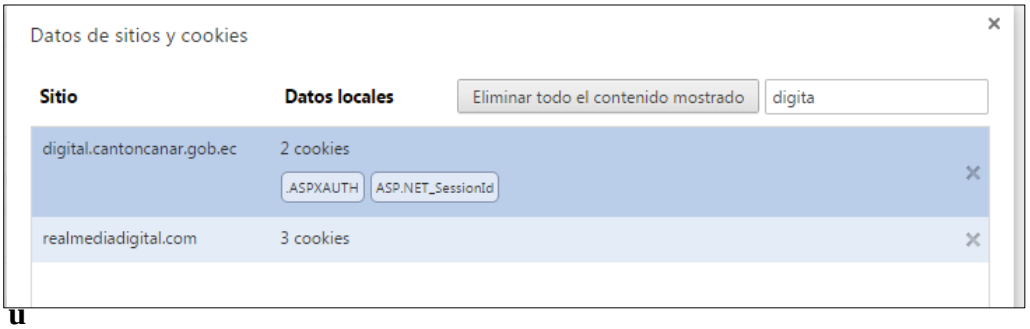


Figura 17. Resultado del análisis realizado al aplicativo WEB utilizando la herramienta xHydra

4.2.4.3.2. Análisis De Expiración De Sesión Y Seguridad De Los Cookies.

Para este análisis se utilizó la información que contienen los cookies generados por cada una de las aplicaciones, las herramientas utilizadas para este análisis fueron: Google Chrome y Accunetix.



u

ra 18. Cookies registrados en el navegador

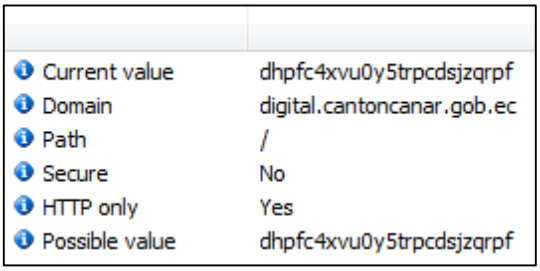


Figura 19. Configuración de los cookies- Análisis realizado con la herramienta ACCUNETIX

Tabla 27

Resumen de los resultados obtenidos en cada una de las herramientas utilizadas.

	APLICACIONES WEB AUDITADAS	
HERRAMIENTAS	digital.cantoncanar.gob.ec	www.canar.gob.ec
XHYDRA	SI	NO
Atributo SECURE	SI	SI
Atributo HTTPONLY	NO	SI
Atributo DOMAIN	NO	NO
PATH inseguro	SI	SI
Cierre de sesión seguro	NO	NO

4.2.4.4. Secuencia De Comandos En Sitios Cruzados (XSS).

Para las pruebas XSS, se tomó como referencia los resultados obtenidos en el análisis general de vulnerabilidades, además de utilizar la herramienta XSSER de KALI LINUX.

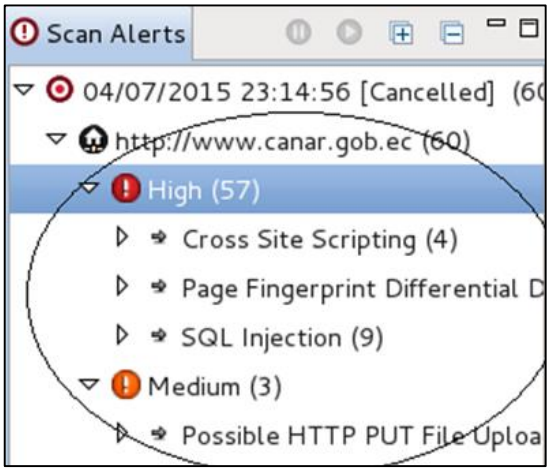


Figura 20. Resultado análisis con VEGA

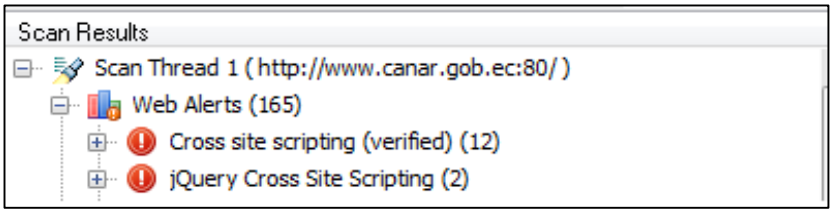


Figura 21. Resultado análisis con ACCUNETIX

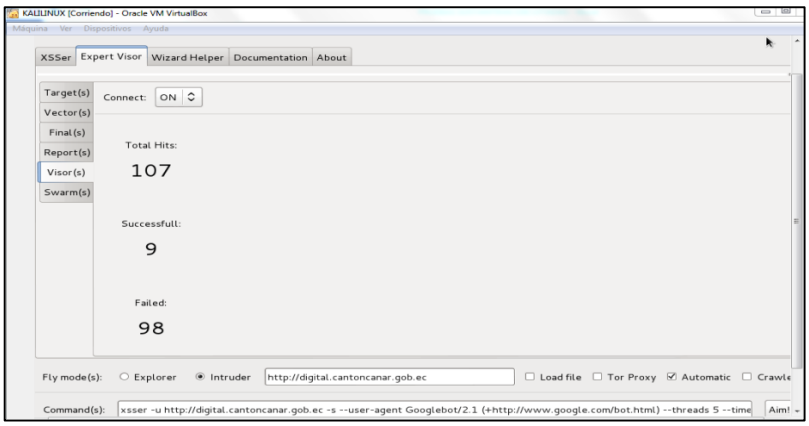


Figura 22. Resultado análisis con **XSSER (KALI LINUX)**

Tabla 28

Resumen de los resultados obtenidos en cada una de las herramientas utilizadas.

	APLICACIONES WEB AUDITADAS	
HERRAMIENTAS	digital.cantoncanar.gob.ec	www.canar.gob.ec
ACCUNETIX	NO	SI
VEGA- KALI LINUX	NO	SI
XSSER- KALI LINUX	SI	NO

4.2.4.5. Análisis De Referencias Inseguras A Referencias De Objetos Directos

Para el actual análisis se utilizó como herramienta ACCUNETIX, y se realizaron pruebas manuales en las aplicaciones web auditadas.

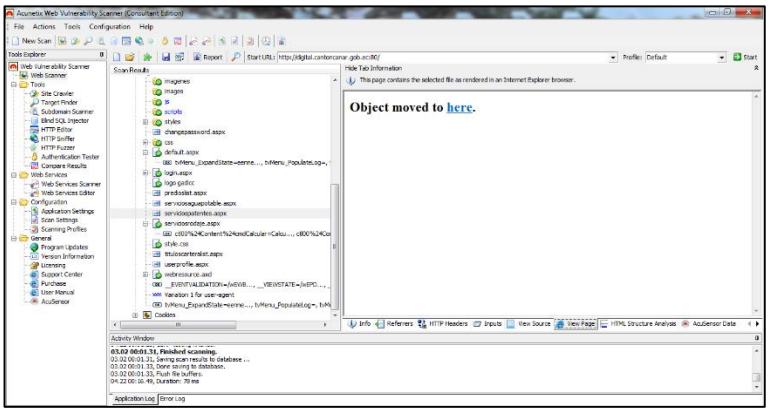


Figura 23. Resultado análisis con **ACCUNETIX**

Tabla 29

Resumen de los resultados obtenidos en cada una de las herramientas utilizadas.

	APLICACIONES WEB AUDITADAS	
HERRAMIENTAS	digital.cantoncanar.gob.ec	www.canar.gob.ec
ACCUNETIX	NO	NO

4.2.4.6. Configuración De Seguridad Incorrecta.

Para la identificar que la configuración de seguridad de los aplicativos WEB es incorrecta, se realizó el análisis de vulnerabilidad de indexación de directorio.

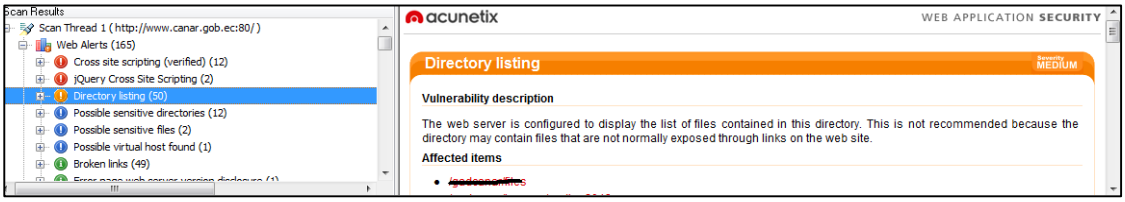


Figura 24. Resultado análisis con **ACCUNETIX**

Tabla 30

Resumen de los resultados obtenidos en cada una de las herramientas utilizadas.

	APLICACIONES WEB AUDITADAS	
HERRAMIENTAS	digital.cantoncanar.gob.ec	www.canar.gob.ec
ACCUNETIX	NO	SI

4.2.4.7. Pruebas de exposición de datos sensibles.

Para este punto de OWASP se realizó el análisis de interceptación de datos no encriptados, determinando si los datos sensibles de la aplicación se encuentran debidamente encriptados.

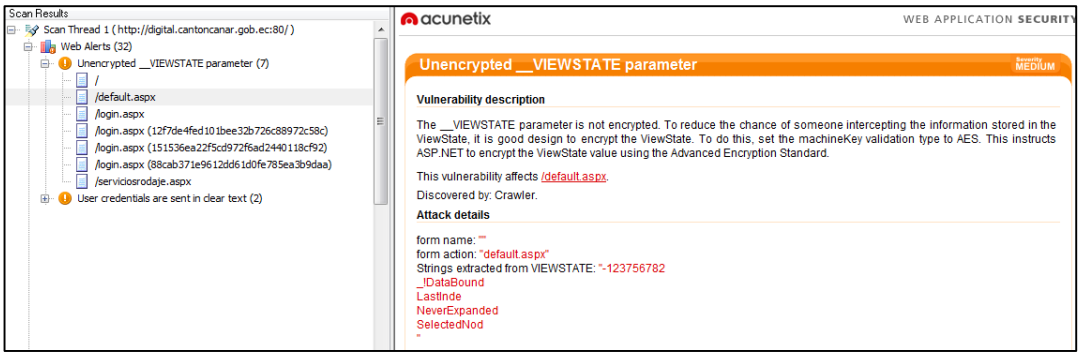


Figura 25. Resultado análisis con **ACCUNETIX.** Datos no encriptados

Figura 26. Resultado análisis con **VEGA (KALI LINUX).** Contraseña sin cifrar.

Tabla 31

Resumen de los resultados obtenidos en cada una de las herramientas utilizadas.

	APLICACIONES WEB AUDITADAS	
HERRAMIENTAS	digital.cantoncanar.gob.ec	www.canar.gob.ec
ACCUNETIX	SI	NO

4.2.4.8. Análisis de ausencia de control de acceso a funciones.

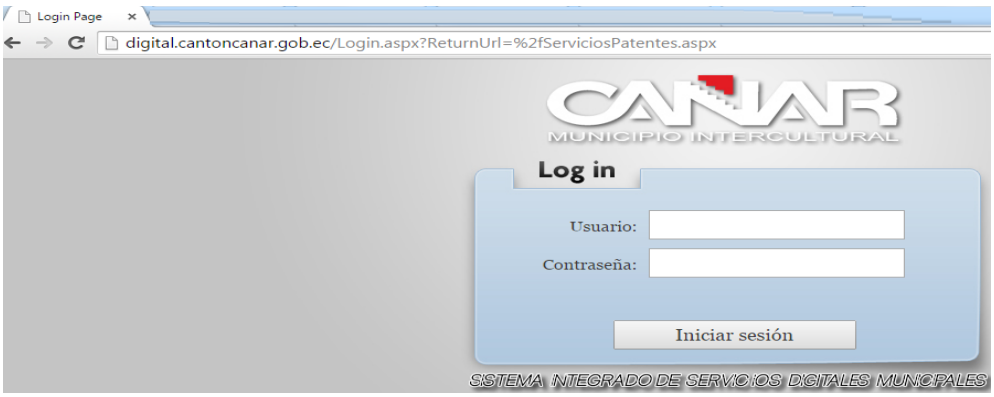


Figura 27. Solicitud de inicio de sesión para el acceso

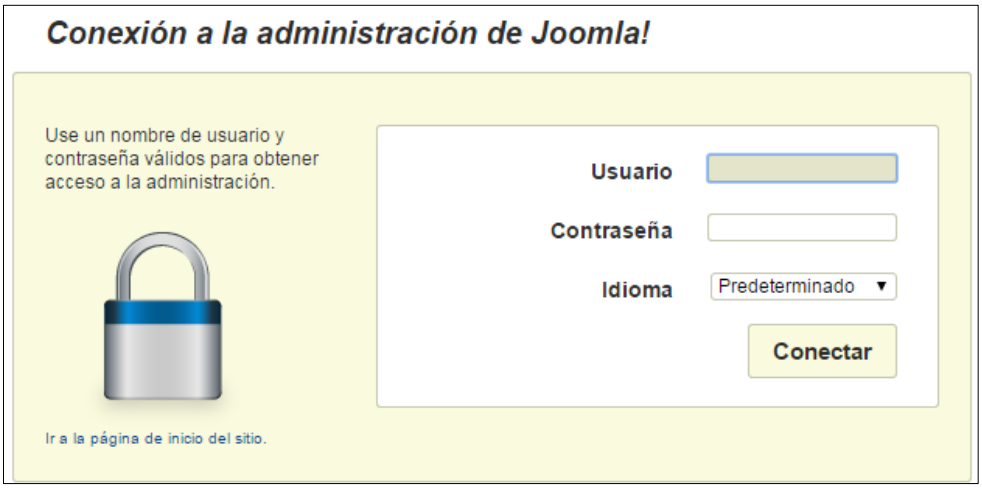


Figura 28. Solicitud de inicio de sesión para el acceso a funciones determinadas

Tabla 32

Resumen de los resultados obtenidos en cada una de las herramientas utilizadas.

	APLICACIONES WEB AUDITADAS	
HERRAMIENTAS	digital.cantoncanar.gob.ec	www.canar.gob.ec
ACCUNETIX	NO	NO
PRUEBAS MANUALES	NO	NO
OBSERVACIONES	Las funciones únicamente se pueden acceder únicamente con autenticación, no existen funciones de administración	Las funciones únicamente se pueden acceder únicamente con autenticación

4.2.4.9. Análisis De Falsificación De Peticiones En Sitios Cruzados (CSRF)

Para este punto se realizaron pruebas manuales, así también se utilizaron las herramientas XSSER y VEGA-, en vista de que si una aplicación es vulnerable a ataques XSS es probable de que también pueda ser de los ataques CSRF.

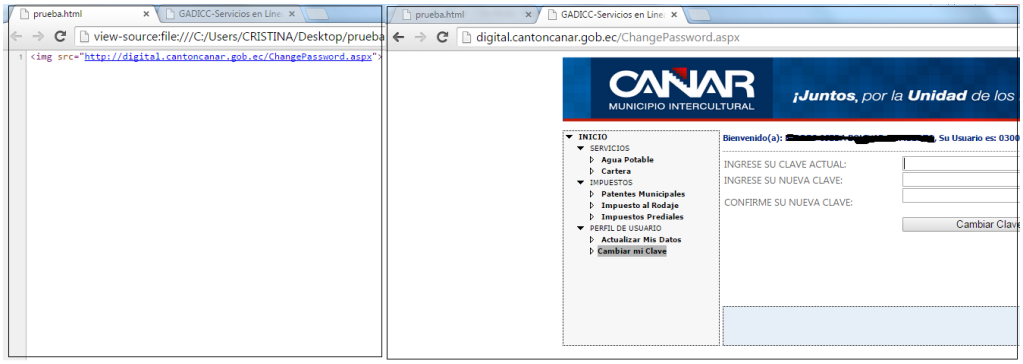


Figura 29. Prueba exitosa (CSRF) a la aplicación web digital.cantonanar.gob.ec. Ausencia de mecanismos de re-autenticación (CAPTCHA)

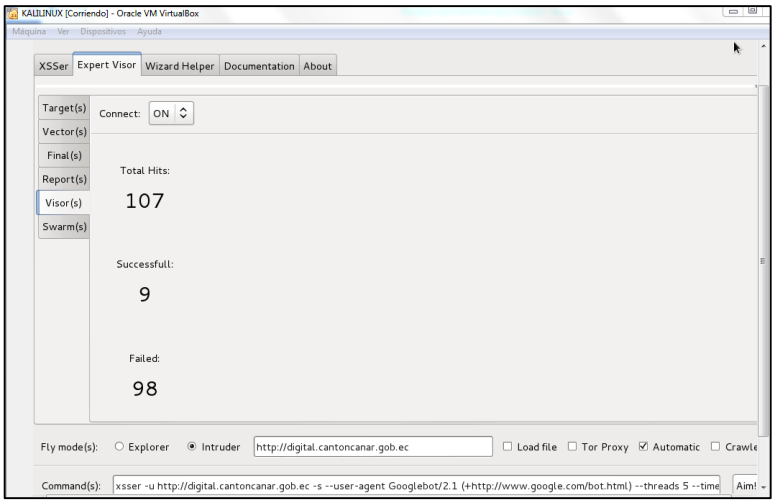


Figura 30. Vulnerabilidad XSS detectada. Influye a ser vulnerable a ataques **(CSRF)**

Figura 31. Presencia de mecanismos de re-autenticación (CAPTCHA)

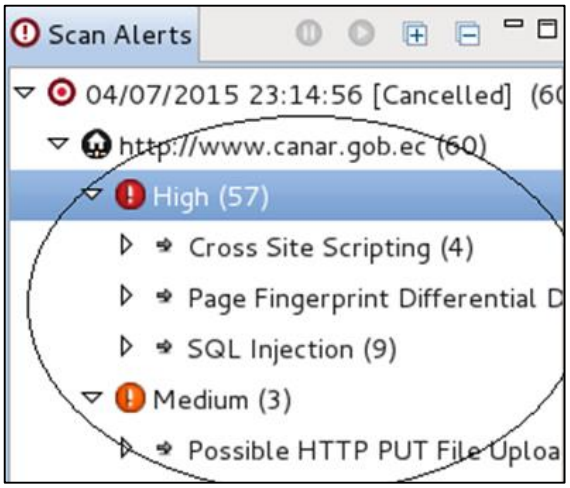


Figura 32. Vulnerabilidad XSS detectada. Influye a ser vulnerable a ataques **(CSRF)**

Tabla 33

Resumen de los resultados obtenidos en cada una de las herramientas utilizadas.

	APLICACIONES WEB AUDITADAS	
HERRAMIENTAS	digital.cantoncanar.gob.ec	www.canar.gob.ec
SCRIPT	SI	NO
CAPTCHA	SI	NO
XSS	SI	SI

4.2.4.10. Análisis De Falsificación De Peticiones En Sitios Cruzados (CSRF).

Para este análisis se utilizaron diferentes herramientas para cada una de las aplicaciones auditadas, es así que para el sitio web del municipio se utilizó JOOMSCAN que es una herramienta de KALI Linux propia para determinar la vulnerabilidad de las aplicaciones web diseñadas en JOOMLA.

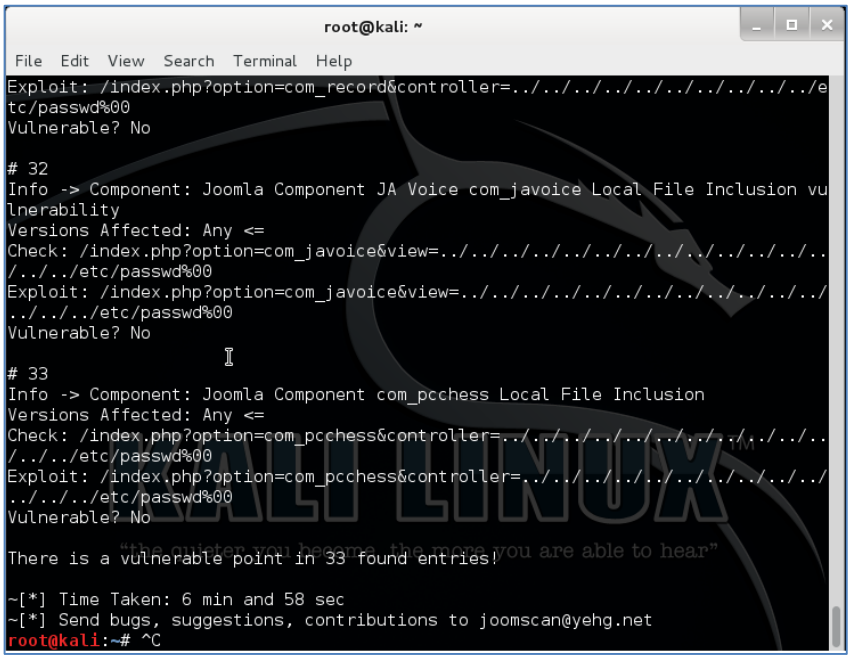


Figura 33. Resultados del análisis efectuado con la herramienta JOOMSCAN

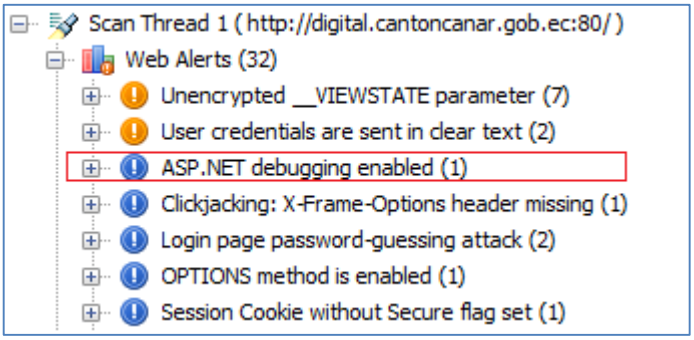


Figura 34. Resultados del análisis efectuado con la herramienta ACCUNETIX

Tabla 34

Resumen de los resultados obtenidos en cada una de las herramientas utilizadas.

	APLICACIONES WEB AUDITADAS	
HERRAMIENTAS	digital.cantoncanar.gob.ec	www.canar.gob.ec
VULNERABILIDADES DE ASP. NET	SI (CRITICIDAD BAJA)	
VULNERABILIDADES DE JOOMLA		NO

4.2.4.11. Análisis de redirecciones y reenvíos no validados.

Para desarrollar este punto se realizaron pruebas manuales con el fin de determinar si la aplicación hacia uso de redirecciones y reenvíos, para luego determinar si se encuentran correctamente validado. Es así el caso de la aplicación www.canar.gob.ec, en la misma que pudimos constatar que no se encontraba implementados redirecciones y reenvíos.

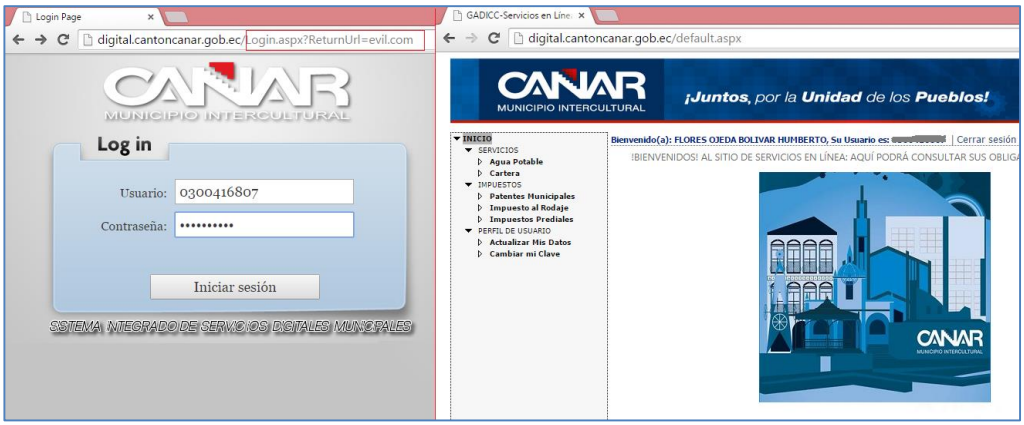


Figura 35. Resultados de las pruebas de redirecciones y reenvíos no validados

Tabla 35

Resumen de los resultados obtenidos en cada una de las herramientas utilizadas.

	APLICACIONES WEB AUDITADAS	
HERRAMIENTAS	digital.cantoncanar.gob.ec	www.canar.gob.ec
PRUEBAS MANUALES	NO	NO

Tabla 36

Resumen general de las vulnerabilidades detectadas en la aplicación Web.

	VULNERABILIDADES DE APLICACIONES WEB AUDITADAS	
OWASP TOP 10	digital.cantoncanar.gob.ec	www.canar.gob.ec
A1- Inyección	**NO**	**SI**
A2 – Pérdida de Autenticación y Gestión de Sesiones.	**SI**	**SI**
A3 – Secuencia de Comandos en Sitios Cruzados (XSS)	**SI**	**SI**
A4 – Referencia Directa Insegura a Objetos	**NO**	**NO**
A5 – Configuración de Seguridad Incorrecta	**NO**	**SI**
A6 – Exposición de datos sensibles	**SI**	**NO**
A7 – Ausencia de Control de Acceso a Funciones	**NO**	**NO**
A8 - Falsificación de Peticiones en Sitios Cruzados (CSRF)	**SI**	**NO**
A9 – Utilización de componentes con vulnerabilidades conocidas	**SI**	**NO**
A10 – Redirecciones y reenvíos no validados	**NO**	**NO**

4.2.5. Pruebas de cumplimiento ejecutadas.

Para ejecutar las pruebas de cumplimiento fue necesario visitar las instalaciones del departamento informático y entrevistarnos con el Ing. Danny Andrade Cárdenas responsable del departamento, con quien pudimos constatar la existencia o no de controles y documentación requerida para el análisis.

Los resultados obtenidos se encuentran en la siguiente tabla que ilustra el cumplimiento o no de los parámetros seleccionados.

Tabla 37

Resultado de la aplicación del cuestionario de pruebas de cumplimiento.

CUESTIONARIO	SI	NO	MEDIO DE VERIFICACIÓN
A1- INYECCIÓN			
El departamento informático cuenta con una política de pruebas de desarrollo seguro, estableciendo procedimientos en contra de los posibles ataques de Inyección. ?		X	Cuenta con política de desarrollo pero no se encuentra documentada.
A2 – PÉRDIDA DE AUTENTICACIÓN Y GESTIÓN DE SESIONES.			
Se encuentra establecido el cumplimiento de los requisitos de autenticación y gestión de sesiones definidos en el APPLICATION SECURITY VERIFICATION STANDARD de OWASP, o de alguna otra normativa. ?		X	No cuenta con políticas
A3 – SECUENCIA DE COMANDOS EN SITIOS CRUZADOS (XSS)			
Cuenta con políticas de seguridad de contenido para defenderse contra XSS. ?		X	No cuenta con política
¿El software se encuentra actualizado? Esto incluye el SO, Servidor Web/Aplicación, DBMS, aplicaciones.	X		El software se encuentra con la última actualización estable.
A5 – CONFIGURACIÓN DE SEGURIDAD INCORRECTA			
¿El manejo de errores revela **NO** rastros de las capas de aplicación u otros mensajes de error demasiado informativos a los usuarios?	X		Mensajes de error únicamente indican versión del software.
A6 – EXPOSICIÓN DE DATOS SENSIBLES			
Se utiliza algún algoritmo criptográfico. ?		X	La aplicación WEB implementada en el entorno ASP.NET no utiliza ningún algoritmo criptográfico.
A8 - FALSIFICACIÓN DE PETICIONES EN SITIOS CRUZADOS (CSRF)			
La aplicación WEB cuenta con mecanismos de re-autenticación (CAPTCHA). ?		X	No cuenta con mecanismos de re-autenticación (CAPTCHA).
La aplicación web desarrollada aplica la propiedad ANTI-FORGERY TOKENS para evitar ataques CRSF?		X	Dentro el código no se aplica la propiedad ANTI-FORGERY TOKENS

4.2.6. Evaluación de los resultados obtenidos en las pruebas de auditoría

Para finalizar esta fase se evaluaron los resultados obtenidos en las pruebas de cumplimiento y sustantivas, analizando las observaciones de auditoría y puntos que se pueden mejorar para los controles y datos deficientes, identificando las causas, el impacto y los efectos de dichas observaciones para la organización y verificando los estándares y mejores prácticas que no se están cumpliendo.

Como última etapa de esta fase se elaboran las conclusiones de auditoría para los resultados no satisfactorios.

Tabla 38

Anexos de cada una de las actividades desarrolladas en la etapa actual.

PRODUCTOS DE LA ETAPA	ANEXOS
Listado con análisis de observaciones de auditoría para pruebas de cumplimiento y sustantivas.	S-07.01 Evaluación De Resultados De Pruebas Ejecutadas
Conclusiones de los resultados obtenidos.	S-07.01 Evaluación De Resultados De Pruebas Ejecutadas

4.3. FASE III. Comunicación de los resultados

Esta es la última fase de la auditoría, en ella se resumen los resultados más significativos obtenidos en las etapas anteriores.

Estos son los insumos para elaborar el informe de auditoría con el cual se comunicará a la alta dirección y a los demás interesados, las observaciones y conclusiones sobre las características de seguridad, calidad y confiabilidad de la información y de los recursos tecnológicos y humanos que intervienen en las actividades de control de los procesos de negocio y sistemas de información.

Organizar y cerrar expediente y archivo con hojas de trabajo. Se elabora el resumen de observaciones que servirá de base para desarrollar y aprobar informe preliminar; luego se analizará respuesta del servicio al informe preliminar para diseñar las conclusiones generales y específicas de la auditoría. Para finalizar con la elaboración

y aprobación y emisión del informe final de auditoría, para proceder a organizar y cerrar expediente y archivo con hojas de trabajo

La etapa de seguimiento a las observaciones de auditoría ya no será realizada ya que se encuentra fuera del alcance del proyecto, y será la entidad receptora del proyecto la encargada de su ejecución

4.3.1. Elaboración del informe con los resultados de la auditoría

Tabla 39

Anexos de cada una de las actividades desarrolladas en la etapa actual.

PRODUCTOS DE LA ETAPA	**ANEXOS**
Resumen de observaciones obtenidas.	S-08.01 Hoja De Hallazgos
Informe preliminar de auditoría.	
Documento con el análisis de las respuestas emitidas por el servicio auditado al informe preliminar.	S-08 .02 Borrador Del Informe
Informe final de auditoría.	S-08.03 Informe Final
Expediente de auditoría con observaciones organizadas y referenciadas adecuadamente.	S-08 .02.02 Convocatoria Socialización Informe

CAPTÍTULO V
PROPUESTA DE BUENAS PRÁCTICAS DE SEGURIDAD

5.1. Objetivo

El objetivo de esta guía instruir al personal técnico, autoridades y consultores del GADIC CAÑAR; sobre las secuelas que podrían dejar sobre su organización las vulnerabilidades de seguridad de sus aplicativos web. Es difícil romper de las costumbres mantenidas por mucho tiempo y por esta causa puede que no estés de acuerdo con algunas de las recomendaciones aquí emitidas. En cualquier caso, creemos que si sigues estas buenas prácticas podrás desarrollar aplicaciones mucho más seguras y eficientes.

5.2. A quién se dirige esta Guía

Esta guía está pensada para el personal informático del GADIC CAÑAR, así como para los consultores independientes que laboran conjuntamente en la institución, sin importar si es experto o principiante. Se intentó construir una guía muy compacta y de fácil lectura y consulta.

5.3. Buenas prácticas de seguridad para el desarrollo web.

5.3.1. Mitigación del OWASP Top 10 2013

El OWASP Top 10 nos suministra un grupo de procedimientos básicos que ayuda a protegerse del alto riesgo que provoca mantener estas vulnerabilidades y los pasos a seguir para minimizarlas.

El atacante usará diferentes rutas dentro de la aplicación web para dañar su empresa. Todas estas rutas representarán un riesgo que puede, o no, ser altamente grave como para fijar la atención.

De igual forma el daño causado podrá se insignificante o sacarlo del negocio. Para calcular el riesgo en su organización, se calcula la probabilidad relacionada a la agente de amenaza, vector de ataque, y la debilidad en la seguridad, y combinarla con una estimación del impacto técnico y de negocios para su organización. En conjunto, estos factores determinan el riesgo global. (OWASP FOUNDATION, 2013)

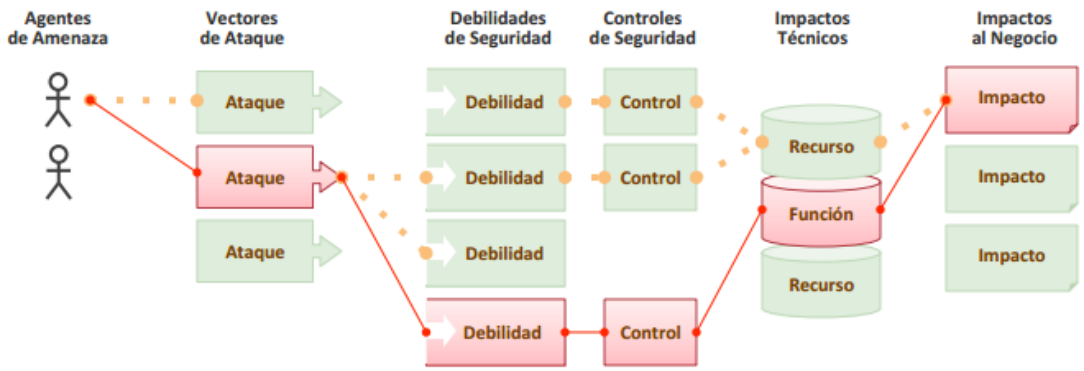


Figura 36. Método de determinación del Riesgo global

Fuente: (OWASP FOUNDATION, 2013)

El OWASP Top 10 se enfoca en la identificación de los riesgos más serios para la organización, proporcionando información sobre la probabilidad y el impacto técnico a través del siguiente esquema de calificaciones.

Agente de Amenaza	Vectores de Ataque	Prevalencia de Debilidades	Detectabilidad de Debilidades	Impacto Técnico	Impacto al Negocio
Específico de la aplicacion	Fácil	Difundido	Fácil	Severo	Específico de la aplicación /negocio
	Promedio	Común	Promedio	Moderado	
	Difícil	Poco Común	Difícil	Menor	

Figura 37. Esquema de calificaciones basado en Metodología de Evaluación de Riesgos

Fuente: (OWASP FOUNDATION, 2013)

Usted debe evaluar cada riesgo, enfocándose en los agentes de amenaza, los controles de seguridad y el impacto al negocio

5.3.1.1. A1 – Inyección.

La inyección es una técnica frecuente para atacar aplicaciones web, existen variantes como son SQL, OS, y LDAP, consiste en la inclusión de datos no confiables en un intérprete como parte de un comando o consulta engañándolo para ejecutar comandos no premeditados o acceder datos no autorizados.

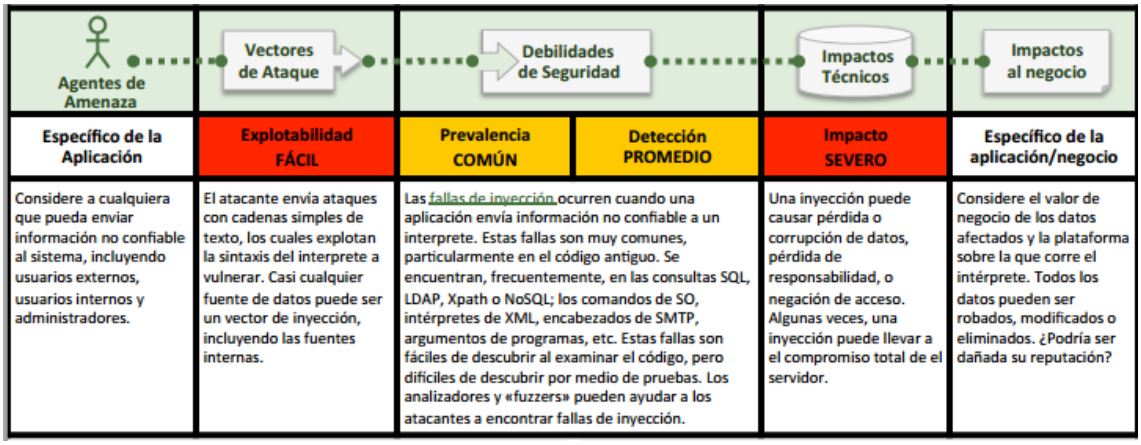


Figura 38. Evaluación del riesgo por Inyección.

Fuente: (OWASP FOUNDATION, 2013)

Par evitar esta clase de ataques es necesario evitar que el usuario introduzca datos ni caracteres sin control alguno, es así que se debe separar los comandos y consultas.

1. El uso de una API segura que evite el uso de intérpretes por completo o provea una interface parametrizada, es uno de los métodos más utilizados.
2. En caso de no disponer de una API parametrizada, la codificación de los caracteres especiales, utilizando la sintaxis de escape específica.
3. La validación de entradas positiva es otra técnica utilizada, aunque no es una protección completa debido a que algunas aplicaciones necesitan de estos caracteres en sus entradas.

5.3.1.2. A2-Pérdida de autenticación y gestión de sesiones.

Es un tipo de inseguridad informática ocasionada cuando las funciones de autenticación y gestión de sesiones son vulnerables, permite a los atacantes acceder a contraseñas que podrán asumir la identidad de otros usuarios.

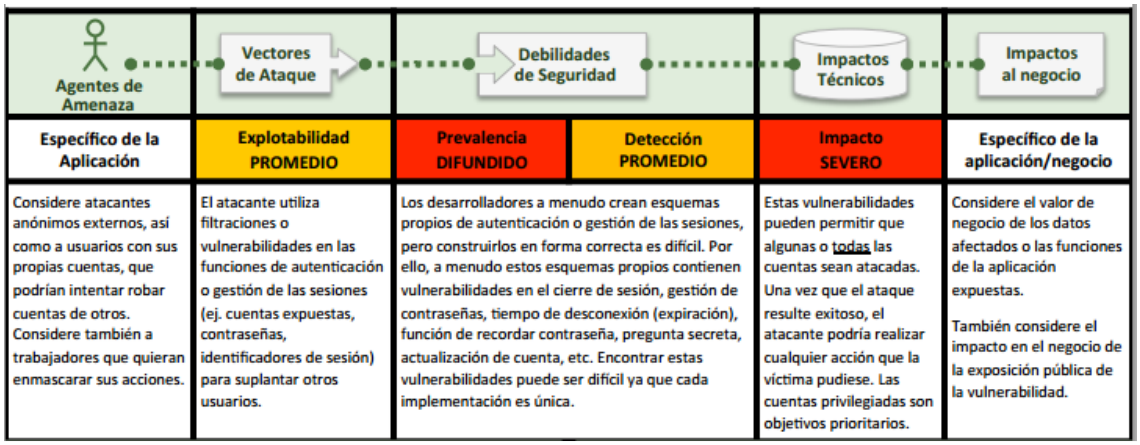


Figura 39. Evaluación del riesgo por Pérdida de autenticación y gestión de sesiones

Fuente: (OWASP FOUNDATION, 2013)

La recomendación es la siguiente:

La Organización facilitará a los desarrolladores de un único conjunto de controles de autenticación y gestión de sesiones fuerte. Estos controles deben cumplir con todos los requisitos de autenticación y gestión de sesiones definidos en el APPLICATION SECURITY VERIFICATION STANDARD (ASVS) de OWASP

5.3.1.3. A3-Secuencia de comandos en sitios cruzados XSS

Es un agujero de seguridad típico de aplicativos web cuando toma datos no confiables y los envía al navegador web sin validarlos y codificarlos. XSS permite a los atacantes ejecutar secuencia de comandos en el navegador de la víctima los cuales pueden robar información sensible, tomar por secuestro sesiones de usuario, destruir sitios web, o dirigir al usuario hacia un sitio malicioso

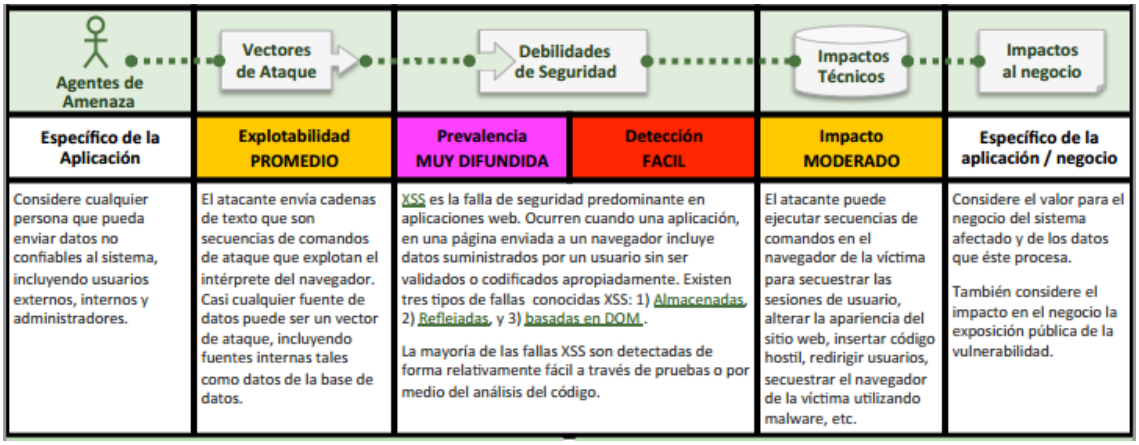


Figura 40. Evaluación del riesgo por Secuencia de comandos en sitios cruzados XSS

Fuente: (OWASP FOUNDATION, 2013)

Para evitar ataques XSS se requiere mantener los datos no fiables separados del contenido activo del navegador.

1. La solución más propicia para este tipo de ataque consiste en la codificación de los datos no confiables basados en el contexto HTML donde serán ubicados.
2. Es recomendable también la validación de entradas positiva considerando que una variedad aplicativos acepta caracteres especiales como entradas válidas. Esta validación contendrá el largo, los caracteres, el formato y reglas de negocio que debe cumplir el dato antes de ser aceptarlo como entrada valida.
3. Para el contenido de formato enriquecido, las bibliotecas de auto sanitización como AntiSamy de OWASP o el proyecto sanitizador de HTML en Java son una buena opción.
4. Las políticas de seguridad de contenido podrían minimizar el riesgo

5.3.1.4. A4-Referencia directa insegura a objetos.

Es una vulnerabilidad informática ocasionada cuando un desarrollador revela la referencia a un objeto de implementación interno. (Fichero, directorio, o base de datos)

Lo que permite que los atacantes puedan manipular dichos objetos y acceder a esta información.

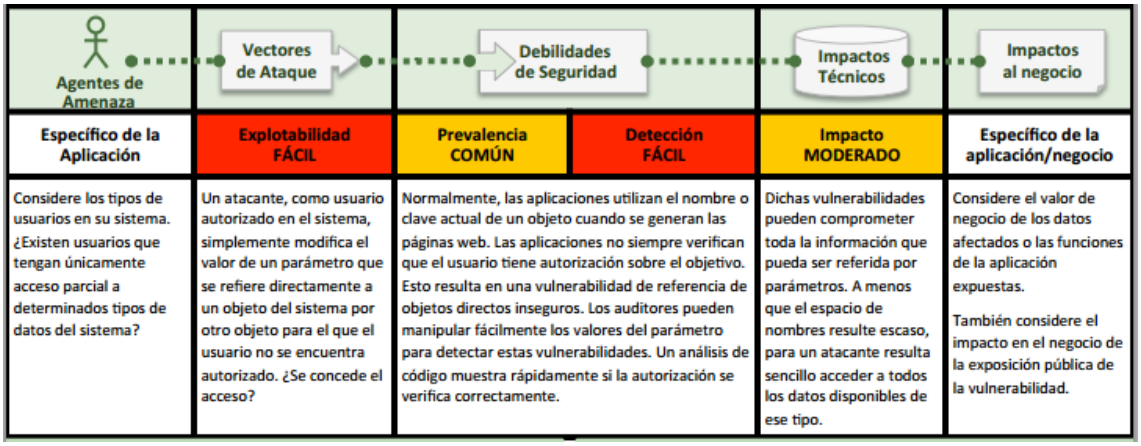


Figura 41. Evaluación del riesgo por Referencia directa insegura a objetos

Fuente: (OWASP FOUNDATION, 2013)

Las recomendaciones principales para este tipo de ataque son:

- Una solución a este tipo de ataque es el uso referencias indirectas por usuario o sesión. Evitando el acceso directo a los recursos por parte de los atacantes. ESAPI de OWASP dispone relaciones secuenciales y aleatorias de referencias de acceso que los programadores pueden utilizar para eliminar las referencias directas a objetos.
- Incluir una comprobación de control de acceso en cada uso de una referencia directa a un objeto de una fuente que no es de confianza para asegurar que el usuario está autorizado a acceder al objeto solicitado.

5.3.1.5. A5-Configuración de seguridad incorrecta.

Esta vulnerabilidad es ocasionada por no definir, implementar y mantener la configuración de seguridad y mantener la configuración por defecto de la aplicación, entorno de trabajo, servidor de aplicación y web, base de datos, y plataforma.

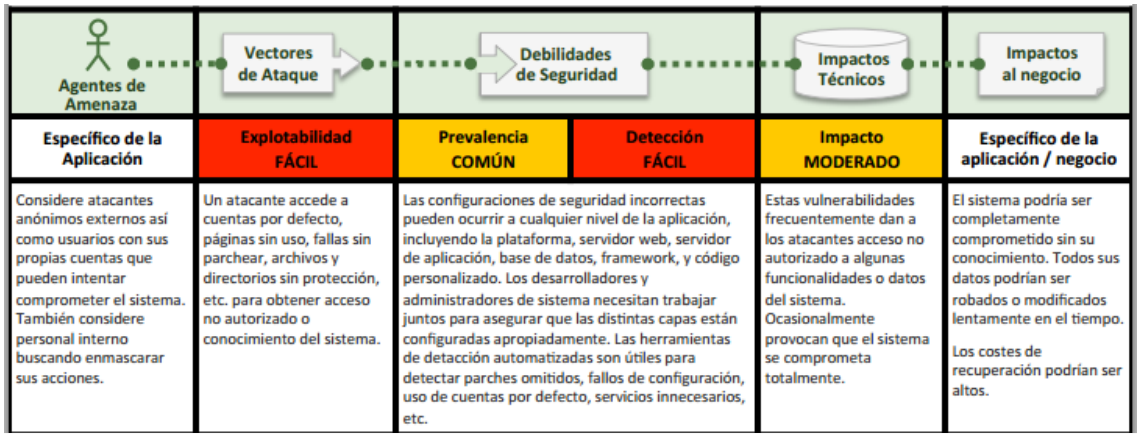


Figura 42. Evaluación del riesgo por Configuración de seguridad incorrecta

Fuente: (OWASP FOUNDATION, 2013)

Las recomendaciones para esta vulnerabilidad informática son:

1. El proceso de fortalecimiento debe ser rápido, fácil y repetible para lograr un entorno apropiadamente asegurado. Los ambientes de Desarrollo, QA y Producción deben ser configurados idénticamente
2. Mantener al día la actualización y los parches del software necesario para el funcionamiento de los aplicativos
3. Mantener siempre una robusta arquitectura de aplicación separando efectiva y seguramente los componentes.
4. Ejecutar escaneos y realizar auditorías periódicamente para detectar fallos de configuración.

5.3.1.6. A6-Exposición de datos sensibles

Esta vulnerabilidad ocurre cuando las aplicaciones web descuidan la protección datos sensibles como son las credenciales de autenticación, números de tarjetas de crédito claves. Los atacantes pueden acceder a estos datos para modificarlos, realiza robos, fraudes, suplantación de identidad, estafas etc.

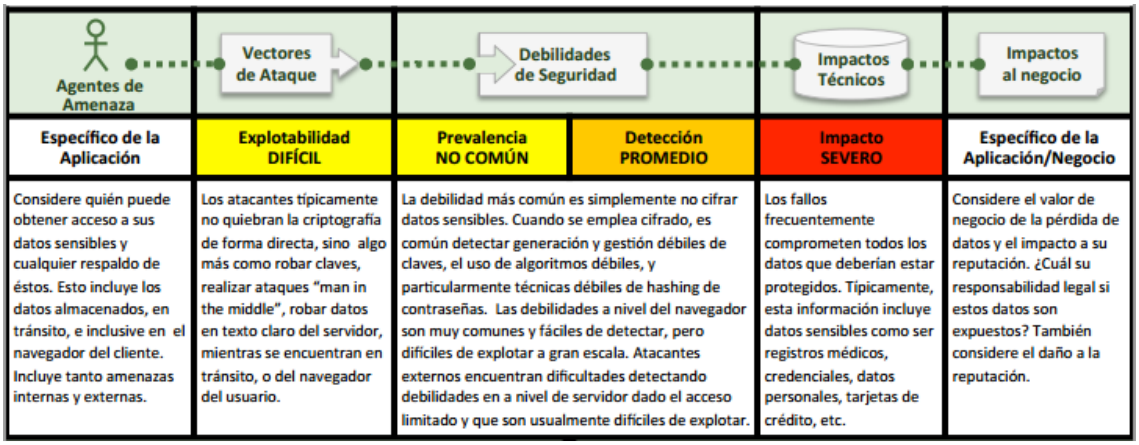


Figura 43. Evaluación del riesgo por Exposición de datos sensibles

Fuente: (OWASP FOUNDATION, 2013)

Para los datos sensibles, se deben realizar como mínimo los siguientes procedimientos:

- Asegúrese de cifrar todos los datos sensibles almacenados o en tráfico de manera de defenderse de las amenazas.
- No almacene datos sensibles que no sean necesarios, deséchelos inmediatamente
- Aplicar algoritmos de cifrado fuertes y estándar así como claves fuertes y gestiónelas de forma segura.
- Las claves deben ser almacenadas con algoritmos diseñados para protegerlas como pueden ser bcrypt, PBKDF2 o scrypt.
- Se debe deshabilitar la opción de autocompletar de los formularios que reciben estos datos sensibles.
- También se debe deshabilitar la opción de cacheado de las páginas que contengan datos sensibles.

5.3.1.7. A7-Ausencia de control de acceso a las funciones

Las aplicaciones web requieren de una verificación del control de acceso al servidor cuando desde este se tiene acceso a cada función. Cuando estas no son verificadas, el ataque consistirá en realizar peticiones sin la respectiva autorización

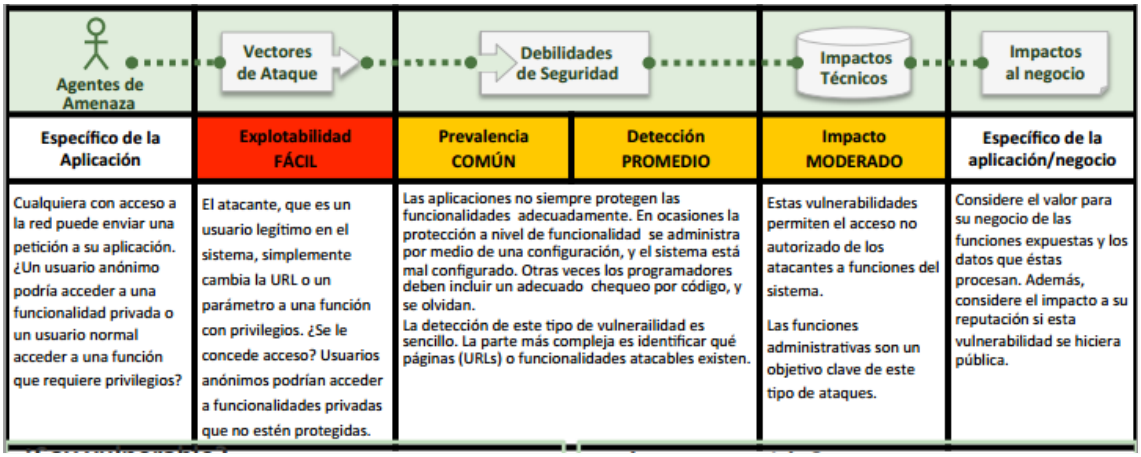


Figura 44. Evaluación del riesgo por Ausencia de control de acceso a las funciones

Fuente: (OWASP FOUNDATION, 2013)

La aplicación contará de un módulo de autorización sólido y fácil de analizar, el cual se podrá invocar desde todas las funciones de negocio.

1. El proceso para gestión de accesos y permisos debería ser actualizable y auditable con facilidad. No lo implemente nuevo código que no se encuentre parametrizado.
2. El mecanismo negará cualquier acceso por defecto, solicitando el permiso a roles específicos para acceder a cada funcionalidad.
3. Si la funcionalidad es parte del flujo de trabajo, se debe comprobar que las condiciones del flujo se encuentren adecuadamente establecidas para permitir el acceso.

5.3.1.8. A8-Falsificación de peticiones en sitios cruzados CSRF

Es un exploit malicioso en el cual el navegador web validado es obligado a enviar una solicitud HTTP falsificado, que incluye la sesión del usuario y otra información de autenticación incluida de forma automática, a una aplicativa web vulnerable. El navegador de la víctima genera pedidos que el aplicativo con vulnerabilidades cree son solicitudes validas provenientes de la víctima.

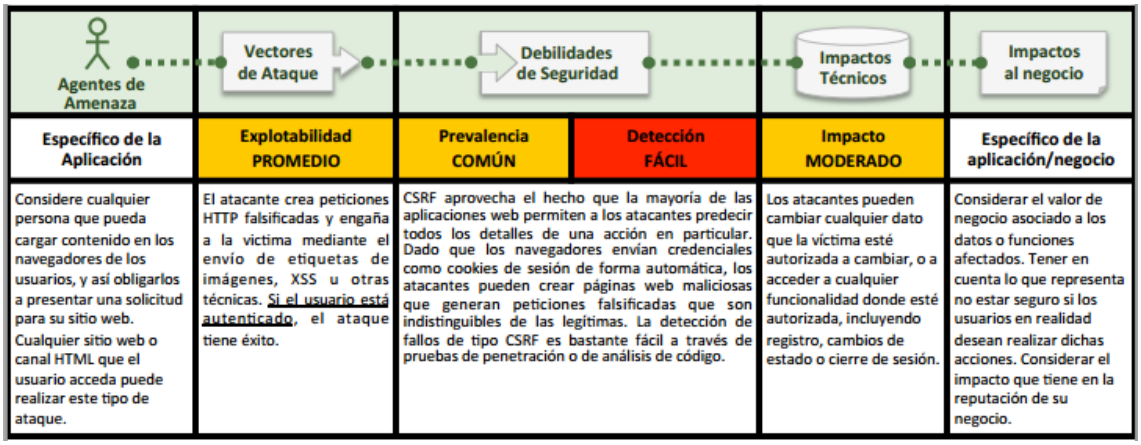


Figura 45. Evaluación del riesgo por Falsificación de peticiones en sitios cruzados

Fuente: (OWASP FOUNDATION, 2013)

Para evitar este tipo de ataque es necesario un TOKEN único en cada solicitud HTTP. Estos TOKENS deben cambiar y ser únicos en cada sesión del usuario.

1. Incluir el TOKEN único en un campo oculto, dicho campo debe enviarse en el cuerpo de la solicitud HTTP, evitando que se incluya en la URL, donde puede estar más sujeta a exposición.
2. También se puede incluir este TOKEN único en la URL, o un parámetro de la misma este método presenta el riesgo de que la URL sea expuesta a un atacante y pueda comprometer el TOKEN secreto.
3. Solicite una nueva autenticación por parte del usuario, o pruebas que se trata de un usuario legítimo, esto se puede realizar mediante el uso de CAPTCHA.

5.3.1.9. A9-Uso de componentes con vulnerabilidades conocidas

Este ataque consiste en actuar sobre un componente vulnerable lo cual facilita la el acceso servidor o una pérdida de datos. Utilizar componentes con vulnerabilidades conocidas permite ampliar el rango de posibles ataques e impactos.

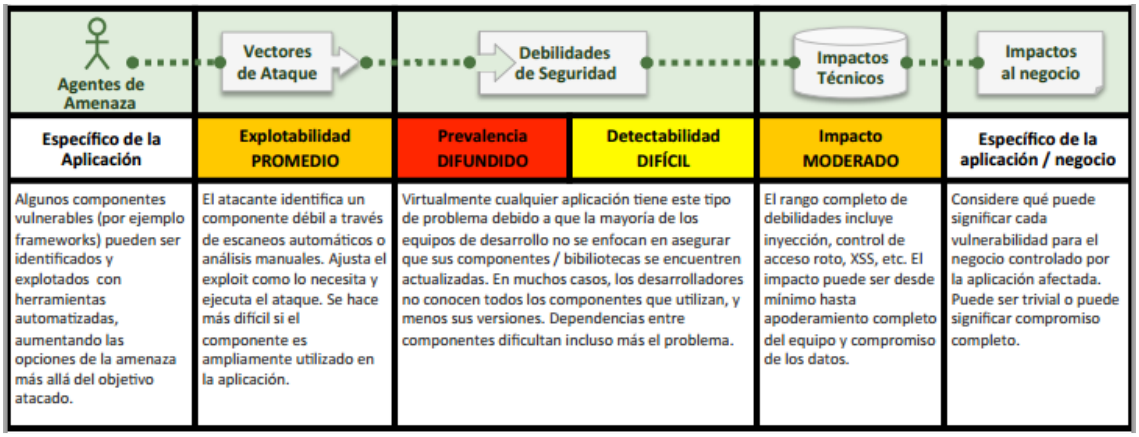


Figura 46. Evaluación del riesgo por Uso de componentes con vulnerabilidades conocidas

Fuente: (OWASP FOUNDATION, 2013)

El hecho actualizar los componentes a las nuevas versión es crítico. Proyectos de software debieran tener un proceso para:

1. Mantener actualizada la seguridad de los componentes mediante en bases de datos públicas, lista de correos del proyecto, y lista de correo de seguridad.
2. Políticas de seguridad para regular el uso de componentes
3. Agregar capas de seguridad sobre el componente para asegurar los aspectos débiles o vulnerables de este.

5.3.1.10. A10-Redirecciones y reenvíos no validados

Esta vulnerabilidad informática se aprovecha de que los aplicativos web redirigen y reenvían a las victimas hacia otras páginas o sitios web, si la validación no es la apropiada, las víctimas son redirigidos hacia páginas web de phishing o malware, o páginas no autorizadas.

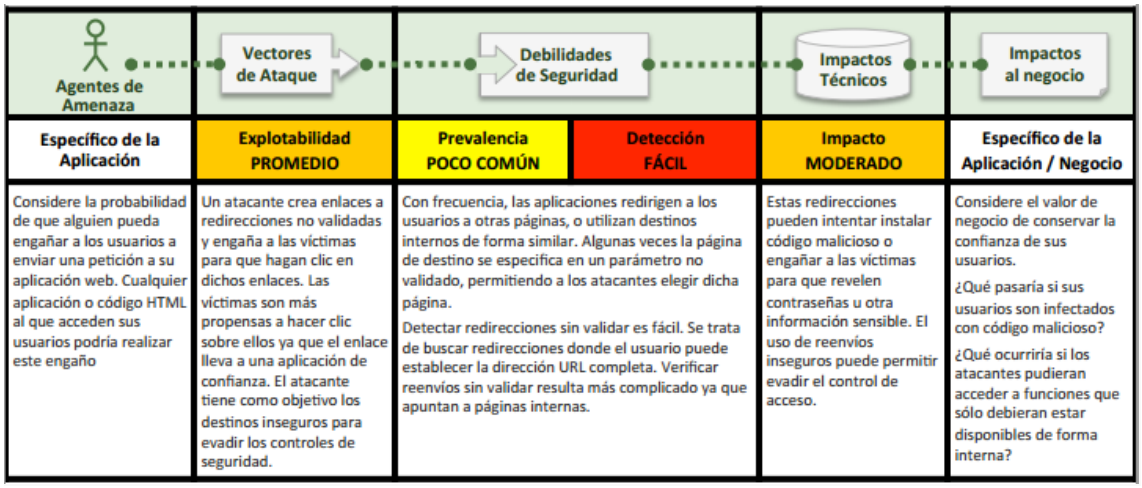


Figura 47. Evaluación del riesgo por Redirecciones y reenvíos no validados

Fuente: (OWASP FOUNDATION, 2013)

El reenvío y redirección de manera segura se puede realizarse de varias maneras:

1. No realizar reenvíos y redirecciones.
2. No involucrar parámetros manipulables.

5.3.2. En caso de que los reenvíos y redirecciones no pueden ser evitados el valor de cualquier parámetro de destino debe ser un valor de mapeo, en lugar de la dirección URL real y en el código del servidor traducir dicho valor a la dirección URL.

5.3.3. Políticas de seguridad de la información (ISO 27002).

Para el correcto manejo de los aplicativos web del GADIC CAÑAR se recomienda la implantación de diferentes políticas que garanticen la seguridad de la información:

A. Política de asignación de responsabilidades en materia de seguridad de la información
B. Política de autorización para instalaciones de procesamiento de información
C. Política de contratación de asesoramiento especializado en materia de seguridad de la información
D. Seguridad frente al acceso por parte de terceros
E. Requerimientos de seguridad en contratos o acuerdos con terceros

CAPÍTULO 6
CONCLUSIONES Y RECOMENDACIONES

6.1. CONCLUSIONES

La metodología de OWASP Top 10 presenta una alternativa concisa para determinar las vulnerabilidades de los aplicativos WEB, ya que se han realizado las pruebas sobre los ataques más comunes que comprometen a una aplicación WEB, y esta metodología presenta la mejor alternativa.

Es de gran importancia que las organizaciones gubernamentales apliquen buenas prácticas de desarrollo de aplicaciones WEB, ya que se encuentran sensibles a cualquier ataque, en vista que se encuentran publicadas en el Internet y los datos sensibles de los usuarios pueden ser vulnerados.

La importancia de tener una mejor estructura departamental es trascendente para que los procesos que se desenvuelven internamente sean eficientes, es por ello que el proceso de desarrollo de software debe estar guiado por políticas y procedimientos definidos de manera correcta para evitar comprometer los datos simples de la organización.

Las vulnerabilidades detectadas en las aplicaciones WEB auditadas, han demostrado que la principal causa es el desconocimiento por parte de los desarrolladores, quienes no conocen el impacto de un posible ataque ni los vectores de ocurrencia.

El proceso de auditoría debe ser llevado bajo una metodología de aplicación adecuada, que provea la documentación precisa que permita al auditor demostrar los resultados obtenidos en su evaluación.

La evaluación de riesgos en base a las vulnerabilidades encontradas, se torna de gran importancia debido a que se puede detectar el nivel de criticidad del mismo, y así es posible priorizar a los riesgos que puedan generar daños críticos a la organización si no son mitigados a tiempo.

6.2. RECOMENDACIONES

Aplicar las recomendaciones detalladas en el Informe de Auditoría, para mitigar el riesgo de explotación de las vulnerabilidades detectadas.

Legalizar el manual de buenas prácticas generado en el presente trabajo de tesis mediante el consejo del GADIC Cañar, para pueda ser utilizando por el departamento informático.

Elaborar una política para el personal de desarrollo, quienes deberían estar en el compromiso de seguir las instrucciones descritas en el manual de buenas prácticas para el desarrollo de aplicaciones WEB seguras.

Realizar análisis periódico de vulnerabilidades de las aplicaciones WEB que se generan en el GADIC Cañar, de manera de mitigar riesgos de seguridad que comprometen la estabilidad de los mismos.

BIBLIOGRAFÍA

Amaya Tarazona, C. A. (2014). *SEGURIDAD EN APLICACIONES WEB.* Obtenido de http://datateca.unad.edu.co/contenidos/233008/AVA_2014-I/MATERIAL/UNIDAD_2/UNIDAD_2_SEGURIDAD_EN_APLICACIONES_WEB_2014.pdf

Cabrera Garcia , S., García Castro, M., Salinas Romero, J., Montalvo Gonzales , E., & Rodriguez Arce , M. (2009). *MODELO DE SEGURIDAD EN LAS APLICACIONES WEB DESARROLLADAS POR UN TERCERO.* Mexico DF: UPIIESA.

CAPEC. (13 de Julio de 2014). *https://capec.mitre.org*. Obtenido de https://capec.mitre.org/data/definitions/253.html

CWE. (31 de 12 de 2010). *http://cwe.mitre.org/*. Obtenido de http://cwe.mitre.org/top25/archive/2010/2010_cwe_sans_top25.pdf

Ferrer Martinez, J. (2012). *IMPLANTACION DE APLICACIONES WEB (GRADO SUPERIOR).* España: Ra-Ma.

Gallegos Varela , M. (s.f.). *http://repositorio.utn.edu.ec/.* Obtenido de http://repositorio.utn.edu.ec/bitstream/123456789/1116/5/04%20ISC%20064%20CAPITULO%20V.pdf

General, C. (1 de 1 de 2009). *http://www.cgr.gob.ni/.* Obtenido de Contraloria General, Nicaragua: http://www.cgr.gob.ni/cgr/index.php?option=com_docman&task=doc_download&gid=1631&Itemid=184

Grupo IWI. (2009). *Implantación de la LOPD en la empresa : medidas de seguridad.* España: Málaga Vértice D.L. .

GUAGALANGO VEGA, R. N., & MOSCOSO MONTALVO, P. E. (08 de 2011). *Repositorio Digital ESPE.* Recuperado el 20 de 01 de 2015, de http://repositorio.espe.edu.ec/handle/21000/4279

Gutiérrez, J., & Tena, T. (2003). *Protocolos criptográficos y seguridad de redes.* España: Santander : Universidad de Cantabria.

Hardy, G., & Heschl, J. (2008). ISO/IEC 27002. En G. Hardy, & J. Heschl, *Alineando COBIT® 4.1, ITIL® V3 e ISO/IEC 27002 en beneficio de la empresa* (pág. 17).

ISO/IEC 27000:2005. (2014). *ISO/IEC 27000:2014*. Obtenido de www.iso.org

Luján Mora, S. (2001). *Programación en Internet: Cilentes WEB.* Alicante: Editorial Club Universitario.

Machuca, C. A. (s.f.). Estado del Arte: Servicios Web . *Universidad Nacional de Colombia*, 9.

Melena Yanez, C., & Muñoz Ibsen, E. S. (5 de mARZO de 2015). *Organización Latinoamericana y del Caribe de Entidades Fiscalizadoras Superiores*. Obtenido de OLACEFS: http://www.olacefs.com/wp-content/plugins/google-document-embedder/load.php?d=http%3A%2F%2Fwww.olacefs.com%2Fwp-content%2Fuploads%2F2014%2F08%2F1erlugar.pdf.

OWASP. (Noviembre de 2014). *OWASP*. Obtenido de https://www.owasp.org/index.php/Sobre_OWASP

OWASP FOUNDATION. (31 de 12 de 2013). Obtenido de www.owasp.org/: https://www.owasp.org/index.php/Code_Injection

OWASP FOUNDATION. (2013). *OWASP TOP 10 -2013.* Obtenido de https://www.owasp.org/images/5/5f/OWASP_Top_10_-_2013_Final_-_Espa%C3%B1ol.pdf

Patrick Cauldwell, R. C. (2002). *Servicios Web XML*. España: ANAYA MULTIMEDIA.

Portal ISO 27000. (2013). *El portal de ISO 27001 en Español*. Obtenido de http://www.iso27000.es/iso27000.html

Salgado Yanez, A. L. (Abril de 2014). *http://repositorio.espe.edu.ec/*.

Serrao, C., Aguilera Díaz, V., & Cerullo, F. (2010). *Web Application Security*. Springer.

Steve, P., Cross, M., Kapinos, S., Meer, H., & Muttik, I. (2011). *Web Application Vulnerabilities.* Syngress.

TARLOGIC. (31 de 12 de 2013). *www.tarlogic.com*. Obtenido de https://www.tarlogic.com/servicios/auditorias-de-seguridad-it/auditoria-seguridad-owasp

Van Der Stock, A. (2005). *Una Guía para Construir Aplicaciones y Servicios Seguros.*

Web Application Security Consortium. (1 de 1 de 2014). *http://projects.webappsec.org/*. Obtenido de

http://projects.webappsec.org/w/page/13246973/Threat%20Classification%20Previous%20Versions

Yañez de la Melena, C., & Ibsen Muñoz, S. E. (2011). Enfoque Metodológico de la Auditoría a las Tecnolgías de la información y Comunicaciones. *OLACEFS*, 26-36.

ANEXOS