análisis y definición de requisitos de seguridad informática fundamentado en owasp para el cumplimiento en los aplicativos basados en software libre en gestión documental

DIANA MARCELA CAUCALI BELTRÁN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ, D.C.
2020

ANÁLISIS Y DEFINICIÓN DE REQUISITOS DE SEGURIDAD INFORMÁTICA FUNDAMENTADO EN OWASP PARA EL CUMPLIMIENTO EN LOS APLICATIVOS BASADOS EN SOFTWARE LIBRE EN GESTIÓN DOCUMENTAL

DIANA MARCELA CAUCALI BELTRÁN

Trabajo de Grado para optar por el título

ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Director de Trabajo de Grado

Ing. Yolima Esther Mercado

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ, D.C.
2020

Nota de aceptación:

_____

_____

_____

_____

Presidente del Jurado

_____

Firma del jurado

_____

Firma del jurado

DEDICATORIA

Este proyecto está dedicado a Dios quien siempre está presente y me brinda cada día nuevas oportunidades, bendiciones y salud para poder cumplir mis objetivos.

A mi familia en especial a mi madre y mi hermano quienes son fuerza, apoyo y bienestar, y Dani compañero de vida quien está allí apoyándome incondicionalmente a cada momento y en cada paso para mi crecimiento personal.

AGRADECIMIENTOS

A la ingeniera Yolima por su orientación para el desarrollo de este trabajo, por el tiempo de dedicación y su conocimiento profesional que permitió la culminación de este trabajo.

CONTENIDO

LISTA DE TABLAS

LISTADO DE FIGURAS

LISTADO DE ILUSTRACIONES

LISTADO DE GRÁFICOS

INTRODUCCIÓN

Actualmente, las entidades cuentan con diversas herramientas para la administración y flujo de información producto de las diferentes actividades que realizan las dependencias. Toda esta información suele ser sensible y es objetivo de amenazas, filtraciones, ataques informáticos por medio de diferentes causas, medios o dispositivos que suelen ser inseguros en un sistema, los cuales pueden ser foco o filtro de inseguridad, es por ello que se debe garantizar y mitigar los posibles riesgos, amenazas, vulnerabilidades e impactos que puedan exponer y afectar la información contenida en una aplicación.

La seguridad informática permite establecer mecanismos necesarios para los sistemas informáticos de una organización, por ello así establecer las estrategias, políticas, procedimientos y la aplicación de medidas preventivas para salvaguarda la información y mantenerla libre de daños.

En este sentido, la seguridad informática establece nuevos retos los cuales se deben abordar en materia de seguridad, por lo cual se tomó como modelo de requisitos el OWASP <<Open Web Application Security Project>>, que en español es el “Proyecto abierto de seguridad de aplicaciones web”, este permite documentar y definir actividades para la implementación segura y verificación para así determinar mejoras.

Para este caso, el desarrollo de este proyecto busca identificar los conceptos básicos de seguridad informática que aplican para un software libre de gestión documental y así realizar el análisis de la aplicación en un entorno web de las posibles amenazas, riesgos y vulnerabilidades del sistema, cuyo objetivo es documentar y presentar como resultado de esta monografía las características y requisitos basado en OWASP que debe contener la aplicación que permita administrar y almacenar todo tipo de información de una forma segura.

1. DEFINICIÓN DEL PROBLEMA

1.1 PLANTEAMIENTO

Las organizaciones bien sean de servicio público o privado cuentan con un departamento que administra y dan línea técnica en materia de la documentación que produce una organización, área conocida como gestión documental y correspondencia o grupo de archivo. En la búsqueda de facilitar la administración de los documentos se plantea la implementación en un software que permita la administración de la información de forma eficiente, efectiva y eficaz para optimizar sus procesos en materia de producción documental y gestión de la información con el uso de herramientas tecnológicas.

Por lo cual, aquellas instituciones que no cuenten con los recursos económicos para la adquisición de un software licenciado y la implementación de un gestor documental para la administración de la información analizan y buscan la posibilidad de darle uso a un software libre que cumpla con las características y especificaciones técnicas necesarias como gestor documental o mejorar el que tienen. En este sentido, es importante identificar y describir los requisitos necesarios con los que debe contar un software libre que garantice la seguridad informática. Por ello el modelo basado en OWASP permite diversificar y analizar los diferentes aspectos para definir los aquellos mecanismos de protección de la información de un sistema que almacena el documento electrónico y digital de forma segura.

Por consiguiente, es necesario estudiar el software libre y los posibles tipos de vulnerabilidades que afecten la seguridad, es así como es importante revisar, investigar y analizar de qué forma se pueden aplicar controles de seguridad, permitiendo así a partir de pruebas de un aplicativo crear controles efectivos, mitigar riesgos y detectar de forma temprana las amenazas que se pueden presentar, para aplicar las medidas de seguridad pertinentes, acciones de mejora y correctivas sobre el sistema.

Teniendo en cuenta, que la información es un activo que tiene un alto valor para las organizaciones y la pérdida de esta representa un costo incalculable, dado que representa la memoria institucional y el patrimonio documental producto de sus actividades, así mismo el activo de información sirve de soporte que muchas veces es producido desde una aplicación y/o medios tecnológicos puede servir como soporte de un proceso o en la mayoría de los casos para conservarse en el tiempo para la continuidad del negocio.

Es importante verificar que el aplicativo de software libre permita garantizar la confidencialidad, integridad y disponibilidad de la información, a partir de la aplicación de pruebas que permitan identificar las posibles causas de inseguridad,

y asimismo buscar los mecanismos de protección y seguridad de la información de los documentos electrónicos y digitales que se administren y gestionen en la herramienta.

Analizando y previendo que el aplicativo de software libre va a administrar toda la información producto de la gestión y trámite de las actividades de una entidad, es así, que se identifica una oportunidad para presentar, desarrollar, proponer un modelo de requisitos que debe cumplir un gestor documental, que cuente con los mecanismos de seguridad informática para una organización basado en la metodología OWASP para aplicaciones web.

1.2 FORMULACIÓN

¿Cómo garantizar la seguridad de un aplicativo de gestión documental de software libre en ambiente web, mediante definición de requisitos de seguridad informática fundamentado en OWASP para evitar fallos de seguridad y vulnerabilidades que puedan comprometer los documentos electrónicos de la organización?

2. JUSTIFICACIÓN

La seguridad informática de aplicaciones de software libre requiere ser estudiada para identificar los posibles riesgos, causas, problemas, amenazas y fallos de seguridad que en las herramientas de gestión documental se pueden presentar, pues estás administran y almacenan la producción documental que da cuenta de las actividades de una organización. Hoy día se habla de los Sistemas de Gestión Documentos Electrónicos de Archivos – SGDEA, según las diferentes iniciativas promulgadas por el Ministerio de Tecnologías de Información y las Comunicaciones – MINTIC mediante la Directiva Presidencial 004 de 2012 eficiencia administrativa y lineamientos de política cero papel promulgada por la Presidencia de la República y demás estrategias donde se busca que a partir del uso de las herramientas tecnológicas y medios electrónicos se optimice la gestión de la información.

Es por ello, que este proyecto busca definir los requisitos de seguridad que requiere una aplicación de acceso libre, con el fin de comprobar de forma rápida y eficiente a través del OWASP (Proyecto Abierto de Seguridad en Aplicaciones Web), las debilidades del sistema, mitigar los diferentes fallos y agujeros donde se presenta posibles ataques a los sistemas y la creación de código seguro para así documentar el proceso aplicado.

La necesidad de implementar mejores prácticas en materia de seguridad de la información y seguridad informática permite contar con aplicaciones de software libre en entornos web para la gestión de documentos electrónicos de archivo seguros en los cuales prevalezca la información producida, tramitada, gestionada y almacenada en una herramienta. Es decir, se pueda contar con los mecanismos necesarios y estrategias que permitan proteger, resguardar la memoria documental de una institución.

Por otra parte, resuelve aquellos fallos y agujeros de seguridad que surgen cada vez de que se filtra de manera inequívoca ataques a los sistemas u herramientas con los que cuenta una organización. El análisis y pruebas basado el modelo OWASP ayuda identificar los diferentes riesgos y así mitigarlos para además seleccionar de forma estratégica la aplicación de código abierto que mejor convenga para resguardar y administrar la información, y la optimización de esta a través de uso de medidas de seguridad informática que mejor le aplique.

A partir de la realización de pruebas de software abierto este será aplicado en dos herramientas de gestión documental, basado en las guías OWASP cuyo fin es realizar la comprobación de programas, de esta manera detectar las posibles vulnerabilidades. A partir de ello diseñar un modelo de requisitos de seguridad informática y generar conocimiento desde los controles de seguridad que deberían garantizar de forma confiable el uso y la administración de la información desde un aplicativo.

Como resultado final, este proyecto permitirá la identificación y descripción de las características de seguridad que debe cumplir un sistema para la gestión de documentos electrónicos y digitales, con el fin de que sean administrados de forma segura. Por consiguiente, la aplicación y uso de los fundamentos del OWASP (Proyecto de Seguridad de aplicaciones Web - *Open Web Application Security Project*) es proyecto de código abierto permite la realización de técnicas, métodos y pruebas de penetración.

3. OBJETIVOS DE PROYECTO

3.1 OBJETIVO GENERAL

Definir los requisitos de seguridad informática para un software libre de gestión documental, a partir de la aplicación de la metodología OWASP, con el fin de que se garantice de forma segura la producción, gestión, trámite y conservación de los documentos electrónicos y digitales.

3.2 OBJETIVOS ESPECÍFICOS

1. Documentar los conceptos de sistema de gestión de seguridad informática en la producción de documentos electrónicos y digitales generados en una organización.

2. Identificar las fallas de seguridad que tiene el software libre de gestión documental (ORFEO y OpenDocMan) en materia de seguridad informática.

3. Definir los requisitos de seguridad informática a partir del OWASP que debe tener un gestor documental, para la producción del documento electrónico y digital de forma segura.

4. MARCO DE REFERENCIAL

4.1 MARCO TEÓRICO

A continuación, se hace revisión de investigaciones acerca de las posturas teóricas planteadas que aportan al desarrollo de este proyecto. El sustento teórico se enmarca dentro del concepto de seguridad de aplicaciones web basados en OWASP las diferentes técnicas que se usan para la identificación de las ellas y ofrecer recomendaciones de seguridad.

Para realizar la definición de algunos aspectos en el proceso de la metodología OWASP y la revisión bibliográfica en el contexto investigativo se identificaron los siguientes temas a abordar: seguridad informática, seguridad en aplicaciones web, requisitos de seguridad, aplicaciones web, software y aplicaciones.

James P. Anderson para 1980 realizó los primeros escritos acerca de <<*Computer Security Threat Monitoring and Surveillance*>>, describe la importancia del comportamiento enfocado hacia la seguridad en materia de informática, y donde se menciona por primera vez ataque o vulnerabilidad protección de la infraestructura, la cual empieza a concientizar acerca de la importancia de la seguridad de la información y todo lo que está alrededor de ella.

Según un estudio realizado a la norma ISO/IEC 27001 Estrada, Alba y Martín define la seguridad informática – SI "como aquellas características y condiciones de sistemas de procesamientos de datos y su almacenamiento que permite garantizar la confidencialidad, integridad y disponibilidad"[1], por lo cual, aporta los pasos para la implantación de un sistema de gestión seguro.

Por lo tanto, la seguridad informática – SI, se especializa en la protección de la infraestructura computacional y todo lo que la relaciona, en este sentido, la seguridad del software cuyo fin es el uso de buenas prácticas sobre las aplicaciones seguras en una organización o entidad, a partir de la identificación de vulnerabilidades y fallas en los sistemas, es por ello que el estándar OWASP (Open Web Application Security Project) en su variado catálogo de guías emite herramientas que sirven para analizar y evaluarla seguridad en aplicaciones y así

[1] ESTRADA, ALBA, MARTÍN. Fundamentos para implementar y certificar un sistema de gestión de seguridad informática bajo la norma ISO/IEC 27001. Serie científica de la Universidad de las Ciencias Informáticas. 2012

de forma temprana detectar los posibles riesgos y vulnerabilidades del software. Según OWASP Top 10 – 2017, contiene los diez riesgos más críticos en Aplicaciones Web, está documentación sirve como modelo para la identificación de los requisitos.

En el artículo de la revista cubana de ciencias informáticas, se aborda el tema de *"Requisitos de Seguridad para las Aplicaciones Web"* por el autor Benítez Niño, teniendo en cuenta, el incremento de software que en la búsqueda de las entidades por mejorar sus procesos y procedimientos incorporando el uso de las herramientas tecnológicas, presenta una oportunidad de mejora, pues el aseguramiento de la información y de los sistemas es importante en una organización ya que almacena activos de información para darle un adecuado tratamiento, protección, y así mitigar los riesgos asociados al uso y acceso de las aplicaciones tecnológicas que hoy día se encuentran expuestas y son objeto de ataques informáticos.

En la investigación de la Universidad Católica desarrolla por los autores Rodríguez Rafael y Sánchez Andrés, se presenta el tema "Desarrollo de un modelo para calcular el nivel de seguridad en sitios web según el marco de referencia OWASP" teniendo en cuenta que un software no es 100% seguro, por lo cual se entra a evaluar y clasificar las vulnerabilidades de un sistema a partir de modelos y metodologías en materia de seguridad informática, para así clasificar a partir de las vulnerabilidades presentadas en una aplicación libre y darle una ponderación.

Teniendo en cuenta la aparición de sitios web, aplicaciones web y servicios web, en el marco de la WWW (World Wide Web) a través de esta se dio el intercambio de información y fue adoptada como un medio de negocios y servicios, por lo cual, diversas organizaciones la utilizan como canal u medio de información, es por ello que estudios dados en materia de seguridad en aplicaciones web permiten realizar la detención temprana de fallas de seguridad, la definición de requisitos y aplicación de pruebas según la Guía de Testing de OWASP que orienta de forma práctica para proteger un software que han sido realizados desde 2001 hasta la fecha, ya que cada ataque informático va evolucionado en el tiempo.

4.2 MARCO CONCEPTUAL

A continuación, se aborda los diferentes términos que enmarca el tema de seguridad informática y de la información y demás teoría que gira en torno al tema del Sistema de Gestión de Seguridad Informática (SGSI), como también se aborda el tema principal que corresponde a la metodología OWASP.

4.2.1 Auditoría de Seguridad Informática

Es el estudio que comprende el análisis, evaluación de los sistemas, este se lleva a cabo por profesionales, con el objetivo de identificar, enumerar, describir las vulnerabilidades que se pueden presentar en un sistema en la organización, por medio de las redes, los servidores, los computadores. A partir de esta se aplican pruebas basados en estándares y modelos que permiten de forma metodológica describir requisitos y características que debe cumplir un aplicativo en cuanto a seguridad informática.

La auditoría de seguridad permite identificar interna y externamente en la organización las posibles amenazas a las que está expuesto el sistema y la información, por lo cual busca proteger los activos de la información mediante mecanismos y técnicas de protección, control y medidas de seguridad.[2]

La ISO 27002 estándar de la Comisión Electrotécnica (CEI) en inglés IEC (International Electrotechnical Commission) emitió un código de buenas prácticas para seguridad de la información, directriz de auditoría de seguridad la cual define requisitos para la auditoría, por otra parte, el modelo COBIT, es un conjunto de directrices y buenas prácticas que busca garantizar la seguridad de los sistemas.

A continuación, existes diferentes tipos de auditorías cuyo servicio varía de acuerdo con la necesidad; auditoría de seguridad interna, se realiza análisis a nivel de seguridad de la red, redes locales y equipos a nivel interno. Auditoría de seguridad perimetral, se realiza estudio en el perímetro local o corporativo, para identificar la seguridad que ofrecen enlaces externos. Test de intrusión, este tipo de test realiza pruebas para identificar el acceso a la información por medio de la intrusión, en algunos casos se utiliza hacker ético. Análisis forense, este estudio a partir de

[2] MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES – MINTIC. Guía de auditoria. Seguridad y privacidad de la información. Bogotá, Colombia: 2016.

incidentes busca reconstruir la escena del crimen informático, y como se perpetra a un sistema, y auditoría de páginas web, conocido como análisis externo por medio de la web, a través de inyección SQL.

Por lo cual, el tipo de auditoría que se realizará para el desarrollo de este trabajo es la auditoría de seguridad interna.

4.2.2 Seguridad en el acceso a la información

Es importante que los activos de la información de una organización estén protegidos, por los diferentes tipos de riesgos que buscan perpetrar y vulnerar la seguridad de un sistema, buscando adquirir y acceder a la información de una institución de forma fraudulenta, es por ello por lo que se debe implementar herramientas y el uso de modelos y estándares que generan buenas prácticas para la protección de la información basados en OWASP (*Open Web Application Security Project*).

4.2.3 Acceso a la información

El acceso a la información busca que toda persona pueda tener conocimiento de la información que se produce en una organización pública o privada, siempre y cuando no existan restricciones o excepciones a esta. El acceso a la información es un derecho fundamental, consagrado en la Constitución Política de Colombia de 1999 en los artículos 15 y 74, por lo cual esta información responderse de forma eficaz, eficiente y efectiva, de manera adecuada, veraz, oportuna y accesible a las solicitudes de acceso, que a su vez conlleva a la obligación de producir o capturar la información pública, por lo cual se deben realizar e implementar procesos que permitan garantizar la disponibilidad de la información en el tiempo real.[3]

- Confidencialidad

La norma ISO/IEC 27000 define la confidencialidad, como propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos autorizados.[4] Lo cual quiere decir, que no cualquiera puede acceder a

[3] CONGRESO DE COLOMBIA. Ley 1437 de 2011 [en línea] Bogotá, 2011. Disponible en Internet: <http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/ley143718012011.pdf>.
[4] ISO. ISO/IEC: 27000 Seguridad de la información. Bogotá, 2013.

información de carácter privado o que no cuente con los privilegios de acceder a esta.

- Integridad

Propiedad de la información relativa a su exactitud y completitud[5], significa la totalidad de la información, que esta no se encontrara en partes diferentes, para el caso de la tecnología se identifica como la totalidad de los datos se encontraran almacenados en un solo sitio garantizando que la información no sea modificable, alterada, o falsificada, caso por el cual se da la seguridad de la información para evitar la vulneración y riesgos entorno a la información que produce una organización y que se da bajo un sistema.

- Disponibilidad

Propiedad de la información de ser accesible y utilizable cuando lo requiera una entidad autorizada[6], por lo cual la seguridad informática y de la información, busca que se garantice el acceso a la información siempre y cuando no sea afectada, alterada o sufra perdida de esta, asimismo se cuente con mecanismos y técnicas de seguridad en una herramienta tecnológica que permita el acceso de forma controlada, la disposición de la información y integridad de esta.

4.2.4 Seguridad Informática

Seguridad informática busca proteger toda la parte que hace referencia a los equipos de cómputo de una organización, correspondientes a los servidores, redes, router, cableado, firewall, software de los equipos, los sistemas operativos, DNI, una buena parte que busca la protección de los sistemas como tal.

4.2.5 Seguridad de la información

La información, se da a partir de los activos de información en la cual se debe garantizar que por medio de la protección de los equipos y los diferentes canales de comunicación no se pueda acceder de forma ilícita a la información que produce una organización.

[5] ISO. ISO/IEC: 27000. Ibíd.
[6] ISO. ISO/IEC: 27000. Ibíd.

4.2.6 OWASP (Proyecto de Seguridad de aplicaciones Web - *Open Web Application Security Project*)

Es un proyecto que busca realizar pruebas de seguridad en aplicaciones web para identificar las posibles vulnerabilidades que presenta un aplicativo de este tipo, a partir de la realización de pruebas de intrusión cuyo objetivo es diagnosticar y resolver problemas de seguridad. Esta metodología de código abierto permite determinar y combatir las causas que hacen inseguro un software, como también realizar y comprobar de seguridad a partir de las características de un aplicativo, para que justamente desarrollar requisitos que garanticen la protección de la información.

4.2.7 OWASP Top 10

OWASP Top 10 es un documento que identifica la categorización de las vulnerabilidades que se presentan en cuanta, a seguridad de la información y informática, presentando los riesgos más comunes que se presentan en las aplicaciones web, permitiendo la revisión y aplicación de pruebas de seguridad en el software, lo cual ayuda y propone de una forma correcta verificar el aplicativo.

De acuerdo con el modelo OWAPS, se describe el TOP 10 que indica los riesgos más críticos en materia de seguridad en aplicaciones, donde se asocia a la frecuencia de la debilidad y se detalla los controles de seguridad.

A1:2017 – Inyección: ataque por inyección se presenta con código SQL, LDAP, código SSI (Sever-Side-Include), Xpath, este ataque permite inyectar instrucciones de forma maliciosa para la manipulación de bases de datos donde se encuentra los datos almacenados.

A2:2017 – Perdida de autenticación: vulnerabilidad relacionada con el usuario y contraseñas, cuentas administrativas, se pueden presentar ataques de fuerza bruta o diccionarios con el fin de explorar y atacar la identidad de la herramienta. este tipo de vulnerabilidad permite a un atacante suplantar la identidad de un usuario,

preferiblemente la administración lo cual permite sabotear los controles de autorización y registro de aplicación.[7]

A3:2017 – Exposición de datos sensibles: este tipo riesgos requiere de método de control eficiente y protección adicional con el objetivo de proteger la información sensible y evitar el robo de las contraseñas, se requiere cifrado de almacenamiento y tránsito que proteja las APIS y la aplicación web.

A4:2017 – Entidades Externas XML (XXE): "Las entidades externas pueden utilizarse para revelar archivos internos mediante la URI o archivos internos en servidores no actualizados, escanear puertos de la LAN, ejecutar código de forma remota y realizar ataques de denegación de servicio (DoS)."[8]

A5:2017 – Perdida de control de acceso: hace referencia a la administración de las aplicaciones por lo tanta las restricciones que poseen los usuarios autenticados pueden hacer que se explore de manera malintencionada y de forma no autorizada las funciones y datos de la herramienta, por los ataques están dados a cambio de derechos de acceso, permisos, modificaciones de datos entre otros.

A6:2017 – Configuración de seguridad incorrecta: este tipo de vulnerabilidad hace referencia a la actualización y configuración de aplicaciones, marcos de trabajo, servicio de aplicación, servidor web, base de datos, y plataforma[9].

A7:2017 – Secuencia de comandos de sitios cruzados (XSS) – *Cross-Site Scripting,* es un tipo de agujero de seguridad, este tipo de vulnerabilidad se presenta en sitios web y aplicaciones, funciona con un tipo de secuencia de comandos en sitios cruzados.[10] Se da en sitios que aparentemente son seguros y roban la identidad), donde el usuario proporciona información lo que sucede a continuación, es que toma la información de la víctima sino que se puede tomar el control de la aplicación web, un ejemplo claro son las páginas web de bancos, permitiendo así que el atacante tome control de las cuentas bancarias y realizar transacciones.

A8:2017 – Deserialización insegura: esto sucede cuando la aplicación es atacada a través de la recepción de objetos seriados que están dañados, los cuales pueden

[7] S2GRUPO. OWAPS TOP 10 (III): Pérdida de autenticación y gestión de sesiones. <http://www.securityartwork.es/2010/03/24/owasp-top-10-iii-perdida-de-autenticacion-y-gestion-de-sesiones/>
[8] OWASP. Top 10 2017 – Riesgos de Seguridad en Aplicaciones Web. p. 6.
[9] Ibid., p. 6.
[10] AVAST. Secuencia de comandos en sitios cruzados (XSS). Consultado en: <http://www.zurichmaratonsevilla.es/zm2-recomendaciones>

ser manipulados para penetrar el sistema mediante inyecciones, privilegios o ejecución remota.

A9:2017 – Componentes vulnerables conocidas: esto sucede cuando diferentes componentes como bibliotecas, módulos ejecutan privilegios en la aplicación, lo cual puede debilitar la defensa y filtrar ataques.

A10:2017 – Registro y monitores insuficientes: cuando no se ejecutan las debidas acciones de monitoreo, control y seguimiento a la aplicación esto puede permitir que el atacante manipule el sistema para extraer, destruir y atacar la herramienta, estas debilidades no detectadas a tiempo son un hueco de seguridad que filtra las vulnerabilidades al no mitigarse en el momento adecuado.

4.2.8 Técnicas de pruebas de seguridad

Define cuatro técnicas principales para llevar a cabo en la seguridad de aplicaciones Web: inspecciones manuales y revisiones, modelamiento de amenazas, pruebas de penetración y revisión de código.[11]

4.2.9 Aplicación web

Una aplicación web, hace referencia a un software que es almacenado total o parcialmente en un servidor web, y cuyo lenguaje es codificado con la WWW (world Wide Web), la forma de acceder es mediante un navegador, para su utilización se debe valer del protocolo HTTP (HyperText Transfer Protocol). Las principales características son: que se puede acceder desde cualquier lugar, plataforma o navegador, la información es pública y puede ser consultada por cualquier usuario, y finalmente la información contenida en un sitio web se actualiza instantáneamente. Siempre y cuando esté conectado a una red que permita el acceso a internet o intranet.

4.2.10 Ingeniería de Software

“La Ingeniería del software, la cual es la encargada de estudiar los principios y metodologías para el desarrollo y mantenimiento de sistemas software, define

[11] OWASP Foundation. Testing guide v3. Consultado en: <https://www.owasp.org/images/5/56/OWASP_Testing_Guide_v3.pdf>

aplicación web como el conjunto de herramientas que los usuarios pueden usar para acceder a un servidor web a través de Internet o Intranet mediante el uso de navegadores web"[12]. Es decir, una la aplicación web se conoce como ingeniería de software.

4.2.11 Software libre

Se conoce como *free software* hace referencia a libertad de uso, significa que debe los programas deben cumplir y tener cuatro criterios para considerarse libre; ejecutar el programa con cualquier propósito, estudiar como funciona, redistribuir copias, y modificar y mejorar el software. Este no genera costos y es permisible en el sentido que el usuario (individuo o empresa) controle el programa, es así como el programa puede ser adaptado, modificado y/o personalizado para uso propio

4.2.12 Software de Código Abierto

OSS – *Open Source Software es* el software cuyo código fuente y otros derechos que normalmente son exclusivos para quienes poseen los derechos de autor, son publicados bajo una licencia de código abierto o forman parte del dominio público.[13] El propietario del software permite distribuir, utilizar, cambiar y modificar a los usuarios, este se puede usar de forma colaborativa.

4.2.13 Gestor Documental

Se define como un software de gestión documental que permite la administración de la información a partir de la conservación, el tratamiento y el manejo de los documentos electrónicos y digitales, el cual contiene características para la gestión de los documentos producto de las actividades de una organización, desde la planificación hasta disposición final.

---

[12] Cardador Cabello, Antonio Luis. Implantación de aplicaciones web en entornos internet, intranet y extranet (MF0493_3). Madrid, ESPAÑA: IC Editorial, 2014.

[13] Laurent, Andrew M. Understanding Open Source and Free Software Licensing. Consultado en linea: <https://books.google.com.co/books?id=04jG7TTLujoC&pg=PA4&redir_esc=y#v=onepage&q&f=false> O'Reilly Media, 2008

4.3. MARCO LEGAL

En cuanto al tema de seguridad de la información y seguridad informática se abordan diferentes normas, estándares y modelos que permiten mantener bajo el marco legal para la protección de la información y de los sistemas, a continuación, se enunciaran los lineamientos nacionales e internacionales referentes al tema.

De acuerdo con la normatividad vigente, se presentan la normatividad nacional que aplica al desarrollo del trabajo en materia de protección y seguridad de información.

- Ley 527 de 1999. Reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales. Teniendo en cuenta el intercambio electrónico de datos (EDI), y de información se da entre aplicaciones web, cuyo fin es conservar la integridad de la información y el uso de firma digital o electrónicas para la emisión de documentos y certificaciones, estampado cronológico como medio de autenticación para la validez de documentos electrónicos.[14] Para el desarrollo del proyecto da origen a la creación, producción y trámite de los documentos electrónicos que son generados a través de aplicativos, brindado soporte y lineamientos que soporten el intercambio de información y que estos brinden protección para garantizar de manera segura su conservación e inalterabilidad en el tiempo, así como le integridad de los expedientes y el no repudio de estos. Referente al marco de la gestión documental e incorporación de sistemas de gestión de documentos electrónicos.

- Ley 1273 de 2009. Protección de la información y de los datos que se preservan en los sistemas que utilicen tecnologías de información, esta ley informática tiene como objetivo describir los principales delitos que se presentan en los diferentes medios tecnológicos, donde se preserva, almacena o transfiere la información.[15] Esta norma apunta a la descripción de posibles delitos que se presentan en un sistema que almacena información de una organización.

- Ley 1712 de 2014. Ley de Transparencia y del Derecho de Acceso a la Información Pública.[16] Trata acerca de la disposición de la información a través de los diferentes medios como la página web de una entidad, como derecho fundamental de acceso a la información y la clasificación como pública, reservada y clasificada a la ciudadanía. Por lo cual, es necesario

[14] CONGREGO DE LA REPUBLICA. Ley 527 de 1999. Bogotá, Colombia: 1999.
[15] CONGREGO DE LA REPUBLICA. Ley 1273 de 2009. Bogotá, Colombia: 2009.
[16] CONGREGO DE LA REPUBLICA. Ley 1712 de 2014. Bogotá, Colombia. 2014.

contar con diferentes mecanismos de seguridad de la información para los entornos web y asimismo que se garantice que la información contenida allí sea integra.

- Decreto reglamentario 2609 de 2012. AGN. Compilado en el Decreto 1080 de 2015, artículo 2.8.2.6.1 Sistema de Gestión Documental y 2.8.2.6.2 literal c) Seguridad. Los sistemas de gestión documental deben mantener la información administrativa en un entorno seguro. La incorporación de aplicaciones tecnológicas para la administración de los documentos a partir del sistema de gestión de documentos y su alineación con los instrumentos archivísticos para lograr una eficaz y eficiente organización de la información que produce la entidad desde el marco normativo del AGN.

- Decreto 19 de 2012. Ley Antitrámites, suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública, Artículo 38 numeral 2) *Facilitar el acceso a la información y ejecución de los trámites y procedimientos administrativos por medios electrónicos, creando las condiciones de confianza en el uso de los mismos, y literal 3) Contribuir a la mejora del funcionamiento interno de las entidades públicas que cumplan una función administrativa, incrementando la eficacia y la eficiencia de las mismas mediante el uso de las tecnologías de la información, cumpliendo con los atributos de seguridad jurídica propios de la comunicación electrónica*.[17] Su aplicación dada en los sistemas de gestión que deberán contar con las características propias de seguridad de la información para que su uso y aplicación sea segura.

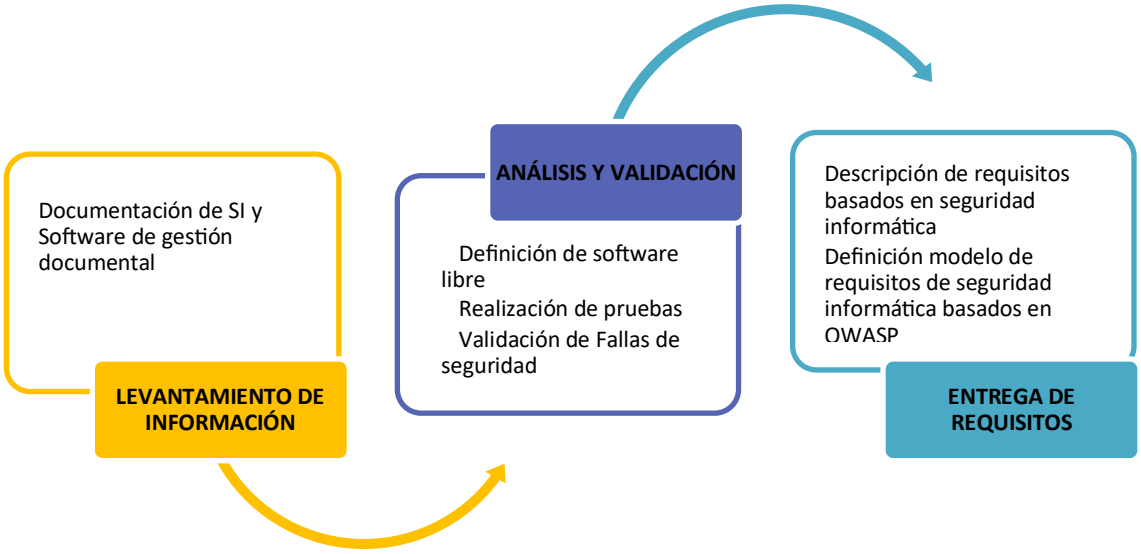
- Directiva Presidencial 03 de 2011. Eficiencia administrativa y lineamientos de la política cero papel en la Administración Pública. Artículo 5 literal 2. Avanzar en la producción de documentos públicos y actos administrativos por medios electrónicos, asegurando la autenticidad, integridad y disponibilidad de estos, así como la integración de expedientes electrónicos. Esta norma pone en funcionamiento en las entidades públicas los sistemas tecnológicos que permitan agilizar sus procesos a través de herramientas. La implementación sistemas de gestión para la producción documental a partir del uso de tecnologías y a su vez que el este cuente con la triada de la seguridad de la información ya que la documentación contenida es sensible de ataques informáticos.

[17] DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Decreto 019 de 2012. Bogotá, Colombia: 2012. Pág.12.

4.4. METODOLOGÍA DEL PROYECTO

Se han definido las siguientes etapas para la descripción y el desarrollo del trabajo, en la figura 1 se representan de las fases:

Figura 1.Descripción etapas para el desarrollo del trabajo.



Fuente: El autor

4.4.1. Levantamiento de información y documentación

En esta etapa se realizará el levantamiento de información para identificar y definir los conceptos de sistema de gestión de seguridad informática – SI, sistema de gestión de documentos electrónicos de archivo – SGDEA de una aplicación web libre y todos los temas que giran en torno a la producción de documentos electrónicos y digitales que generan una organización, a partir investigación e información encontrada se documentará el resultado.

4.4.2. Análisis y validación de fallas

Para el desarrollo de esta etapa inicialmente se selecciona las aplicaciones de software libre a los cuales se les aplicara la metodología OWASP, cuyo fin es describir cada una de las aplicaciones web enfocadas en la seguridad informática.

Una vez identificadas las aplicaciones se describirán las pruebas a aplicar y recolección de información, para así determinar y describir los tipos de ataques que se presentan en cada aplicativo que lo hace vulnerable, con el fin de documentar paso a paso las pruebas de penetración realizadas.

A partir de ello, analizar y validar el cumplimiento de los requisitos del software libre de gestión documental para que sea seguro y garantizar la protección de la información que este administra para una organización.

4.4.3. Entrega de los resultados de los requisitos

Como resultado del análisis de las pruebas de penetración y la aplicación de la metodología OWASP al software libre de gestión documental, en esta etapa se propondrán recomendaciones basados en OWASP, tales como:

- Técnicas y mecanismos de seguridad de la información
- Descripción de requisitos basados en seguridad informática
- Documento de cómo se aplica el Top ten OWASP

El modelo de propuesta a partir de la aplicación y validación de pruebas tiene como fin para el desarrollo de este trabajo contribuir en la seguridad informática de aplicaciones web libre para la gestión de documentos electrónicos.

5. SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA BASADO EN DOCUMENTOS ELECTRÓNICOS Y DIGITALES

Se hace necesario revisar la documentación acerca de la descripción y caracterización del concepto del Sistema de Gestión de Seguridad Informática (SGSI), de los casos aplicables para la administración de un aplicativo de documentos electrónicos y digitales en una organización que son necesarios para dar cumplimiento de software libre en ambiente web.

Para la definición del SGSI se deben explorar los principios de la seguridad informática y seguridad de la información, y la relación que tienen con la serie de normas ISO. En 1995 aparece por primera vez en el *British Standards Institution* – BSI la publicación de la norma BS 7799, como Sistema de Gestión de Seguridad de la Información – (*Information Security Management System – ISMS*), posteriormente en 1998 se publica la norma BS 7799-2 que da especificaciones para los sistemas de gestión de la seguridad de la información, cuyo objetivo es el de proporcionar a cualquier empresa un conjunto de buenas prácticas para la gestión de la seguridad de su información quedando así (BS7799-1:1999 y BS7799-2:1999), en 2000 fueron adaptadas bajo la ISO/IEC 17799 como norma internacional aprobada por la Organización Internacional de Estandarización – ISO y por la Comisión Electrónica Internacional – IEC.

En el 2000 se publico la ISO/IEC 17799:2002 Código de buenas prácticas para la gestión de la seguridad de la información, luego se adopta en España como UNE (UNE 17799). La UNE-ISO/IEC 17799 establece 10 dominios de control y de los cuales se derivan 36 objetivos de control y 127 controles, que cubren la Gestión de Seguridad de la Información:

- Política de seguridad
- Aspectos organizativos para la seguridad
- Clasificación y control de activos
- Seguridad ligada al personal
- Seguridad física y del entorno
- Gestión de comunicaciones y operaciones
- Control de acceso
- Desarrollo y mantenimiento de sistemas
- Gestión de continuidad del negocio

- Conformación con la legislación[18]

Norma UNE-ISO/IEC 17799:2005 para la segunda versión se desarrollaron 11 dominios de control, esta incluye 39 objetivos de control y 133 controles muy parecidos a los anteriormente nombrados.

- Política de seguridad
- Aspectos organizativos para la seguridad de la información
- Gestión de activos
- Seguridad de los recursos humanos
- Seguridad física y ambiental
- Gestión de comunicaciones y operaciones
- Control de acceso
- Adquisición, desarrollo y mantenimiento de los sistemas de información
- Gestión de incidentes de seguridad de la información
- Gestión de continuidad del negocio
- Cumplimiento

Posteriormente la ISO 17799:2005 se renombro como la ISO 27002 equivalente de la BS 7799 segunda parte, y el estándar BS 7799-2 queda sustituido aprobado con la publicación del estándar internacional ISO/IEC 27001:2005 en octubre de este mismo año, bajo la serie 27000 reservado para los estándares de Sistemas de Gestión de Seguridad de la Información – SGSI sobre tecnología de la información, técnicas de seguridad, vocabulario y glosario de términos, para la operación e implementación de esta en los sistemas de las organizaciones.

La "ISO/IEC 17799 fue preparado por el Comité Técnico Conjunto – JTC (ISO/IEC JTC 1, tecnología de la información, Subcomité SC 27, técnicas de seguridad TI"[19], por lo cual la "familia incluye Estándares Internacionales sobre requerimientos gestión del riesgo, métrica y medición, y el lineamiento de implementación del sistema de gestión de seguridad de la información."[20]

En el marco de referencia de la familia de la serie ISO/IEC: 27000 según muestra la tabla 1 se encuentran descritas las normas de los SGSI que para efectos de un

[18] ORGANIZACIÓN INTERNACIONAL DE ESTANDARIZACIÓN. ISO/IEC 17799:2002. Tecnología de la información. Código de buenas prácticas para la Gestión de la Seguridad de la Información. 2002.
[19] ORGANIZACIÓN INTERNACIONAL DE ESTANDARIZACIÓN. ISO/IEC 17799-2:2005. Tecnología de la información, Técnicas de seguridad, Código para la práctica de la gestión de la información. 2005. pág.7
[20] Ibíd., p. 8.

SGDE nombran algunas de las normas relevantes que la constituyen hacia el contenido de las mejores prácticas recomendadas en seguridad de la información y posteriormente otros estándares internacionales enmarcadas en los sistemas de gestión de documentos electrónicos de archivo.

Tabla 1. Estándares ISO/IEC aplicables al desarrollo del trabajo propuesto.

Norma	Título
ISO/IEC 27000	Términos y definiciones, vocabulario de la familia 27000 correspondiente al SGSI.
SO/IEC 27001	Requisitos de implantación del modelo SGSI
ISO/IEC 27002	Buenas prácticas para controles de la seguridad de la información
ISO/IEC 27003	Guía de implementación del sistema de gestión de la seguridad de la información
ISO/IEC 27004	Medición de seguridad de la información
ISO/IEC 27005	Gestión de riesgos de seguridad de la información
ISO/IEC 27007	Directrices para auditoría en Sistemas de Gestión de la Seguridad de la Información
ISO/IEC 27014	Gobernanza de la seguridad de la información
ISO/IEC 27035	Seguridad de la información – Técnicas de Seguridad – Gestión de Incidentes de Seguridad
Fuente	El autor. Norma ISO 27000 y título de las normas derivadas

En este sentido, la ISO/IEC 27000 especifica los requisitos necesarios para establecer, implementar, mantener y mejorar un SGSI, cuyo fin es ser certificable e implementado en las organizaciones, para proporcionar las mejores prácticas de gestión de la seguridad de la información, teniendo en cuenta todo el desarrollo que se ha generado desde 2006 hasta su última edición a la fecha.

Para el desarrollo del documento se realiza un breve resumen y descripción de las distintas normas de seguridad informática que componen la serie ISO 27000 citadas en la Tabla No.1 las cuales se tomaron en cuenta y que aportan para el desarrollo este:

- ISO/IEC 27000 De forma muy general tiene la visión de la serie de normas que la componen, contiene el alcance de actuación y propósito de la seguridad informática, desarrollando las definiciones, vocabulario y terminología del SGSI e introducción de este para los sistemas de gestión y el cumplimiento e implantación.

- ISO/IEC 27001 contiene los requisitos de la implantación del SGSI en las organizaciones, promoviendo la gestión de riesgos y la mejora continua en los procesos. La norma que dio origen BS 7799-2:2002 fue anulada dándole paso a esta, con certificación de auditores y controles que se desarrollan en la siguiente norma.

- ISO/IEC 27002 Código de buenas prácticas para la gestión de seguridad de la información, previo de la BS 7799-1 y la ISO/IEC 17799, es una guía que describe las buenas prácticas de control y controles en cuanto a seguridad de la información, la cual fue actualizada en el 2013 contiene "14 dominios, 35 objetivos de control y 114 controles"[21].

- ISO/IEC 27003 Directrices para la implementación de un SGSI, bajo el ciclo de Deming con las siglas PDCA (*Plan, Do, Check, Act* – Planificar, Hacer, Verificar, Actuar). Anexo B de la norma BS 7799-2. Se basa en el diseño e implementación desde el inicio hasta la puesta en marca de planes de implementación, para la aprobación de la SGSI, pero esta no es certificable.

- ISO/IEC 27004 Es la guía que utiliza métricas para el desarrollo y técnica de medidas aplicables para al SGSI, proporciona recomendaciones de quién, cuándo y cómo se debe realizar la medición, esta no es certificable.

- ISO/IEC 27005 Proporciona directrices para la gestión de riesgos, esta norma proporciona recomendaciones y lineamientos de métodos y técnicas de evaluación de riesgos de Seguridad en la Información.

- ISO/IEC 27007 Es una guía para proceder a la auditoría de un SGSI, su última actualización fue 2020 esta norma es complemento de la ISO 19011[*].

- ISO/IEC 27014 Es una guía que brinda ideas y principios para el gobierno de la seguridad de la información para todo tipo de entidades, permite dirigir, evaluar, monitorear, comunicar y asegurar las actividades relacionadas con la seguridad de la información que se desarrolla en una organización.

- ISO/IEC 27035 Es una guía que proporciona principios sobre la gestión de incidentes y técnicas de seguridad, por lo cual se enfoca en la detección, reporte y evaluación de incidentes de seguridad y sus vulnerabilidades.

[21]ISO/IEC 27002:2013. En línea << http://www.iso27000.es/assets/files/ControlesISO27002-2013.pdf >>

[*] ISO 19011 esta norma proporciona orientación sobre la gestión de un programa de auditoría, sobre la planificación y la realización de un sistema de gestión de la calidad, así como la orientación sobre la evaluación de la competencia de los individuos que participan en el proceso de auditoría. ISO 19011:2018 Directrices para la auditoria de los sistemas de gestión.

En el marco de la ISO 27000 y la ramificación de sus normas desde la ISO/IEC 27001 a la 27103 contiene cada una especificaciones técnicas con el fin de abordar en materia de seguridad de la información los aspectos de articulación, acción y el contexto de la información donde se desarrolla cada uno de los sistemas como sectores y ámbitos que se han presentado, por lo cual, estas guías son el paso a paso para el establecimiento, monitorización, mantenimiento, auditoría, gestión de riesgos, requisitos, prevención, orientación, directrices y mejoramiento de un SGSI, para así mitigar y prevenir e identificar aquellos aspectos a partir del ciclo PHVA (planear, hacer, verificar y actuar).

5.1 SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN

Para la definición de un sistema gestión de seguridad de la información, se debe contextualizar acerca de ¿qué es Seguridad de la información? es el conjunto de medidas de prevención y protección de la información de amenazas para poder asegurar los datos que produce y usa una organización.

Tomando como iniciativa la norma ISO/IEC 27000 define el Sistema de Gestión de la Seguridad de la Información – SGSI como "el conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua"[22].

Por otra parte, la ISO 27000 menciona al Sistema de Gestión de Seguridad de la Información como el conjunto de medidas de la preservación de su confidencialidad, integridad y disponibilidad[23], así como los sistemas integrados en una organización y un sistema de gestión de seguridad de la información en inglés <<*Information Security Management System – ISMS*>>, es el conjunto de políticas de administración de la información, el objetivo principal es clasificar cual es la información que se requiere protección.

[22] ISO/IEC 27000. Glosario de términos
[23] NORMA TÉCNICA COLOMBIANA. ISO. NTC-ISO/IEC: 27001 Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos. Bogotá, 2006.

La información es considerada un activo que tiene un valor y requiere de la protección adecuada, la norma lo define como “cualquier cosa que tiene valor para la organización”[24] en este sentido, es un componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la información. Los activos se dividen en varios tipos, pero en este caso se concentran en dos tipos, activos de información y activos de servicios prestados, están en las dependencias de una organización, se dice que dependen de la estructura de una entidad.

En seguridad informática, busca mitigar las amenazas y las vulnerabilidades que se puedan presentan en una organización y que los riesgos sean materializados por lo cual, se realiza evaluación de riesgos, con el fin de identificar y analizar las posibles consecuencias y probabilidad de ocurrencia, asimismo la priorización de los riesgos en atención de niveles.

Una amenaza consiste en identificar que puede afectar a cada activo que tiene la organización y asimismo una vez identificado los activos, se debe identificar que tipo de amenaza se presenta y esta como afecta, cuantificando el nivel de riesgo.

Se denomina vulnerabilidad a toda debilidad que puede ser aprovechada por una amenaza, más detalladamente a las debilidades de los activos o de sus medidas de protección que facilitan el éxito de una amenaza potencial.

Una amenaza va acompañada de una vulnerabilidad la cual puede afectar la seguridad de la información, es allí donde se puede presentar y materializar un riesgo si no se cuenta con un Sistema de Gestión de Seguridad de la Información, el cual se encarga de:

- Realizar análisis aspectos internos y externos de la organización.
- Identificar las partes interesadas
- Analizar de interfaces y dependencias, para así identificar todos los aspectos bajo control.
- Definir una política de seguridad de la información en función de las características del negocio.
- Establecer y seleccionar los controles necesarios para el tratamiento de los riesgos
- Realización de auditorías internas al SGSI de forma planificada.

[24] Ibíd., p. 2.

- Revisar los recursos tecnológicos que se tienen y su infraestructura
- Definición de un plan de tratamiento de riegos o esquema de mejora
- No conformidades y acciones correctivas
- Declaración de aplicabilidad <<*Statement of Applicability – SOA*>>
- Ejecutar procedimientos de SGSI

El SGSI busca el uso e implementación de buenas prácticas de seguridad a partir de la aplicación de la ISO 27001 de 2013. Lo cual, se da desde que se realiza el levantamiento de información para así definir ciertos requisitos necesarios en una organización para garantizar la protección de la información y como es una actividad que necesita de mejora continua el seguimiento y control la ejecución de procedimientos y controles de monitorización para verificar el cumplimiento de la planificación, el funcionamiento y se requiere la actualización de los planes.

La seguridad informática es un actividad dinámica que requiere de una constante medición y actualización de los procesos, e implantación de mejoras, pues así como en el día a día existen nuevos sistemas informáticos asimismo se presentan diversas formas de atacar y afectar una aplicación, por lo cual, es una actividad constante que debe auditándose y dando el tratamiento adecuado a los riesgos, para mitigar e ir implementando nuevas y mejores prácticas, según las necesidades de la organización.

Tomando en cuenta, que el SGSI va de la mano de toda la gestión de la organización y demás marco normativo que garantice la protección de la información hacia las herramientas tecnológicas se toma en cuenta la norma ISO/IEC 15408, la cual está basada algunos aspectos de seguridad del Proyecto Abierto de Seguridad de Aplicaciones Web – OWASP.

La ISO/IEC 15408 *Common Crieria* – CC, criterios comunes de seguridad, donde se desarrollan 4 criterios básicos: Perfiles de protección, objetos de seguridad, objetos de evaluación y niveles de evaluación de seguridad.

Tabla 2. ISO/IEC 15408 descripción de conceptos Common Criteria – CC

Criterios		Descripción
Perfiles de Protección	PP	Conjunto de requisitos de seguridad, donde se identifica una serie de necesidades para el consumidor.
Objeto de Evaluación	TOE	Identifica el modelo de requisitos en el Objeto de Seguridad (ST) y evalúa determinado los recurso y dispositivos que utiliza implementados en el sistema o entorno que se esta trabajando. Aplica Niveles de confianza, que van desde verificaciones del EAL1 al EAL7.
Objeto de Seguridad	ST	Este identifica conjunto de requisitos de seguridad donde se identifica la aplicación o sistema, basados en la implementación
Nivel de Evaluación de Seguridad	EAL	Conjunto de requisitos que evalúa el nivel de seguridad y confianza de un sistema.
Fuente	Norma ISO/EIC 15408:	

5.2 SISTEMA DE GESTIÓN DE DOCUMENTOS ELECTRÓNICOS

La producción documental es la memoria de una institución, da cuenta de sus actividades y funciones en el marco de su razón social, se da a partir de la creación de los documentos físicos como electrónicos, en este sentido, existen diferentes prácticas y formas para gestionar los documentos como sistemas de gestión, los cuales se han vuelto una herramienta fundamental para el acceso, consulta, gestión, tramite, optimización y disponibilidad de la información.

La gestión documental es el conjunto de procesos y procedimientos enfocados en la administración de la información que se produce en una organización, con el fin de poner esta a disposición de los usuarios tanto internos como externos de forma accesible y efectiva, esta debe estar alineada a ciertas políticas y lineamientos que garanticen su adecuada gestión como: cuadro de clasificación documental – CCD, tabla de retención documental – TRD, tabla de valoración documental – TVD, tabla de control de acceso – TCA, programa de gestión documental – PGD, plan institucional de archivos – PINAR, inventarios documentales, modelo de requisitos para la gestión de documentos electrónicos, bancos terminológicos, y los mapas de

procesos, flujos documentales[25] y la descripción de las funciones de las unidades administrativas de la entidad, entre otros.

Existen diversos mecanismos para gestionar la producción de los documentos como los sistemas y aplicaciones desde donde se originan, y a su vez estos deben garantizar la administración, el almacenamiento y gestión de la información de forma digital y electrónica, por lo cual, también se requiere la conservación y preservación de los documentos digitales a largo plazo en el sistema gestión que garantice su trazabilidad, perdurabilidad en el tiempo y la seguridad de la información.

Un sistema de gestión de documentos - SGD o en ingles *document management system – DMS* es el programa que garantiza la organización de los documentos tanto físicos como electrónicos a partir de contar con ciertos requisitos que permitan la administración de todas las operaciones de los documentos y que cumpla con la integración de los documentos electrónicos de archivo que cuente con las siguientes características, la autenticidad, integridad y confidencialidad de la información e incorporación de tecnologías. La ISO 30301 incorpora el concepto de SGD proponiendo un sistema de gestión para las organizaciones y su alineación con las Tecnologías de la Información y las Comunicaciones – TIC, teniendo en cuenta la evolución y los diferentes medios donde se produce la información, a partir de la palabra "documentar" se empieza a incluir los diferentes procesos de trabajo que tiene las organizaciones cuyo enfoque es sistemático y hacia el uso de herramientas informáticas para la creación y el control de los documentos, con el fin de optimizar procesos y recursos.

Un sistema de gestión de documentos electrónicos – SGDE en ingles *Electronic Documents Management System – EDMS, "*es un sistema de software que controla y organiza los documentos en toda la organización, independientemente de que se hayan declarado documentos electrónicos de archivo o no"[26].

El Sistema de Gestión de Documentos Electrónicos de Archivo – SGDEA <<*Electronic Document and Records Management System – EDRMS*>>, es la incorporación de tecnologías de la información a partir de unos requisitos técnicos funcionales según la MoReq – Modelo de Requisitos para la Gestión de

[25] PRESIDENCIA DE LA REPUBLICA. Decreto Único Reglamentario del Sector Cultura, Decreto 1080 de 2015. Colombia: Bogotá, 2015.
[26] ARCHIVO GENERAL DE LA NACIÓN – AGN. Guía implementación de un Sistema de Gestión de Documentos Electrónicos de Archivo – SGDEA. En línea: <<https://drive.google.com/drive/u/1/folders/1Ex7-xrNBUHOlYv08CLKsOsZ3__VapB7b>> pág.12

Documentos Electrónicos[**] que incorpore funcionalidades como la interoperabilidad entre sistemas, gestión de contenidos, neutralidad tecnológica, adaptabilidad y flexibilidad para la planificación, manejo y organización de la documentación producida en una organización facilitando su uso, gestión, tramite y conservación de una entidad a otra. Por lo cual, se requiere de tecnología con funcionalidades particulares que cumplan con la clasificación de la información de acuerdo con la estructura de la entidad y gestionar el ciclo de vida documento desde que se crea hasta su disposición final.

Lo ideal de un SGDEA es que cumpla con 5 (cinco) componentes; captura, gestión, almacenamiento, distribución y conservación, de acuerdo con los lineamientos archivísticos nacionales como políticas internas de la entidad, procesos, procedimientos, instructivos, guías y demás que sean necesarios, entre otros que este alineados a los flujos de trabajo electrónicos.

En consecuencia, existe un marco de estándares nacionales e internacionales para la gestión documental y su alineación a los sistemas de gestión que la integran, en la tabla 3 se mencionan algunas normas como referencia de la producción documental física como electrónica y su aplicabilidad.

Tabla 3. Estándares de gestión documental

Norma	Título
UNE/ISO 30300	Sistema de gestión para los documentos. Fundamentos y vocabulario
UNE/ISO 30301	Sistema de gestión para los documentos. Requisitos
UNE/ISO 30302	Sistemas de gestión para los documentos. Guía de implantación
UNE/ISO 15489	Información y documentación. Gestión de documentos y aplicaciones
UNE/ISO 23081:2011	Metadatos para la gestión de documentos
NTC 16175-1:2013 NTC 16175-2:2015	Información y documentación. Principios y requisitos funcionales para los registros en entornos electrónicos de oficina. Parte 1 Información general y declaración de principios Parte 2 directrices y requisitos funcionales para sistemas de gestión de registros digitales

[**] El MoReq define las características que debe tener una aplicación destinada a la gestión de documentos electrónicos de archivo, se ocupa de definir los requisitos funcionales y no funcionales para la gestión de registros, este modelo se alinea con la norma ISO 15489-1:2001.

Norma	Título
NTC-ISO 14641-1:2014	Archivado electrónico. Parte 1: especificaciones relacionadas con el diseño y el funcionamiento de un sistema de información para la preservación de información electrónica.
GTC-ISO 15801:2009	Gestión de documentos. Información almacenada electrónicamente. Recomendaciones para la integridad y la fiabilidad.
Fuente El autor. Normas de la gestión documental y descripción.	

- UNE/ISO 30300 gestión documental <<*Management Systems for Records*>>, esta norma se alinea con las técnicas y procesos documentales con la metodología de los sistemas de gestión. Terminología, objetivos y beneficios. En esta norma se desarrolla el concepto de "documento" como toda evidencia de una actividad y como activo, en cualquier medio, forma o formato en que sea contenida.

- UNE-ISO 30301 esta norma propone un sistema muy concreto de gestión basado en la mejora continua y en la utilización de técnicas y conocimientos de lo que habitualmente se conoce como "gestión documental", para identificar riesgos y aprovechar oportunidades. La formulación del diseño a partir de la creación y control de los documentos durante el tiempo necesario para así establecer recursos, puntos de monitoreo. Se describen las acciones que se deben llevar a cabo para diseñar e implementar un sistema de gestión para los documentos, los cuales deben estar alineados con los objetivos y estrategias de la organización. En el anexo técnico se menciona las condiciones exigibles para las aplicaciones informáticas de gestión documental.

- UNE-ISO 30302 - Sistema de gestión para los documentos. Guía para la implementación de un SGD en las organizaciones, busca establecer, implementar, mantener y mejorar un SGD busca asegurar la alineación con la política de gestión de documentos. Esta norma tiene como base y se integra en conjunto con la ISO 30300 y ISO 30301.

- ISO 15489-1:2001 proporciona directrices acerca de la política de gestión documental, en el apartado 8.4 relaciona el diseño y la implementación de sistemas de gestión de documentos. B) la adaptación o integración de soluciones tecnológicas; y c) la definición de la forma más adecuada de incorporar estos cambios para mejorar la gestión de los documentos en la

organización. Creación, captura y gestión de registros en ambientes tecnológicos a lo largo del tiempo y la gestión de documentos en las organizaciones.

- UNE/ISO 23081:2011 Procesos de gestión de documentos. Esta norma permite una descripción normalizada de los documentos y así la definición de los elementos de metadatos para la gestión de documentos y ofrecer directrices genéricas, independientemente de su tipo de soporte (físico, análogo o digitales), esta norma también define un nivel mínimo de agrupación que son necesarios para interoperabilidad.[27]

  Esquemas de metadatos para la gestión de los documentos desde el punto de vista de las organizaciones para su implementación y la gestión de ellos a lo largo del tiempo, e inclusión de estos para las aplicaciones informáticas específicas para la gestión de documentos.

- NTC 16175-1 y 16175-2 Principios y requisitos funcionales para los registros en entornos electrónicos de oficina. Establece los requisitos funcionales que debe cumplir el software diseñados principalmente para gestionar registros que administrarán el sistema de gestión de los documentos en un entorno digital, tales cómo expedientes electrónicos, gestión de contenidos, gestión de los recursos humanos, gestión financiera, entre otros, basadas en las necesidades especificas y condiciones del negocio.

- NTC-ISO 14641-1:2014 Parte 1 especificaciones relacionadas con el diseño y el funcionamiento de un sistema de información para la preservación de información electrónica, la implementación de captura, almacenamiento y acceso a documentos electrónicos, con el fin de garantizar la legibilidad, integridad y trazabilidad de los documentos durante el tiempo de preservación.

- GTC-ISO-TR 15801 Gestión de documentos. Información almacenada electrónicamente. Recomendaciones para la integridad, usabilidad, legible y la fiabilidad a lo largo del tiempo. Es una guía que describe la implementación y operación de sistemas de gestión de documentos electrónicos, con el fin especificar las condiciones técnicas que se requieren para el almacenamiento de la información electrónica.

27 REVISTA ESPAÑOLA DE DOCUMENTACIÓN CIENTÍFICA. ISO 23081-1:2008. 3 de mayo Consulta do en línea: << https://www.uma.es/media/tinyimages/file/ISO.23081.Parte_2.pdf>>

Las normas anteriormente citadas en el marco del sistema de gestión documental busca contextualizar todo lo que integra el uso de herramientas tecnológicas para la producción de los documentos en una organización y a su vez la implicación que debe tener un sistema de gestión de la seguridad de la información - SGSI, para así contar con aplicaciones seguras que permitan garantizar desde la creación, gestión y trámite, hasta su disposición final, todo el contenido que esta almacenado en un software libre donde se proponga administrar los activos de información que la organización produce como evidencia y parte de sus funciones e actividades.

En el contexto de los sistemas de gestión documental – SGD la norma NTC-ISO 15489 marca la pauta para la administración de los documentos electrónicos en las aplicaciones tecnológicas y su interoperabilidad con otros sistemas que permitan la colaboración e integren la producción de los documentos en un solo sistema, incorporándose el concepto de Sistemas de Gestión de Documentos Electrónicos y posteriormente los Sistemas de Gestión de Documentos Electrónicos de Archivo – SGDEA.

Teniendo en cuenta que la información es un activo de bastante importancia y un altísimo recurso en una entidad, pues da cuenta de sus actividades y es la memoria de sus transacciones, es indispensable contar con una herramienta que sea segura y que garantice la administración de la información que allí se almacena. Por lo cual tomando como referencia el almacenamiento de documentos en formato electrónico requiere planes y estrategias de almacenamiento complementarios para prevenir posibles pérdidas.[28] Ya sea desde el sistema donde se da la producción del documento en formato electrónico y digital, hasta la preservación de este a través de repositorios digitales.

Una de las estrategias es el uso de modelos que se permitan la implementación de sistemas de gestión seguridad de la información para un software libre y desde un ambiente web, el cual administrara información de una organización, es decir un Sistema de Gestión de Documentos Electrónicos de Archivo (SGDEA). Por otra parte, esta el Modelo de Requisitos para la Gestión de Documentos Electrónicos – *MoReq* el cual contiene un listado de requisitos técnicos funcionales y no funcionales de un SGDEA que son aplicables de acuerdo con las necesidades de la entidad.

[28] ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN. ISO 15489-1:2001.

La MoReq identifica algunos controles y seguridad que un software debe tener para la administración de los documentos electrónicos y digitales, esto dado a los niveles de acceso por parte de los usuarios y roles que estén perfilados para la creación, uso, gestión y tramite de la información, según sea dada por el cuadro de clasificación documental - CCD a partir de un esquema de metadatos y la tabla de control de acceso - TCA, de acuerdo a la jerarquía de la organización, como también su la interacción entre otros sistemas en caso de que se implemente procesos y flujos de trabajo que permitan la interoperabilidad entre sistemas internos o externos de la organización.

El modelo de requisitos y las demás normas mencionadas, las cuales le dan origen a la concepción de la gestión documental e integración con las tecnologías de la información y las comunicaciones al incorporar nuevos mecanismos de producción de la información desde el físico y pasando al documento digitalizado y posteriormente el documento electrónico que nace, se crea, vive y se mantiene en un sistema, hace falta la descripción y aplicación de una metodología de seguridad de la información para mitigar las amenazas, vulnerabilidades a las que están expuesto un Sistema de Gestión de Documentos Electrónicos de Archivo – SGDEA.

El tema central del desarrollo de este trabajo es la aplicación de la metodología OWASP - Proyecto de Seguridad de aplicaciones Web en un sistema de gestión de documentos electrónicos de archivo – SGDEA de software libre y en ambiente web, busca realizar las pruebas pertinentes según el modelo OWASP, documentar y definir los requisitos de seguridad informática deben aplicarse en un sistema de gestión de documentos para que garantice su producción, tramite y conservación en el tiempo y el aplicativo donde se preservara la información.

6. ANÁLISIS DEL APLICATIVOS Y FALLAS DE SEGURIDAD DE UN SOFTWARE LIBRE

Para identificar las fallas de seguridad que se presentan el software libre que operan en un ambiente web es necesario realizar análisis de aquellas aplicaciones que se utilizan para la administración de gestión documental, con el fin de describir como se puede prever y proteger a partir de la aplicación de la metodología OWASP (*Open Web Application Security Project)* – Proyecto Abierto de Seguridad de Aplicaciones Web, la cual permite identificar a partir del top 10 las vulnerabilidades más críticas que pueden presentar.

La seguridad informática, es un elemento importante e imprescindible en una organización sobre todo si se busca proteger la información que se produce, en la mayoría de los casos la fuente principal son los activos de información que dan cuenta de la gestión en una entidad, sin embargo es necesario que se ejerzan los controles para prevenir vulnerabilidades y los posibles ataques a los que están expuestas las herramientas tecnológicas que administran los documentos digitales y electrónicos para así mitigar los riesgos.

Para el efecto del ejercicio se realizan las pruebas de seguridad en dos (2) sistemas de gestión documental que administran los documentos digitales y electrónicos, para detectar posibles vectores de ataque se eligen ORFEO y OpenDocMan los cuales funcionan en ambiente web y como software libre.

6.1 ORFEO

ORFEO es un sistema de gestión documental y de procesos desarrollado por la Superintendencia de Servicios Públicos Domiciliarios (SSDP), creado en Colombia cuyo objetivo es apoyar a todas las entidades en temas de alta gerencia, calidad y gestión documental, cuenta como software libre bajo licencia GNU/GPL. En la Ilustración 1 se puede observar la última versión.

Ilustración 1. ORFEO

Fuente: https://images.app.goo.gl/RCYdzFiZKiwXmxD16

El Sistema de Gestión Documental ORFEO se constituye como la herramienta tecnológica para la gestión de los documentos de algunas entidades estatales a nivel nacional y distrital, conforme con la normatividad archivística vigente y siguiendo el marco normativo del Archivo General de la Nación, da la línea técnica en materia de gestión documental de orden nacional para las entidades del estado públicas, y las que prestan servicios públicos.

El aplicativo cuenta con una serie de funciones que facilitan la gestión de los documentos de las entidades, entre estos radicación, digitalización, y reasignación de las comunicaciones oficiales, al ingresar al aplicativo cuenta con los siguientes módulos: producción, recepción, radicación, distribución, trámite, modificación, anulación, estadísticas, Tablas de Retención Documental (TRD), consultas, módulo de archivo, préstamo de documentos, expedientes virtuales administración, conservación, información del sistema.

6.2 OPENDOCMAN

Es un software de código abierto de gestión documental diseñado para el almacenamiento y acceso de los documentos de forma centralizada, compatible con Windows y Mac, es un aplicativo de gestión de documentos que de forma gratuita tiene uso compartido, almacenamiento e indexación de documentos, múltiples idiomas, gestión de flujos de trabajo e integración con correo electrónico. En la Ilustración 2 se identifica el logo del aplicativo.

Ilustración 2. OpenDocMan.

Fuente: https://www.homeppt.com/es/articles/opendocman-open-source-document-management.html

OpenDocMan se basa en la ISO 17025 en cuanto a documentar sistemas de gestión que se centra en la administración de los documentos electrónicos y de acceso web, esta aplicación permite la integración de las normas archivísticas vigentes, posee control de acceso y actualizaciones automáticas, entre las características para la gestión de documentos están: agregar cualquier tipo de archivo en el sistema, campos de metadatos, historial de revisiones, caducidad de los archivos, flujos de trabajo de los documentos, modificación, aprobación o rechazo de un documento, opciones de notificación por correo electrónico para las revisiones, asignación de categoría de los documentos (clasificación de información), propiedades de los documentos entre otras.

6.3 PRUEBAS DE SEGURIDAD

Las herramientas que se tomaron en cuenta para realizar las pruebas de seguridad como exploración, escaneo, pruebas de intrusión y penetración en aplicaciones web son las que a continuación se describen en la tabla 4.

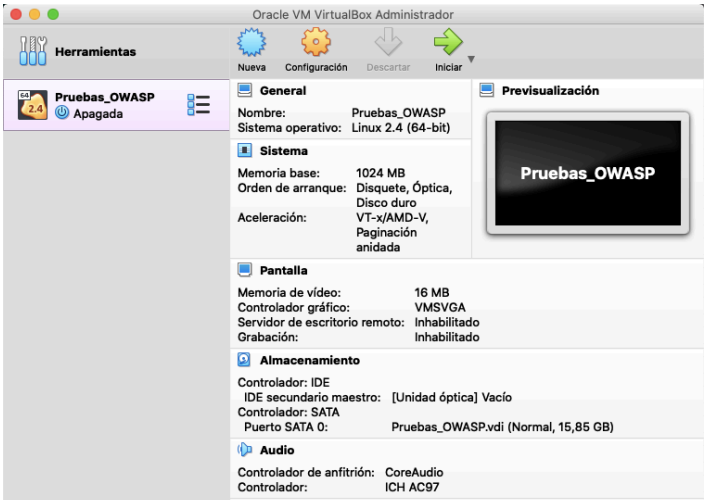
Tabla 4. Herramientas para realización pruebas

Herramientas	Aplicación	Descripción de uso
Software de Virtualización	Oracle VM VirtualBox	Herramienta bajo entorno virtual que permite la instalación y ejecución de sistemas operativos dentro de otro sistema y PC.
Sistema Operativo	Linux Kali	Sistema operativo que permite la realización de auditoría en aplicaciones web y de otras herramientas para pruebas de seguridad.
Plataforma de escaneo y verificación	OWASP ZAP	Plataforma para monitorear la seguridad de la información en las aplicaciones web
Fuente El autor. Descripción de las herramientas con las que se realizará las pruebas de seguridad		

A partir de la metodología OWASP (*Open Web Application Security Project*) se realizaron las pruebas de seguridad con el programa OWASP ZAP versión 2.9.0 (*Zed Attack Proxy*) herramienta que permite comprobar a partir de la penetración en aplicaciones web da la posibilidad de auditar, analizar y monitorear la seguridad.

Con el fin de realizar el análisis se instala en el computador *Oracle VM VirtualBox* (software para virtualización), de acuerdo con la ilustración 3. Para simular un entorno web que permita ejecutar las pruebas de seguridad y la instalación del sistema operativo.

Ilustración 3. Interfaz VM VirtualBox (software de virtualización)



Fuente: elaboración propia

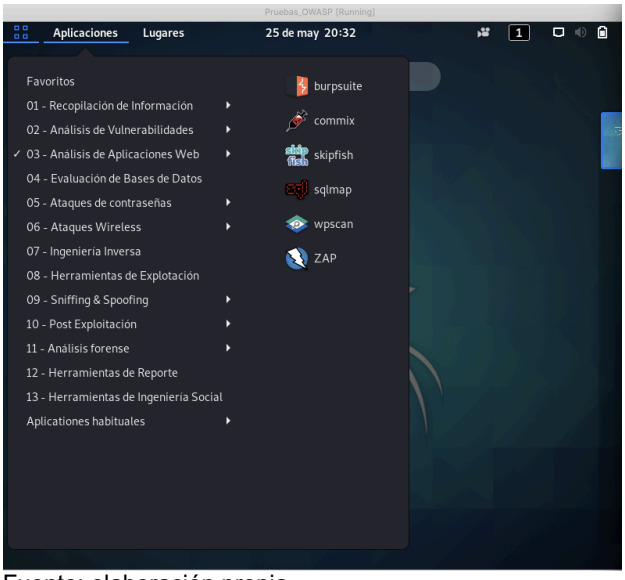
En la ilustración 4 se puede observar la interfaz del sistema operativo Kali Linux (GNU/LINUX) ya instalada en el software de virtualización. El sistema Kali Linux es un software libre y de código abierto que cuenta con diferentes funcionalidades que permiten realizar pruebas de seguridad a partir de diferentes aplicaciones de acuerdo con las necesidades del usuario final, tiene una interfaz de escritorio de fácil uso.

Ilustración 4. Interfaz de escritorio Linux

Fuente: elaboración propia, captura de pantalla

En la herramienta ZAP se puede identificar 13 opciones para seleccionar el tipo de hacking que se realizara dependiendo del interés y análisis que se aplicara en las pruebas de vulnerabilidad; como ingeniería social, análisis forense, ingeniería a la inversa y recopilación de información entre otras. Se seleccionó la opción “análisis de aplicaciones web” y entre otras del aplicativo ZAP según muestra en la ilustración 5.

Ilustración 5. Interfaz de escritorio, Linux y aplicaciones



Fuente: elaboración propia

En OWASP ZAP se ejecuta el desarrollo del proyecto, lo cual permite la aplicación de pruebas de seguridad, como la exploración, escaneo y realizar el monitoreo de los sistemas web a partir de los 10 riesgos que están definidos en la metodología OWASP, ZAP tiene las siguientes características:

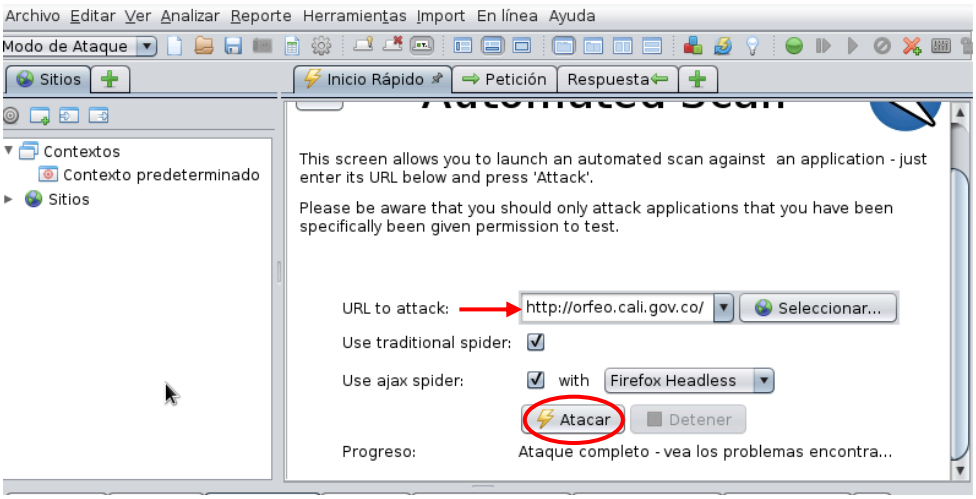
- Aplicación gratuita y de código abierto
- Herramienta multi-plataforma
- Análisis automáticos y pasivos
- Análisis de sistemas de autenticación
- Se puede realizar varios ataques
- Plugins como: control de acceso y secuencia de escaneo

Una vez seleccionadas las aplicaciones web de software libre en sistemas de gestión documental se identificó las URL's de las herramientas, a continuación, se muestra el resultado de las pruebas de penetración e intrusión en cada sistema.

6.3.1 Escaneo de la aplicación web ORFEO

Para realizar el escaneo de la aplicación web ORFEO, se selecciona la opción "*automated scan*" en el campo "*URL to attack"* se digita la URL <<http://orfeo.cali.gov.co/>> y se inicia el escaneo dando clic en "*Atacar*" como se muestra en la Ilustración 6.

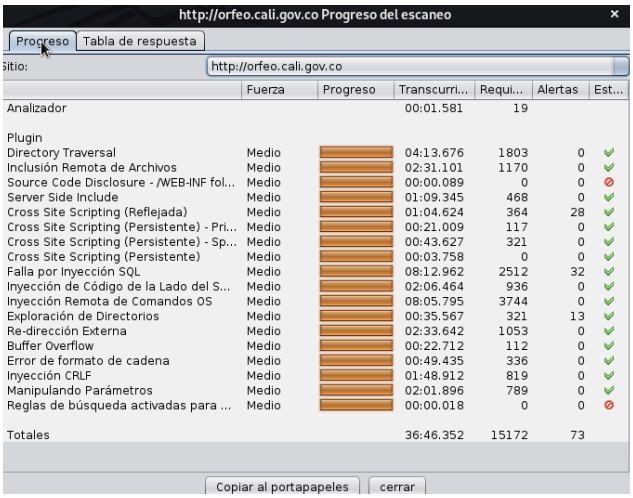
Ilustración 6. Aplicación ZAP e ingreso URL a la opción análisis automático (Automated Scan)



Fuente: elaboración propia, captura de pantalla

Se realiza el proceso de escaneo de la aplicación web según muestra en la ilustración 7 donde contiene los detalles del avance de cada una de las etapas del análisis que realiza ZAP.

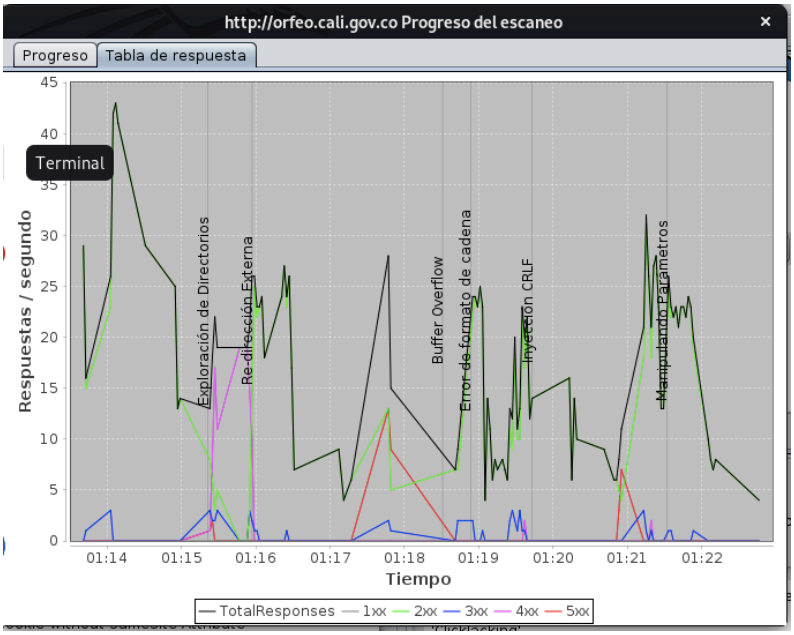
Ilustración 7. Proceso de escaneo



Fuente: elaboración propia, captura de pantalla

La ilustración 8 presenta un gráfico del proceso de respuesta por cada tipo de vulnerabilidad que se presenta, en este caso, para el ejemplo: exploración de directorios, re-dirección externa, buffer overflow, error de formato de cadena, inyección CRLF, manipulación de parámetros

Ilustración 8. Gráfica de proceso de respuesta de escaneo



Fuente: elaboración propia, captura de pantalla

La herramienta ZAP permite realizar diferentes tipos de informes:

- Informe en JSON
- Informe en HTML
- informe en un archivo XML (*eXtensible Markup Language*) el cual contiene los datos de la aplicación web descrito en esquema XML según se muestra en la Ilustración 9.

  1. Línea inicial: contiene la versión del programa, HTTP usado del código de respuesta el host y el puerto de entrada.
  2. Cuerpo: incluye los datos del reporte y las etiquetas de las alertas; alerta ítem de alerta, ID del plugin, nombre, código del riesgo, nivel de confidencialidad, la calificación del riesgo y la descripción del riego. (Anti-MINE-Sniffing X-Content-Type-Optionts)
  3. Conclusión: contiene los datos de la totalidad de las instancias de vulnerabilidades analizadas aplicadas a la categoría del riesgo de cada una donde indica; la URL, el método, el parámetro dentro de la categoría.

Ilustración 9. Reporte XML - ORFEO

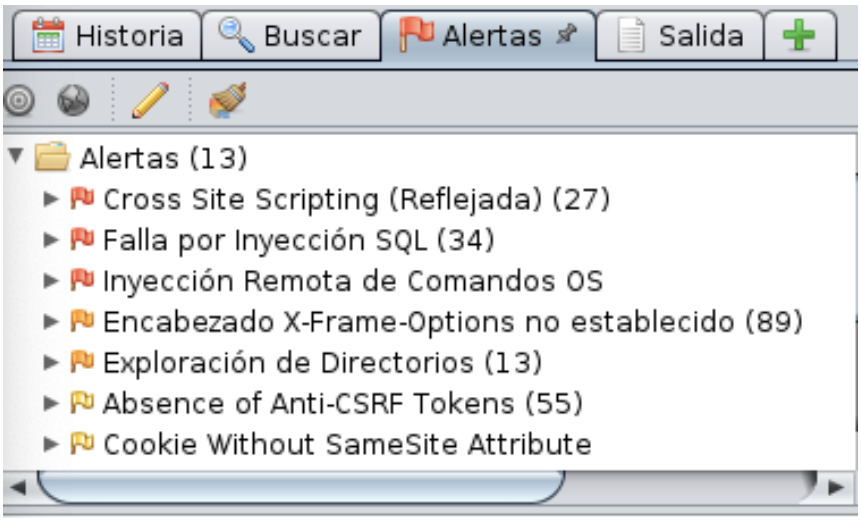
Fuente: elaboración propia, captura de pantalla del informe XML generado por OWASP ZAP.

Como resultado del análisis de la herramienta de gestión documental ORFEO se identificaron 13 alertas de seguridad los cuales varían según la vulnerabilidad por colores y según la relevancia es el orden de las banderas.

- Roja: alertas con alta prioridad (3)
- Naranja: alertas con prioridad media (2)
- Amarillo: alertas con baja prioridad (6)
- Azul: Alertas informativas (2)

En la ilustración 10 se pueden observar el total de 13 alertas generadas por el aplicativo ZAP.

Ilustración 10. Alertas arrojadas en el proceso de escaneo - ORFEO



Fuente: elaboración propia, captura de pantalla

En la tabla 5 se relaciona los resultados arrojados de las pruebas al momento de realizar el proceso de exploración activa y escaneo pasivo en la URL del sistema de gestión documental. Estás se encuentran en el orden de mayor relevancia de acuerdo con las alertas generas. Para identificar cada uno de los riesgos se analiza según la guía OWASP top 10[29] por las categorías de vulnerabilidades que aplica.

[29] OWASP. OWASP Top 10 – 2010. Los diez riesgos más críticos en aplicaciones web.

Tabla 5. Resultado y descripción de alertas arrojas de la aplicación ORFEO

Riesgo	Vulnerabilidad	No. Ins	Top 10 OWASP
Alta prioridad	Cross Site Scripting	27	A3 – Secuencia de Comandos en Sitios Cruzados (XXS)
Alta prioridad	Falla por inyección SQL	56	A1 – Inyección
Alta prioridad	Inyección Remota de Comandos OS	1	A1 – Inyección
Prioridad media	Encabezado X-Frame-Options no establecido	89	A1 – Inyección
Prioridad media	Exploración de Directorios	13	A6 – Configuración de Seguridad Incorrecta
Baja prioridad	Absence of Anti-CSRF Tokens	55	A7 – Secuencia de Comandos en Sitios Cruzados (XSS)
Baja prioridad	Cookie Without SameSite Attribute	1	A6 – Configuración de Seguridad Incorrecta
Baja prioridad	Divulgación de error de aplicación	3	A5 – Pérdida de Control de Acceso
Baja prioridad	No se encuentra encabezado X-Content-Type-Options	1	A1 – Inyección
Baja prioridad	Private IP Disclosure	16	A8 – Desacralización Insegura
Baja prioridad	Server Leaks Information via "X-Powered-By" HTTP Response Header Fields	42	A6 – Configuración de Seguridad Incorrecta
Alerta informativa	Charset Mismatch (Header Versus Meta Content-Type Charset)	55	A6 – Configuración de Seguridad Incorrecta
Alerta informativa	Timestamp Disclosure – Unix	53	A6 – Configuración de Seguridad Incorrecta

Fuente El autor. Recopilación de alertas de la aplicación web ORFEO de acuerdo con el resultado generado por el sistema

Una vez se completa el 100% del escaneo y exploración de la aplicación web ORFEO, junto con la identificación de los riesgos de acuerdo con las categorías de la guía OWASP top 10 de 2017. Se genera y descarga el informe en HTTP, esta contiene los detalles de las alertas que encontró el sistema y a su vez la clasificación por categorías de acuerdo con el nivel vulnerabilidad de la más alta a la inofensiva (informativa).

En la ilustración 11 se puede ver el detalle del informe HTTP que contiene la descripción del análisis por cada una de las alertas que fueron identificadas en el reporte y la prueba de seguridad realizada en la aplicación web ORFEO. Este incluye resumen por las categorías de las alertas, luego el detalle de cada alerta según la categoría de mayor a menor riesgos, se puede identificar la URL donde fue encontrada la alerta de seguridad con método, parámetro, ataque y evidencia, en la parte final del detalle de la alerta esta la cantidad de instancias vulnerables, la posible solución y la referencia

Ilustración 11. Informe HTML - Escaneo en la aplicación web ORFEO.

ZAP Scanning Report

Summary of Alerts

Risk Level	Number of Alerts
High	3
Medium	2
Low	6
Informational	2

Alert Detail

High (Medium)	Falla por Inyección SQL
Description	Inyección SQL puede ser posible.
URL	http://orfeo.cali.gov.co/estadisticas/vistaFormProc.php?fechah=20200523_1590295391&krd=+AND+1%3D1+--+
Low (Medium)	**Cookie Without SameSite Attribute**
Description	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
URL	https://opendocman.soft112.com/
Method	GET
Parameter	S112_UID
Evidence	Set-Cookie: S112_UID
Instances	1
Solution	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Reference	https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site
CWE Id	16
WASC Id	13
Source ID	3

Fuente: elaboración propia, captura de pantalla resultado del escaneo que arroja el aplicativo ZAP

A continuación, se describe la vulnerabilidad y el impacto que esta tienen de acuerdo con el informe HTML que genero la aplicación OWASP ZAP después de realizar las pruebas de seguridad, y según lo descrito en la tabla 5.

6.3.1.1. Alertas de clasificación alta

- Cross-Site Scripting (XSS)

Cross-Site Scripting o comandos de sitios cruzados – XSS, esta técnica de ataque explora la confianza del usuario, permitiendo inyectar en la página web visitada por el uso de código JavaScript u otro lenguaje similar, código malicioso.

Impacto: un atacante puede inyectar código: JavaScript, VBScript, ActiveX, HTML o flash para engañar con el fin de recopilar los datos. Es posible alterar el contenido de la página.

- Falla por inyección SQL

Esta técnica consiste en infiltración de código intrusión sobre la base de datos, busca la infiltración a partir de la incrustación de código SQL dentro del código SQL programado, con el fin de alterar el programa, normalmente es una vulnerabilidad maliciosa, dañina o espía, que puede llegar a ejecutarse en el servidor que aloja el sitio web.

Impacto: pérdida de información, divulgación, denegación del servicio.

- Inyección Remota de Comandos OS

Técnica de ataque usada para la ejecución no autorizada de comandos del sistema operativo.

6.3.1.2. Alertas de clasificación media

- Encabezado X-Frame-Options no establecido

El encabezado X-Frame_options no está incluido en la respuesta HTTP para proteger ante ataques 'ClickJacking'.

- Exploración de Directorios

Es posible ver el listado de directorios. La lista de directorios puede revelar scripts ocultos, incluyen archivos, copia de seguridad de los archivos de origen, etc, que se pueden acceder para leer información sensible.

6.3.1.3. Alerta de clasificación baja

- Absence of Anti-CSRF Tokens

Una solicitud falsa entre sitios en un ataque que compromete y obliga a una víctima a enviar su solicitud HTTP a un destino objetivo sin su conocimiento o intención para poder realizar una acción como víctima. La causa oculta es la funcionalidad de la aplicación utilizando acciones de URL/formulario que pueden ser adivinados de forma repetible.

Impacto: acceso a la base de datos de la aplicación, privilegios y eliminación de información.

- Cookie Without SameSite Attribute

Falsificación de solicitudes entre sitios atributo “SameSite” y ataques de tiempo, que incluye scripts entre sitios.

- Divulgación de error de aplicación

Esta página contiene un mensaje de error/advertencia que podría revelar información sensible como la ubicación del archivo que produjo la excepción no controlada. Esta información puede ser usada para lanzar futuros ataques contra la aplicación web. La alerta podría ser un falso positivo si el mensaje de error es encontrado dentro de una página de documentación.

- No se encuentra encabezado X-Content-Type-Options

El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado.

- Private IP Disclosure

Divulgación de IP privada, se ha encontrado una IP redirigida a otros sistemas internos en la respuesta del HTTP.

Impacto: perdida de la información, acceso no autorizado.

- Server Leaks Information via “X-Powered-By” HTTP Response Header Fields

El servidor web / de aplicaciones está filtrando información a través de uno o más encabezados de respuesta HTTP "X-Powered-By". El acceso a dicha información puede facilitar que los atacantes identifiquen otros marcos / componentes de los que depende su aplicación web y las vulnerabilidades a las que pueden estar sujetos dichos componentes.

Impacto: acceso indebido a la información, vulnerabilidad en los componentes de la aplicación.

6.3.1.4. Alertas de clasificación informativa

- Charset Mismatch (Header Versus Meta Content-Type Charset)

La técnica de ataque consiste en la comprobación para identificar respuestas en los encabezados HTTP Content-Type declara un conjunto de caracteres diferentes del conjunto de caracteres definido por el cuerpo del HTML o XML. Cuando hay una falta de coincidencia de conjuntos de caracteres entre el encabezado HTTP y el cuerpo del contenido, los navegadores web pueden verse forzados a un modo de detección de contenido no deseado para determinar el conjunto de caracteres correcto del contenido.

Impacto: manipulación de contenido de la página, control de contenido, manipulación de navegadores

- Timestamp Disclosure – Unix

Se identificó falla de seguridad en la aplicación web y en el web server marca de tiempo Unix

6.3.2 Escaneo de la aplicación web OpenDocMan

Para realizar el escaneo de la aplicación web OpenDocMan se selecciona la opción "*automated scan*" allí se insertó la URL <<http://opendocman.soft112.com/>> y se dio inicio la prueba como lo muestra en la Ilustración 12.

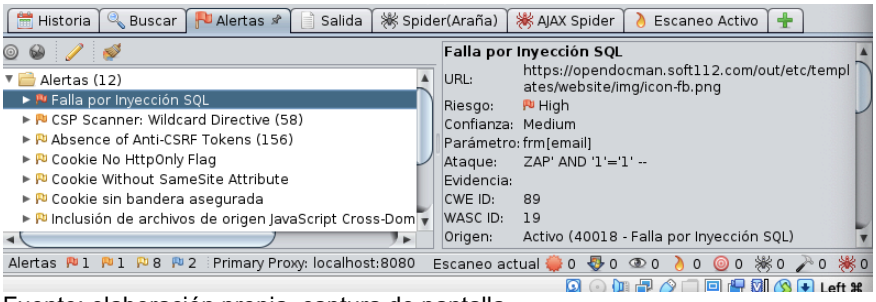
Ilustración 12. Aplicación ZAP y ingreso URL "OpenDocMan" a la opción análisis automático (Automated Scan)

Fuente: elaboración propia, captura de pantalla

Como resultado del análisis de la herramienta de gestión documental OpenDocMan se identificaron 12 alertas de seguridad las cuales varían según la vulnerabilidad por colores y según la relevancia el orden de las banderas. De acuerdo con lo que indica la ilustración 13.

- Roja: alertas con alta prioridad (1)
- Naranja: alertas con prioridad media (1)
- Amarillo: alertas con baja prioridad (8)
- Azul: Alertas informativas (2)

Ilustración 13. Alertas arrojadas en el proceso de escaneo - OpenDocMan



Fuente: elaboración propia, captura de pantalla

A continuación, se relacionan en la tabla 4 el resultado que genero la aplicación OWASP ZAP en las pruebas de seguridad de acuerdo con el proceso de escaneo y exploración de fallas, estas se encuentran en el orden de mayor relevancia de acuerdo con las alertas reportadas, la descripción se realizó en la identificación de cada riesgo según la guía OWASP top 10[30] de acuerdo con las categorías de vulnerabilidades.

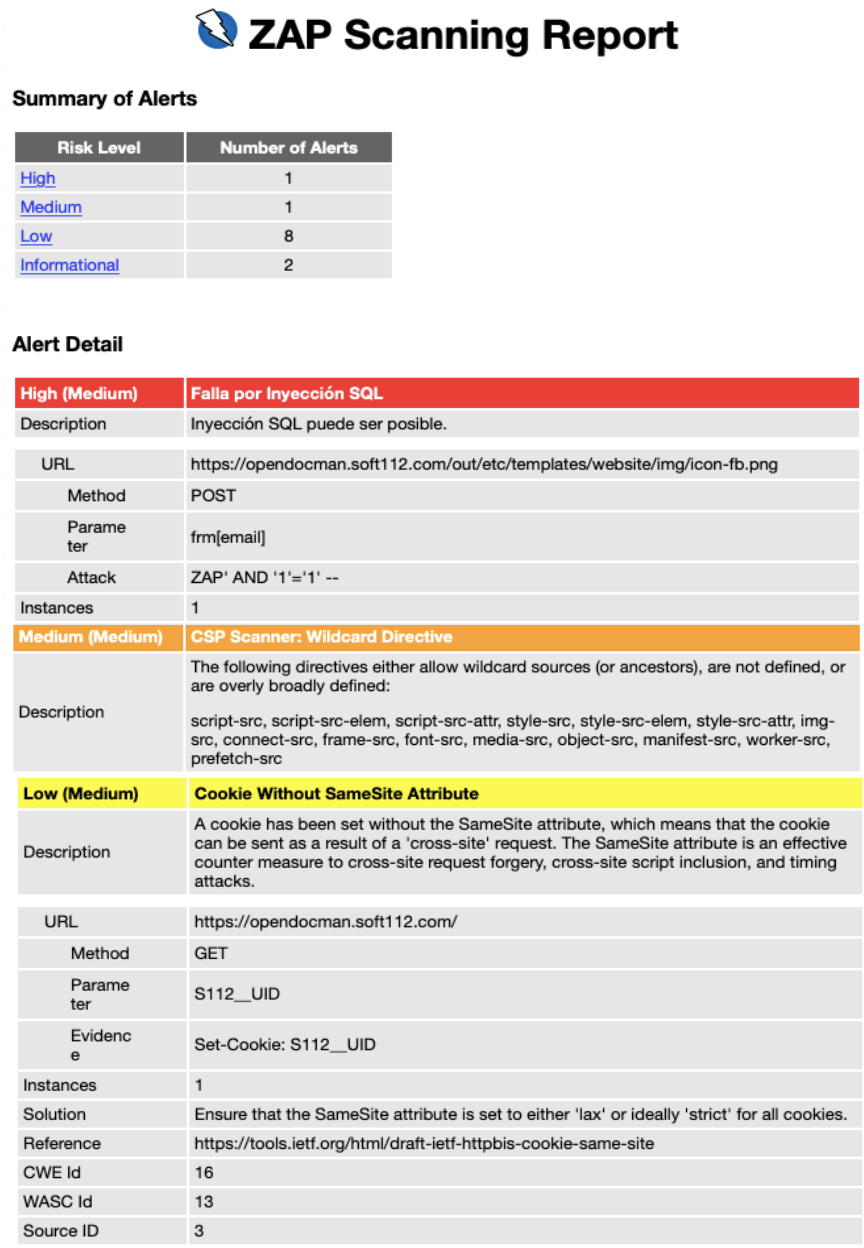
Tabla 6. Resultado y descripción de alertas arrojas de la aplicación OpenDocMan

Riesgo	Vulnerabilidad	No. Ins	Descripción
Alta prioridad	Falla por inyección SQL	1	A1 – Inyección
Prioridad media	CSP Scanner: Wildcard Directive	58	A6 – Configuración de Seguridad Incorrecta
Baja prioridad	Absence of Anti-CSRF Tokens	156	A7 – Secuencia de Comandos en Sitios Cruzados (XSS)
Baja prioridad	No se encuentra encabezado X-Content-Type-Options Header	21	A3 – Exposición de Datos Sensibles
Baja prioridad	Server Leaks Information via "X-Powered-By" HTTP Response Header Fields	59	A6 – Configuración de Seguridad Incorrecta
Baja prioridad	Inclusión de archivos de origen JavaScript Cross-Domain	114	A7 – Secuencia de Comandos en Sitios Cursados (XXS) Cross-Site Scripting (XXS)
Baja prioridad	Cookie No HttpOnly Flag	1	A6 – Configuración de Seguridad Incorrecta
Baja prioridad	Incompleto o no Cache-control y sistema de encabezado HTTP Pragma	14	A3 – Exposición de Datos Sensibles
Baja prioridad	Cookie Without SameSite Attribute	1	A6 - Configuración de Seguridad Incorrecta
Baja prioridad	Cookie sin bandera asegurada	1	A3 – Exposición de Datos Sensibles
Alerta informativa	Timestamp Disclosure – Unix	56	A6 - Configuración de Seguridad Incorrecta
Alerta informativa	Loosely Scoped Cookie	3	A1 – Inyección A5 – Perdida de Control de Acceso
Fuente El autor. Recopilación de alertas de la aplicación web OpenDocMan de acuerdo con el resultado generado por el sistema			

Una vez completado el 100% del escaneo de la aplicación web OpenDocMan e identificación de las alertas de acuerdo con las categorías de la guía OWASP top 10 de 2017, se descarga el informe en HTTP como se muestra en ilustración 14, esta contiene los detalles de las alertas que encontró el sistema y a su vez la clasificación por categorías de acuerdo con el nivel vulnerabilidad de la más alta a la inofensiva.

[30] OWASP. Op. cit. p.6-16

Ilustración 14. Informe HTML - Escaneo en la aplicación web OpenDocMan



ZAP Scanning Report

Summary of Alerts

Risk Level	Number of Alerts
High	1
Medium	1
Low	8
Informational	2

Alert Detail

High (Medium)	**Falla por Inyección SQL**
Description	Inyección SQL puede ser posible.
URL	https://opendocman.soft112.com/out/etc/templates/website/img/icon-fb.png
Method	POST
Parameter	frm[email]
Attack	ZAP' AND '1'='1' --
Instances	1
Medium (Medium)	**CSP Scanner: Wildcard Directive**
Description	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, script-src-elem, script-src-attr, style-src, style-src-elem, style-src-attr, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src, prefetch-src
Low (Medium)	**Cookie Without SameSite Attribute**
Description	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
URL	https://opendocman.soft112.com/
Method	GET
Parameter	S112__UID
Evidence	Set-Cookie: S112__UID
Instances	1
Solution	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Reference	https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site
CWE Id	16
WASC Id	13
Source ID	3

Fuente: elaboración propia, captura del escaneo que arroja el aplicativo ZAP

El informe contiene información relevante de alertas como la cantidad de instancias que aplica según la alerta, las URL`s identificadas para cada caso, el método, parámetro, solución que se puede aplicar, el CWE ID (Diccionario de debilidades comunes – *Common Weakness Enumeration*) y el WASD ID – *Web Application Security Consortium.*

A continuación, se realiza la descripción de acuerdo con las categorías de alertas identificadas en el análisis, a partir de las pruebas de aplicadas en el sistema OpenDocMan.

6.3.1.5. Alertas de clasificación alta

- Falla por inyección SQL

Infiltración de código intruso sobre la base de datos, busca la infiltración a partir de la incrustación de código SQL dentro del código SQL programado, con el fin de alterar el programa, normalmente es una vulnerabilidad maliciosa, dañina o espía, que puede llegar a ejecutarse en el servidor que aloja el sitio web.

Impacto: pérdida de información, divulgación, denegación del servicio.

6.3.1.6. Alertas de clasificación media

- CSP Scanner: Wildcard Directive

Las siguientes fuentes directivas funcionan como comodín, las cuales no están definidas o están definidas de manera demasiado amplia, estos se provocan diversos ataques definidos que no son de confianza:

script-src, script-src-elem, script-src-attr, style-src, style-src-elem, style-src-attr, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src, prefetch-src

Esto quiere decir que existe una falla en la configuración de la aplicación y se debe establecer el encabezado *Content Security-Policy – CSP.* Esta falla de seguridad "esta permitiendo el acceso a datos sensibles almacenados en el servicio de nube (CSP)".[31]

Impacto: acceso a la información almacenada en la aplicación web.

6.3.1.7. Alerta de clasificación baja

[31] OWASP. Op. cit. p.12.

- Absence of Anti-CSRF Tokens

La técnica de este ataque es adivinar la información a través de una funcionalidad de acciones de URL/formulario, en este caso un CSRF – *Cross Site Request Forgery o* Falsificación de petición en sitios cruzados*,* explorando la confianza que un sitio web proporciona, generando falsificación en solicitudes.

Impacto: acceso a la información de la aplicación, divulgación de información.

- No se encuentra encabezado X-Content-Type-Options Header

La aplicación web no cuenta con la configuración del encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto hace que las versiones antiguas de Internet Explorer y Chrome se ejecuta MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado.

Impacto: acceso no autorizado a los datos o funciones de la aplicación.

- Server Leaks Information via “X-Powered-By” HTTP Response Header Fields

Se presenta filtración de información a través de los encabezados HTTP X-Powerer-By, este acceso de información facilita que los componentes de los que depende el servidor y la aplicación web están expuestos.

Impacto: acceso a la información de la aplicación web, exploración de información.

- Inclusión de archivos de origen JavaScript Cross-Domain

Las páginas incluyen uno o mas archivos encriptados de un dominio de terceros.

Impacto: sitio web malicioso, funcionalidad maliciosa en la aplicación

- Cookie No HttpOnly Flag

Se presenta error en la configuración en el software, se ha establecido una cookie sin la bandera HttpOnly, lo que significa que la cookie puede ser accedida mediante JavaScript. Si un script malicioso puede ser ejecutado en esta página entonces la cookie será accesible y podrá ser transmitida a otro sitio.

Impacto: secuestro de sesión, comprometer al sistema.

- Incompleto o no Cache-control y sistema de encabezado HTTP Pragma

El cache-control y encabezado HTTP Pragma no han sido establecidos apropiadamente o faltan, permitiendo al navegador y servidores proxy almacenar contenido.

Impacto: ataques en autenticación, acceso no autorizado a información sensible

- Cookie Without SameSite Attribute

La alerta identifico que la cookie no cuenta con el atributo SameSite, este hace que las cookies sean más seguras, pues evita enviar peticiones de una solicitud 'entre sitios' diferentes a donde se originaron, es una contramedida que evita la falsificación de solicitudes.

Impacto: ataques de tiempo, inclusión de scripts entre sitios y falsificación de peticiones.

- Cookie sin bandera asegurada

Una cookie ha sido enviada sin la bandera asegurada, lo que significa que la cookie puede ser accedida mediante conexiones sin cifrar. Las cookies sensibles en la https no esta configura.

Impacto: acceso a la información

6.3.1.8. Alertas de clasificación informativa

- Timestamp Disclosure – Unix

Se identificó falla de seguridad en la aplicación web y en el web server marca de tiempo Unix

- Loosely Scoped Cookie

Esta alerta corresponde a que el dominio de las cookies es flexible, lo cual puede tener un alcance por dominio o ruta. El alcance del dominio aplicado a una cookie determina qué dominios pueden acceder a ella. Esto quiere decir que el atacante puede modificar las cookies dentro del navegador.

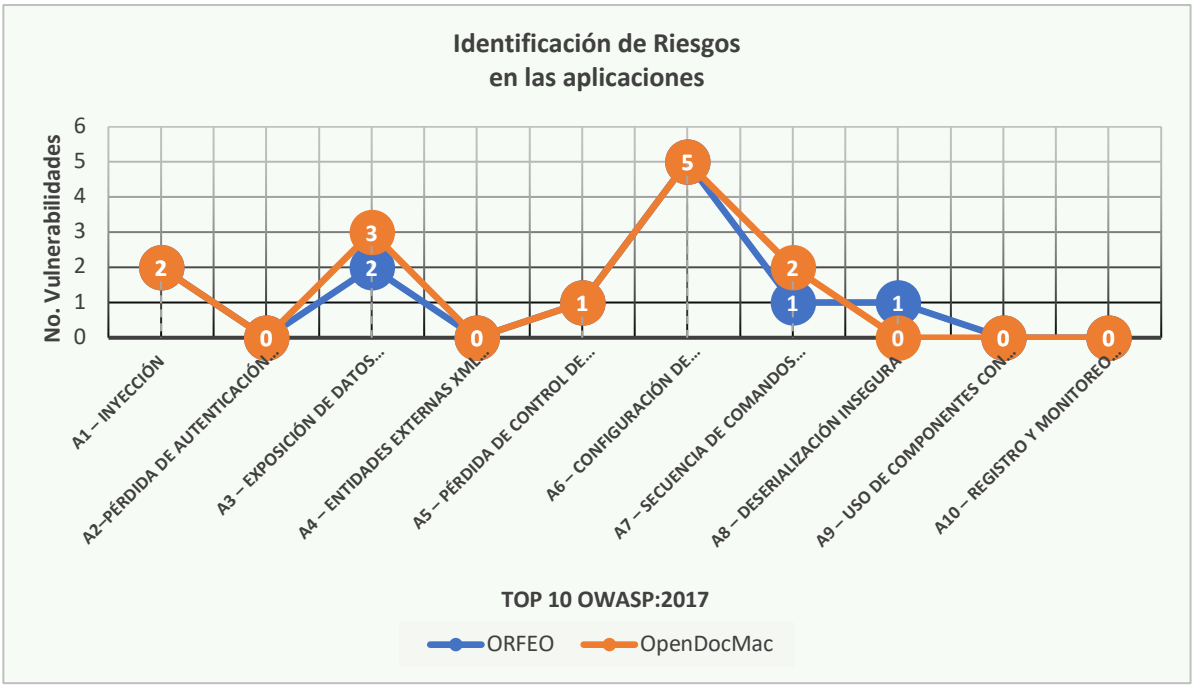
Impacto: eludir la autenticación, realizar ataques de inyección SQL o modificar entradas de maneras inesperadas.

Para finalizar, el resultado de las pruebas realizadas a las aplicaciones, donde ORFEO tiene (13) trece y OpenDocMan tiene (12) doce vulnerabilidades, se identificó (6) seis riesgos en común que tienen estos sistemas de gestión documental de acceso libre.

1. Falla por inyección SQL
2. Absence of Anti-CSRF Tokens
3. Cookie Without SameSite Attribute
4. No se encuentra encabezado X-Content-Type-Options
5. Server Leaks Information via “X-Powered-By” HTTP Response Header
6. Timestamp Disclosure – Unix

En la gráfica 1 muestra las categorías que están asociadas a la clasificación del OWASP de las pruebas generadas en la aplicación ZAP, donde se identifico que de las (25) veinticinco vulnerabilidades presentadas están clasificadas en (6) seis tipologías, tales como: A1:2017 Inyección, A3:2017 Exploración de datos sensibles, A5:2017 pérdida de control de acceso, A6:2017 Configuración de Seguridad Incorrecta, A7:2017 Secuencia de Comandos en Sitios Cruzados (XSS), A8:2017 Deserialización Insegura.

Gráfico 1. Identificación de riesgos de las aplicaciones SGDE - Top 10 OWASP:2017



Fuente: elaboración propia, análisis de las vulnerabilidades identificadas en las aplicaciones ORFEO y OpenDocMan, según el top 10 OWASP:2017.

7. MODELO DE REQUISITOS DE SEGURIDAD INFORMÁTICA BASADOS EN OWASP

Un modelo de requisitos de seguridad informática basado en OWASP, permite definir características de seguridad, el cual contiene la descripción de condiciones que debe cumplir un sistema seguro para este caso el software que se encuentre en un entorno web y que sean para la administración de la gestión documental de los documentos electrónicos y digitales en una organización. Una vez, documentada la información de los estándares para los Sistemas de Gestión de Seguridad de la Información – SGSI y los Sistemas de Gestión de Documentos Electrónicos - SGDE se realizaron las pruebas de seguridad para identificar las amenazas, vulnerabilidades, riesgos de los cuales puede ser objeto un software tomando como instrumento ZAP.

Del ejercicio realizado, el resultado que se obtuvo de la metodología OWASP top 10 del 2017 para los aplicativos de gestión documental ORFEO y OpenDocman se identificaron los riegos más críticos que se presentaron en las pruebas de seguridad realizadas en el capítulo 6. A continuación, en la tabla 7 se presentan los riesgos de seguridad de las aplicaciones web de software libre.

Tabla 7. Identificación de riesgos de las aplicaciones web según la Guía OWASP Top 10 2017.

Riesgos en Seguridad OWASP Top 10 2017	Vulnerable	Nombre de la APP	CWE	Fallas y Vulnerabilidades Identificadas
A1 – Inyección	SI	ORFEO OpenDocMan	89 78 16	- Falla por inyección SQL - Inyección Remota de Comandos OS - Encabezado X-Frame-Options no establecido - No se encuentra encabezado X-Content-Type-Options
A2–Pérdida de Autenticación y Gestión de Sesiones	NO			
A3 – Exposición de datos sensibles	SI	ORFEO OpenDocMan	79 525 13	- Cross Site Scripting - Incompleto o no Cache-control y sistema de encabezado HTTP Pragma - Cookie sin bandera asegurada
A4 – Entidades Externas XML (XXE)	NO			
A5 – Pérdida de control de acceso	SI	ORFEO OpenDocMan	200 565	- Divulgación de error de aplicación - Loosely Scoped Cookie
A6 – Configuración de Seguridad Incorrecta	SI	ORFEO OpenDocMan	200	- Exploración de Directorios - Cookie Without SameSite Attribute - Charset Mismatch (Header Versus Meta Content-Type Charset)

Riesgos en Seguridad OWASP Top 10 2017	Vulnerable	Nombre de la APP	CWE	Fallas y Vulnerabilidades Identificadas
				- Server Leaks Information via "X-Powered-By" HTTP Response Header Fields - Cookie No HttpOnly Flag - Cookie Without SameSite Attribute - Timestamp Disclosure – Unix
A7 – Secuencia de Comandos en Sitios Cruzados (XSS)	SI	ORFEO OpenDocMan	352 829 565	- Absence of Anti-CSRF Tokens - Inclusión de archivos de origen JavaScript Cross-Domain - Loosely Scoped Cookie
A8 – Deserialización Insegura	SI	ORFEO	200	- Private IP Disclosure
A9 – Uso de Componentes con Vulnerabilidades Conocidas	NO			
A10 – Registro y monitoreo insuficientes	NO			
Fuente: el autor a partir de informe de OWASP ZAP identificación de fallas y vulnerabilidades de OWASP Top 10 2017				

En las aplicaciones web ORFEO y OpenDocman se encontraron un total de 6 riesgos de los 10 que describe el OWASP top 10, tipificados en: A1 Inyección, A2 Pérdida de autenticación, A3 Exposición de datos sensibles, A5 Pérdida de control de acceso, A6 Configuración incorrecta de seguridad y A8 Deserialización insegura. Este análisis de riesgos presentados en las aplicaciones web para los sistemas de gestión documental de software libre, dan como resultado la descripción de aspectos relevantes acerca de las vulnerabilidades de seguridad de la información.

Para el desarrollo del modelo de requisitos cuya identificación de riesgos y vulnerabilidades que presenta mayor frecuencia en las aplicaciones web se abordan los siguientes controles:

- **Control de Arquitectura, diseño y modelo de amenazas**

Estos requisitos deben permitir que la aplicación realice controles en los componentes de la aplicación, que la arquitectura y los códigos sean adecuadas, y su utilidad y uso sean eficientes para los fines pertinentes.

- **Control de autenticación**

El objetivo de este control de autenticación es impedir la suplantación de información y que el usuario o persona se autentique de forma segura en la

aplicación, a través de los mecanismos correctos como la utilización de contraseña, credenciales que puedan ser verificadas mediante el correo electrónico de la entidad o el empleo de características específicas, lo cual permitirá tener un control de acceso seguro al sistema de gestión documental.

- **Control de gestión de sesión**

Una aplicación web tiene diferentes componentes, pero es necesario contar con un mecanismo que controle el estado del usuario y su interacción entre la herramienta, es decir que, en la administración de las sesiones, lo cual se requiere que estas sean únicas por rol y se cierre cuando se agote el tiempo de espera e inactividad

- **Control de acceso**

Lo que se busca con este requisito es el acceso directo a la aplicación de los usuarios que están autorizados y pueden realizar ciertas acciones en la herramienta según este definido y a través de roles, perfiles y privilegios que le fueron otórganos una vez se diligenciado el formato de creación del perfil de acceso al sistema de gestión documental u herramienta. Es importante que la aplicación cuente con un esquema de metadatos de los roles y permisos para evitar la manipulación inadecuada de la información.

- **Control para el manejo de entrada de datos maliciosos**

La protección de la entrada de datos de la aplicación web resulta ser una falla muy común, pues es allí donde se presentan la mayor parte de vulnerabilidades al no prestar atención en la validación de entrada y la arquitectura de codificación de salida, en este sentido la información puede presentar vulneraciones como las que fueron identificadas en las pruebas: inyección SQL, ataques de configuración, scripting entre sitios – XXS.

- **Control de criptografía almacenada**

Que la aplicación proporcione mecanismos de autenticación que permitan verificar la identidad del comunicador a partir del cifrado de la información, para que la gestión y trámite en la herramienta sea segura.

- **Control de gestión y registro de errores**

Este control permite identificar que la aplicación web proporcione datos de información útil y que no deberían estar almacenados en esta por ser de carácter

privado y confidencial de acuerdo con la clasificación de estos, lo cual debe garantizar que la información sea manejada de forma segura con el fin de evitar ataques de penetración.

- **Control de protección de datos**

Para este tipo de control aplica los criterios básicos de seguridad de la información: confidencialidad, integridad y disponibilidad. (CIA), lo cual busca la protección de datos en la aplicación y que cuente con los suficientes mecanismos de confianza, ya que almacena información sensible tanto para la entidad como los usuarios externos.

- **Control de comunicaciones**

Este hace referencia a la información de entrada y de salida entre el sistema y su interacción con otros y el servidor de la entidad, por lo tanto, lo ideal es que la aplicación utilice un TLC – *Transport Layer Security*, seguridad de la capa de transporte, o cifrado seguro para la trasmisión de datos.

- **Control de código malicioso**

Se debe controlar que, a partir de las acciones realizadas desde el sistema, deje registro de actividades malintencionadas que no afecten la aplicación, no tenga ataques basados en tiempo asegurar que el código no tiene código malicioso inherentes a la funcionalidad.

- **Control de lógica de negocios**

Este requerimiento hace parte de las reglas de negocio de las funciones que proporciona la aplicación, en este caso para la administración de información que será creada, almacenada y cambiada mediante un entorno web para el procesamiento de los datos de captura y la interfaz del usuario. El fin como tal es que cumpla con los requisitos para la detención de ataques automáticos, protección de falsificación, alteración, repudio y revelación de los datos que contiene los expedientes electrónicos y digitales.

- **Control de archivos y recursos**

Si bien la aplicación administra información de toda la organización, es necesario asegurar que cumpla con requisitos de información tales como; la administración de

los datos confiables y aquellos datos que sean obtenidos de otras fuentes deben tener un tratamiento adecuado de forma segura.

- **Control de API y servicio web**

Garantizar que la aplicación cuenta con API – *Application Programming Interface*, Interfaz de programación de aplicaciones para los servicios de confianza, para que cumpla con los siguientes requisitos:

- "Autenticación adecuada, gestión de sesiones y autorización de todos los servicios web.
- Validación de entrada de todos los parámetros que transitan de un nivel de confianza inferior a superior.
- Controles de seguridad eficaces para todos los tipos de API, incluida la nube y la API sin servidor"[32]

- **Control de configuración**

Este control requiere que al momento de ser instalada la aplicación se cuente con un entorno seguro, que no contenga componentes obsoletos, al ser una aplicación entorno web se debe garantizar una configuración efectiva fuera de la arquitectura tecnológica de la entidad. En aquellos casos donde se presente problemas de seguridad esto no debe interrumpir el servicio, ni el entorno de producción. Garantizar la disponibilidad continua y integridad de la implementación, evitando así mismo vulnerabilidades como: intrusiones, hackeado infraestructura definida por el software, tiempo de inactividad, compilación automatizada en contenedores.

Que la aplicación web a pesar de estar en un entorno público proporcione el uso de bibliotecas, plataforma actualizada, hardening, no este expuesta a debilidades de seguridad o fallas de los sistemas.

Una vez mencionados cada uno de los controles que se aplican para las aplicaciones web de sistemas de gestión documental, es necesario aclarar que a pesar de que las fallas fueron presentadas en un porcentaje de 7 riesgos del OWASP top 10 de 2017, es necesario recurrir a todas las inspecciones de seguridad de la información con el fin de que los sistemas sean seguros.

El modelo de requisitos fue desplegado en los 13 controles para la descripción de cada uno de ellos, los cuales se deben verificar y comprobar en una herramienta de gestión documental de documentos electrónicos y digitales de archivo, en la tabla 8 se presentan con su respectiva descripción y aplicabilidad.

[32] OWASP. Estándar de verificación de seguridad en aplicaciones 3.0.1. 2017. pág.54

Tabla 8. Listado de requisitos propuestos de aplicaciones web de sistemas de gestión documental de documentos electrónicos de software libre basados en OWASP.

No.	Descripción del requisito	Tipo de Control que Aplica
1	Verificar que todos los componentes de la aplicación sean necesarios, usados y se encuentran identificados	Arquitectura, diseño y modelado de amenazas
2	Verificar todos los componentes, tales como bibliotecas, módulos y conexión con sistemas externos, que no son parte de la aplicación pero que esta los necesita esten identificados.	Arquitectura, diseño y modelado de amenazas
3	Verificar que la aplicación tiene definida una arquitectura de alto nivel para la aplicación.	Arquitectura, diseño y modelado de amenazas
4	Verificar que todos los componentes de la aplicación se definen de acuerdo a las funciones de negocio (gestión, trámite, producción, transferencias y preservación a largo plazo).	Arquitectura, diseño y modelado de amenazas
5	Verificar que los componentes que no son parte de la aplicación pero que son necesarios para su funcionamiento, sean definidos de acuerdo al análisis y modelamiento de los procesos de la entidad y seguridad.	Arquitectura, diseño y modelado de amenazas
6	Verificar que se ha realizado un modelo de amenazas para la aplicación y el cual cubra riesgos asociados con la suplantación de identidad, manipulación, repudio, revelación de información y elevación de privilegios.	Arquitectura, diseño y modelado de amenazas
7	Verificar que todos los controles de seguridad (incluyendo las bibliotecas que llaman a servicios de seguridad externos) tienen una implementación centralizada.	Arquitectura, diseño y modelado de amenazas
8	Verificar que los componentes cuenten con controles de seguridad en la segmentación de la red, reglas de firewall, o grupos de seguridad basados en la nube.	Arquitectura, diseño y modelado de amenazas
9	Verificar que la aplicación tiene separación entre las capas (datos, control y presentación), para las desiciones de seguridad.	Arquitectura, diseño y modelado de amenazas
10	Verificar que la apliación no tenga información propietaria de código del lado del cliente, información sensible, claves secretas y políticas de otros desarrolladores	Arquitectura, diseño y modelado de amenazas
11	Verificar que los componentes de la aplicación, módulos, frameworks, plataformas, accesos remotos y sistemas operativos se encuentran libres de vulnerabilidades conocidas y posea un listado de comprobación segura y requisitos de seguridad.	Arquitectura, diseño y modelado de amenazas
12	Comprobar que las contraseñas tienen más de 8 caracteres los cuales deben contener: símbolos, letras mayúsculas, minusculas y números.	Autenticación
13	Verificar en la aplicación para los campos de autenticación de credenciales no reflejen las contraseñas del usuario.	Autenticación

Continuación Tabla 8.

No.	Descripción del requisito	Tipo de Control que Aplica
14	Comprobar que los controles de autenticación se realicen desde el servidor de la entidad.	Autenticación
15	Verificar que los usuarios pueden cambiar la contraseña con cierta periodicidad que este determinado por la aplicación. (SI)	Autenticación
16	Comprar que se use un medidor de fuerza de la contraseña, que permita identificar al usuario que la contraseña es segura. (débil, medio y fuerte)	Autenticación
17	Verificar que la funcionalidad de cambio de contraseña que como medio de autenticación solicite: anterior, la nueva y confirmación de contraseña.	Autenticación
18	Verificar que todas las decisiones de autenticación son registradas en auditoría de la aplicación (bitácora) sin que esto implique el almacenamiento de información la contraseña.	Autenticación
19	Verificar que la aplicación utilice una rutina de hashing para la verificación de contraseñas y que estén almacenadas en el sistema.	Autenticación
20	Comprobar que el correo electrónico institucional solo sea un mecanismo de autenticación y este no proporcione información de la contraseña cuando se solicite recuperación de la contraseña.	Autenticación
21	Verificar que la aplicación no permita el uso de contraseñas por defecto.	Autenticación
22	Verificar que la aplicación cuenta con todos los mecanismos autenticadores para evitar ataques de fuerza bruta, ataques de bloque de cuentas, almacenamiento de diccionarios y demás.	Autenticación
23	Comprobar que la aplicación puede configurarse para que no permita el uso de contraseñas que sean utilizadas nuevamente.	Autenticación
24	Verificar que la aplicación mediante el metodo de autenticación no proporcione datos del usuario y contraseña.	Autenticación
25	Comprobar que el proveedor de servicios de credenciales (CSP) y la aplicación que verifica la autenticación están separados, para evitar el acceso a las contraseñas de los usuarios de la aplicación.	Autenticación
26	Comprobar que la aplicación almacena las contraseñas con la protección suficiente para evitar ataques de recuperación sin conexión, incluido el acceso al sistema local.	Autenticación
27	Comprobar que la aplicación cuente con las integraciones de bases de datos y sistemas de terceros, y las claves de API se administran de forma segura y no se incluyen en el código fuente ni se almacenan en repositorios de código fuente, para la administración de contraseñas y evitar ataques informáticos.	Autenticación
28	Verificar que la aplicación no revele datos de tokens, URL de la sesión.	Gestión de sesiones

Continuación Tabla 8.

No.	Descripción del requisito	Tipo de Control que Aplica
29	Verificar que las sesiones se desactivan e invalidan cuando el usuario cierra la sesión, en un periodo determinado o por inactividad.	Gestión de sesiones
30	Verificar que la aplicación contenga la funcionalidad de cierre de la sesión.	Gestión de sesiones
31	Verificar que el identificador de sesión nunca se revele en URLs, mensajes de error o registros de bitácora. Y no aplique compatibilidad con la re-escritura de URL.	Gestión de sesiones
32	Comprobar que los tokens de sesión basados en cookies tienen el atributo 'HttpOnly', 'SameSite' y 'Secure' establecido, para limitar la exposición a ataques de falsificación de solicitudes entre sitios.	Gestión de sesiones
33	Verificar que la aplicación limita el número de sesiones activas.	Gestión de sesiones
34	Comprobar que una vez se realice el cambio de contraseña el sistema cierra todas las sesiones activas.	Gestión de sesiones
35	Comprobar que los tokens de sesión sin estado utilizan firmas digitales, cifrado y otras contramedidas para protegerse contra ataques de manipulación, envolvente, reproducción, cifrado nulo y sustitución de claves. *****	Gestión de sesiones
36	Verificar que la aplicación en el momento de realizar una transacción de carácter especial solicite nuevamente autenticación del usuario para verificación.	Gestión de sesiones
37	Comprobar que los datos de autenticación no se almacenen en el servidor y sean eliminados una vez terminada la sesión.	Gestión de sesiones
38	Comprobar que la aplicación tiene reglas de control de acceso y sean parametrizables por el administrador de la entidad.	Control de acceso
39	Comprobar que la información y los datos contenidos en la herramienta en cuanto a la política de información no sean manipulables, modificables y que no sean autorizados.	Control de acceso
40	Comprobar que el usuario de acuerdo al rol cuente con los privilegios correspondientes para el acceso y permisos a los documentos electrónicos permitidos.	Control de acceso
41	Verificar que los controles de acceso fallen de forma segura, incluso cuando se presente una excepción.	Control de acceso
42	Comprobar que la aplicación tiene el principio de privilegios mínimos, para los usuarios y que solo deben acceder a funciones, documentos electrónicos, datos y direcciones que estan especificadas y autorizadas por la entidad.	Control de acceso
43	Verificar que la aplicación registre las acciones de control de acceso, acciones fallidas y se pueda validar en la auditoría o bitácora del sistema.	Control de acceso
44	Verificar que la aplicación o su infraestructura emite tokens anti-CSFR aleatorios existe otro mecanismo de protección de la transacción. *	Control de acceso

Continuación Tabla 8.

No.	Descripción del requisito	Tipo de Control que Aplica
45	Verificar que las interfaces administrativas utilicen la autenticación multifactor adecuada para evitar el uso no autorizado a las secciones o módulos de la aplicación.	Control de acceso
46	Verificar que la aplicación tiene desabilitada la exploración de directorios, para evitar divulgación de los datos, archivos, expedientes electrónicos contenidos en la herramienta.	Control de acceso
47	Verificar que la aplicación aplique correctamente la autorización contextual para no permitir la manipulación de parámetros de la URL.	Control de acceso
48	Comprobar que la aplicación tiende defensas contra los ataques de contaminación de parámetros HTTP (GET, cookies, encabezados o variables de entorno, ambiente, entre otros)	Manejo de entrada de datos maliciosos
49	Validar que el único control de validación de entrada sea usado por la aplicación.	Manejo de entrada de datos maliciosos
50	Comprobar que la aplicación protege contra ataques de inyección.	Manejo de entrada de datos maliciosos
51	Comprobar que la aplicación protege contra ataques de SSRF	Manejo de entrada de datos maliciosos
52	Verificar que la aplicación tenga controles de seguridad para prevenir inyección LDAP.	Manejo de entrada de datos maliciosos
53	Verificar que la aplicación cuente con los controles de seguridad que previenen la inyección de comandos del sistema operativo.	Manejo de entrada de datos maliciosos
54	Verificar que la aplicación cuente con todos los controles para los ataques XML como manipulación y ataques de inyección XML	Manejo de entrada de datos maliciosos
55	Verificar que la aplicación no sea susceptible a ataques DOM Cross-Site Scripting (XSS) y asegure los formularios de entrada HTML.	Manejo de entrada de datos maliciosos
56	Comprobar que framework de la aplicación rechase peticiones para el cambio de los campos sensibles de seguridad como "*accountBalance*", "*role*" o "password" sean protegidos de enlaces automáticos maliciosos.	Manejo de entrada de datos maliciosos
57	Comprobar que el framework de la apliación este activo y rechace parametros de petición (GET, POST, cookies, cabeceras, variables de entorno, ambiente, entre otros)	Manejo de entrada de datos maliciosos
58	Verificar que las consultas de SQL, HQL, OSQL, NOSQL y procedimientos almacenados y que no sean susceptibles a la inyección de SQL	Manejo de entrada de datos maliciosos
59	Verificar que los datos de entrada sean validados, para los campos de formularios HTML, los orígenes de entrada como las llamadas REST, parámetros de consulta, encabezados HTTP, cookies, archivos por lotes.	Manejo de entrada de datos maliciosos
60	Comprobar que la aplicación protege contra ataques de inyección XPath o de inyección XML.	Manejo de entrada de datos maliciosos

Continuación Tabla 8.

No.	Descripción del requisito	Tipo de Control que Aplica
61	Verificar que las tecnologías de plantilla de codificación automática, si ésta se ha deshabilitado, asegurar que la sanitización de HTML esté habilitada en su lugar. *	Manejo de entrada de datos maliciosos
62	Verificar que la aplicación tenga herramientas de comprobación de integridad y evite la manipulación de datos.	Manejo de entrada de datos maliciosos
63	Comprobar que los datos de autenticación no se almacenen en el servidor y sean eliminados una vez terminada la sesión.	Manejo de entrada de datos maliciosos
64	Verificar la aplicación cuenta con configuración contra roturas para el cifrado o hash, logitud de clave.	Criptografía almacenada
65	Comprobar que la aplicación cuenta con metodos de autenticación de datos cifrados a traves de las firmas, cifrado autenticado, HMAC	Criptografía almacenada
66	Verificar que la aplicación no almacene claves y estas sean destruidas de forma segura una vez los usuarios sean desactivados de la herramienta.	Criptografía almacenada
67	Verificar que la aplicación use un modelo de seguridad para el almacenamiento de operaciones criptográficas.	Criptografía almacenada
68	Verificar que la aplicación cuente con módulos criptográficos y estos operen según sus políticas de seguridad de la entidad o sean parametrizables de acuerdo a las necesidades.	Criptografía almacenada
69	Verificar que en la aplicación todas las claves y contraseñas sean reemplazables al momento de realizar cambios.	Criptografía almacenada
70	Comprobar que la aplicación no almacene datos de tokens, contraseñas o hashes al momento de que se generen registros de error de uso.	Gestión y registro de errores
71	Verificar que los campos del registro de fuentes confiables y no confiables sean identificables en las entradas del registro.	Gestión y registro de errores
72	Comprobar que la aplicación cuente con registros de seguridad para el control de integridad que permita prevenir y proteger contra modificaciones no autorizadas.	Gestión y registro de errores
73	Verificar que la aplicación no registre y almacene datos confidenciales.	Gestión y registro de errores
74	Comprobar que la aplicación registra todas las acciones de control de acceso y acciones fallidas sobre el sistema.	Gestión y registro de errores
75	Comprobar que la aplicación garantiza la protección de los datos confidenciales almacenados en ella.	Protección de datos
76	Verificar que la aplicación registra anormalidades de solicitudes presentadas, y genera alertas de seguridad.	Protección de datos
77	Verificar la aplicación no usa información sensible que pueda ser envíada al servidor en el cuerpo o cabeceras del mensaje HTTP, o parametros.	Protección de datos

Continuación Tabla 8.

No.	Descripción del requisito	Tipo de Control que Aplica
78	Verificar que al realizar copias de seguridad de la información almacena en la aplicación, no guarde datos sensibles.	Protección de datos
79	Comprobar que la aplicación no almacene datos sensibles y confidenciales que estos no queden registrados y se objeto de exploración.	Protección de datos
80	Verificar que la aplicación tenga la capacidad para detectar y alertar sobre las anomalidades presentadas como solicitudes para la recolección de datos por medio captura de pantalla (screen scrapping).	Protección de datos
81	Verificar que la aplicación cuente con la cadena de confianza que utilice TLS entre esta y el servidor.	Seguridad de las Comunicaciones
82	Verificar que la aplicación utiliza y deja el registro de los fallos de conexiones TLS.	Seguridad de las Comunicaciones
83	Verificar que todas las conexiones a la aplicación de sistemas externos que involucran acciones o información sensible cuente con los mecanismos de autenticación.	Seguridad de las Comunicaciones
84	Comprobar que exista una sola implementación estándar de TLS utilizada por la aplicación.	Seguridad de las Comunicaciones
85	Comprobar que la aplicación utiliza únicamente algoritmos, cifradores y protocolos fuertes, a través de toda la cadena de confianza, incluyendo certificados raíz y certificados intermediarios de la autoridad certificadora seleccionada.	Seguridad de las Comunicaciones
86	Comprobar que se está utilizando una herramienta de análisis de código que puede detectar código potencialmente malintencionado, como funciones de tiempo, operaciones de archivos no seguras y conexiones de red.	Código malicioso
87	Verificar en la aplicación a través de busquedas que no exista código malicioso en las funcionalidades.	Código malicioso
88	Verificar que el código fuente de la aplicación no recopile información de los datos que almacena el sistema.	Código malicioso
89	Compruebe que la aplicación tiene alertas configurables y registra ataques automatizados o actividad inusual.	Lógica de negocio
90	Comprobar que la aplicación cuente con los mecanimos de protección para la verificación y validación de archivos comprimidos. (expedientes electrónicos)	Archivos y recursos
91	Verificar que la aplicación tenga escáneres y antivirus que permita verificar la recepción de los archivos y expedientes para evitar la carga de contenido malicioso.	Archivos y recursos
92	Comprobar que la aplicación cuente con un número determinado de tamaño y cantidad de archivos por usuario, para evitar llenar el almancenamiento permitido y conformación del expediente.	Archivos y recursos
93	Comprobar que los metadatos de los documentos esten validados de acuerdo al esquema de metados que este parametrizado en la herramienta.	Archivos y recursos

Continuación Tabla 8.

No.	Descripción del requisito	Tipo de Control que Aplica
94	Verificar que los metadatos de los documentos electrónicos almacenados en la herramienta esten protegidos contra inyección de comandos del sistema operativo.	Archivos y recursos
95	Verificar que la aplicación web tenga configurado mecanismos de autenticación y confianza para evitar las solicitades de carga datos o archivos no permitidos.	Archivos y recursos
96	Verificar la configuración por defecto para negar el acceso a recursos remotos o sistemas fuera del servidor web o de aplicación.	Archivos y recursos
97	Verificar que la aplicación utilice la misma codificación entre en el cliente como el servidor.	Verificación de API y servicio web
98	Verificar que el acceso a las funciones de administración y gestión de la aplicación proveedora del servicio sea limitado y únicamente a los administradores autorizados.	Verificación de API y servicio web
99	Verificar que la aplicación cuenta con los servicios web basados en SOAP y que estos son compatibles con el perfil básico de interoperabilidad de servicios Web.	Verificación de API y servicio web
100	Comprobar que las direcciones URL de la API no expongan información confidencial. Passwors, token's, acceso a documentos, firmas digitales.	Verificación de API y servicio web
101	Verificar que los servicios REST se encuentren protegidos de Falsificación de Peticiones en Sitos Cruzados (CSRF).	Verificación de API y servicio web
102	Verificar que no existen rutas de acceso alternativas y menos seguras para el acceso a la aplicación.	Verificación de API y servicio web
103	Verificar que los encabezados HTTP o cualquier parte de la respuesta HTTP no expongan información detallada de la versión de los componentes de la aplicación.*	Verificación de API y servicio web
104	Comprobar que todos los componentes de la aplicación esten actualizados a las configuraciones y versiones de seguridad adecuadas, y que no almacene información que contegan datos configuración y carpetas no requeridas.	Requisitos de Configuración
105	Verificar la seguridad de las comunicaciones entre componentes, tales como entre el servidor de aplicaciones y el servidor de base de datos, deberían ser cifradas, particularmente cuando los componentes están en diferentes contenedores o en sistemas diferentes.	Requisitos de Configuración
106	Comprobar que existan mecanismos de autenticación para la comunicación entre componentes del servidor de aplicaciones y el servidor de base de datos.	Requisitos de Configuración
107	Verificar que los despliegues de la aplicación se encuentren dentro de ambiente de pruebas, en otros contenedores para evitar o retrasar los posibles ataques de otras aplicaciones.	Requisitos de Configuración
108	Verificar que los procesos de compilación y despliegue de la aplicación se realizan de forma segura y no afecte la operación de la herramienta.	Requisitos de Configuración

Continuación Tabla 8.

No.	Descripción del requisito	Tipo de Control que Aplica
109	Verificar que los componentes de la aplicación proceden de repositorios de confianza y cuenta con mecanismo de seguridad para el servidor fuente.	Requisitos de Configuración
110	Comprobar que un encabezado X-Frame-Options o Content-Security-Policy: frame-ancestors está en uso para sitios donde el contenido no debe incrustarse en un sitio de terceros con el fin de prevenir ataques de clickjacking.	Requisitos de Configuración
111	Verificar que todos los recursos de la aplicación se encuentran alojados en la aplicación o repositorios digitales que mitiguen la perdida o robo de información.	Requisitos de Configuración
Fuente: propuesta de modelo de requisitos a partir de la revisión de la metodología OWASP de aplicaciones web para los sistemas de gestión documental de documentos electrónicos.		

El modelo de requisitos de seguridad es una propuesta que se realiza a partir de la documentación OWASP como los estándares de Sistemas de Gestión de Seguridad de la Información, también se tuvo en cuenta la guía Estándar de Verificación de Seguridad en Aplicaciones 4.0 y la identificación de las pruebas realizadas con la aplicación OWASP ZAP. Por lo cual, se presenta un listado de requerimientos de seguridad de las aplicaciones web para un gestor documental, y se alineo con los controles que son pertinentes para este tipo de sistemas.

La propuesta de modelo de requisitos de seguridad informática se conforma por un total de 111 puntos, los cuales están divididos 13 controles:

- Arquitectura, diseño y modelado de amenazas (11)
- Autenticación (16)
- Gestión de sesiones (10)
- Control de acceso (10)
- Manejo de entrada de datos maliciosos (16)
- Criptografía almacenada (6)
- Gestión y registro de errores (5)
- Protección de datos (6)
- Seguridad de las Comunicaciones (5)
- Código malicioso (3)
- Lógica de negocio (1)
- Archivos y recursos (7)
- Verificación de API y servicio web (7)
- Requisitos de Configuración (7)

Para algunos casos se tomo el requisito tal como lo menciona el Estándar de verificación de seguridad de aplicaciones web, que puede aplicar según con la descripción del OWASP, teniendo en cuenta las pruebas de seguridad realizadas en las aplicaciones de gestión documental ORFEO y OpenDocMac generaron un resultado de 12 y 13 vulnerabilidades en 7 tipos de riesgos. Lo cual indica que existen temas muy susceptibles en la seguridad de los expedientes electrónicos y que es necesario que el requisito sea verificado, comprobado y que el control debe ser aplicado como obligatorio para mitigar el riesgo.

CONCLUSIONES

Al realizar análisis de la documentación de las aplicaciones web para los sistemas de gestión de documentos electrónicos – SGDE y la documentación de los sistemas de seguridad de información – SGSI, el desarrollo de este trabajo permitió identificar que se requiere establecer controles efectivos que permitan mitigar posibles vulnerabilidades, las cuales es importante que las organizaciones y el área de sistemas tomen en cuenta, con el objetivo principal de garantizar la protección de la producción documental como primera fuente y principal activo de información que se genera desde las herramientas informáticas.

Este trabajo permitió realizar una exploración en las aplicaciones web de software libre destinadas para la administración de documentos electrónicos y digitales, con el fin de identificar a partir de la metodología OWASP las vulnerabilidades y ataques de seguridad de las cuales están expuestas y que se presenta de manera frecuente, para así proponer requisitos que permitan establecer sistemas seguros para la protección de información desde las aplicaciones.

Al definir los requisitos de seguridad informática basado en la metodología OWASP, se pudo identificar la necesidad que tienen las organizaciones para la adquisición de un software de gestión documental, en este sentido es importante que el sistema no solo cumpla los requisitos normativos y lineamientos archivísticos, si no que cuente con un modelo básico de requerimientos de seguridad de la información que permita garantizar que a pesar de ser una aplicación libre en ambiente web esta tenga los mecanismos suficientes que para el aseguramiento de la información.

La exploración de vulnerabilidades que tienen los sistemas de gestión de documentos electrónicos que se analizaron para el desarrollo de este proyecto, permitió identificar que de los 10 riesgos que están definidos en la metodología OWASP, de las veinticinco vulnerabilidades, se estaban asociados con la clasificación del top 10, estás aplicaciones son susceptibles en cuanto a seguridad, protección y preservación de la información. Este resultado indica que el nivel de impacto del software libre para las aplicaciones de este tipo presenta un alto riesgo en materia de seguridad. Por consiguiente, se debe garantizar y propender por un análisis profundo en cuanto a seguridad de la información y que a pesar de ser un software libre se debe reforzar, evaluar y controlar, desarrollando mecanismos que permitan garantizar la confiabilidad, integridad y confidencialidad en las herramientas que administran información en las diferentes organizaciones.

RECOMENDACIONES

Se recomienda al profesional de seguridad de información hacer el uso de diferentes herramientas que existen para realizar pruebas de fallas y vulnerabilidades en las aplicaciones web de software libre, con el fin de identificar y adaptar a las necesidades de la organización, para así mitigar los posibles riesgos y debilidades que se presenten en los sistemas destinados para la administración de documentos electrónicos.

A nivel de las entidades privadas y públicas, se invita que al momento de realizar los estudios para la adquisición de sistemas de gestión de documentos electrónicos – SGDE en aplicaciones web, se realice una mesa conjunta con el agente de seguridad de la información para que sean tenidos en cuenta los mecanismos necesarios para la protección de los activos de información, donde se pueda establecer requisitos mínimos que la herramienta debe cumplir, no solo citando la ISO 27000 y su derivación, concebida para la administración en ambiente web de forma segura para la organización.

Se sugiere tener en cuenta los hallazgos presentados en el desarrollo de este trabajo, donde se identifico las siete vulnerabilidades que presentan el software libre para los sistemas de gestión de documentos electrónicos, a fin de fortalecer y controlar las vulnerabilidades a partir generar mecanismos de seguridad, que permitan garantizar y mitigar riesgos de la información para la administran de este tipo de sistemas en las organizaciones.

Para finalizar, es importante que, si bien existe bastante documentación de metodologías, proyectos y mecanismos para seguridad de la información, es necesario que los mecanismos de seguridad sean adaptables a los tipos de sistemas que tiene la entidad. Los agentes de seguridad estén actualizados en la materia, que de manera periódica se realicen controles de seguridad, para así mitigar los posibles riesgos que presentan las aplicaciones, gestionar pruebas de escaneo y penetración para identificar la vulnerabilidad de las aplicaciones web con el fin de fortalecer y proteger de forma segura los documentos electrónicos de archivo de la organización.

BIBLIOGRAFÍA

ARCHIVO GENERAL DE LA NACIÓN. Guía implementación de un Sistema de Gestión de Documentos Electrónicos de Archivo. Bogotá: Archivo General de la Nación, 2019. 77 p. Disponible en Internet: <https://www.archivogeneral.gov.co/sites/default/files/Estructura_Web/5_Consulte/Recursos/Publicacionees/ImplementacionSGDEA.pdf>

_____. CONGRESO DE LA REPÚBLICA. Ley 594. (14, julio, 2000) Por la cual se dicta la Ley general de archivos y se dictan otras disposiciones. Diario Oficial Bogotá, D.C. 2000. 44084. p. 1.

_____. CONGRESO DE COLOMBIA. Ley 1437 de 2011 (18, enero, 2011) Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo. Bogotá D.C.: Congreso, 2011. 115 p. (Disponible en internet): <http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/ley143718012011.pdf >

_____. CONGRESO DE COLOMBIA. Ley 1273 de 2009 (5, enero, 2009) Por la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “De la protección de la información y de los datos”- y se preservan integralmente los sistemas utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Bogotá D.C.: Congreso, 2009. 4 p. (Disponible en internet): <https://mintic.gov.co/portal/604/articles-3705_documento.pdf>

_____. PRESIDENCIA DE LA REPUBLICA. Decreto 1080 de 2015. (26, mayo, 2015) Por el cual se expide el Decreto Único Reglamentario del Sector Cultura. Bogotá D.C.: Presidencia, 2015. 235 p.

_____. PRESIDENCIA DE LA REPUBLICA. Decreto 2609 de 2012. (14, diciembre, 2012) Por el cual se el Titulo V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado Colombiano. Bogotá D.C.: Presidencia, 2015. 16 p.

_____. PRESIDENCIA DE LA REPUBLICA. Decreto 0019 de 2012. (10, enero, 2012) Por el cual se dictan normas para suprimir o reformar regulaciones,

procedimientos y trámites innecesarios existentes en la Administración Pública. Bogotá D.C.: Presidencia, 2012. 89 p. (Disponible en internet): < http://wsp.presidencia.gov.co/Normativa/Decretos/2012/Documents/Enero/10/Dec1910012012.pdf>

_____. PRESIDENCIA DE LA REPUBLICA. Directiva Presidencial 04 de 2012. (3, abril, 2012) Eficiencia administrativa y lineamientos de la política cero papel en la administración pública. Bogotá D.C.: Presidencia, 2012. 3 p. (Disponible en internet): < https://www.mintic.gov.co/portal/604/articles-3647_documento.pdf>

CENTRO EUROPEO DE EMPRESAS E INNOVACIÓN. (2010) Sistema de gestión de seguridad de la información, ISO 27001: Formación SGSI. Disponible en: <http://www.ceeisec.com/nuevaweb/doc/FORMACION_SGSI_2010.pdf>

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS. Norma Técnica Colombiana. Sistema de Gestión de Seguridad de la Información. Bogotá, D.C.: ICONTEC, 2006. NTC_ISO/IEC 27001.

INTERNATIONAL STANDARS ORGANIZATION – ISO. ISO/IEC 17799:2002. Tecnología de la Información. Código de buenas prácticas para la Gestión de la Seguridad de la Información.

_____. ISO/IEC 17799:2005. Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información.

_____. ISO/IEC 27000. Tecnología de la Información – Técnicas de seguridad . Sistemas de Gestión de la Seguridad de La Información (SGSI).

_____. ISO/IEC 27002 Código de buenas prácticas para la gestión de seguridad de la información

FERRER, R. (s.f.) Sistema de gestión de la seguridad de la información (SGSI). Disponible en internet): <http://www.sisteseg.com/files/Microsoft_PowerPoint_-_Estrategias_de_seguridad_v52.pdf>

NTC- ISO 16175-1 Información y documentación. Principios y requisitos funcionales para los registros en entornos electrónicos de oficina. Parte 1: información general y declaración de principios. (Disponible en internet): <http://sigme.superservicios.gov.co/sigme-calidad/CALIDAD/NORMOGRAMA/NORMA/NTC_ISO_16175.pdf>

NTC ISO/IEC 16175-2 Principios y requisitos funcionales para los registros en entornos electrónicos de oficina.

OWASP FOUNDATION. OWASP Top 10 – 2017: Los diez riesgos más críticos en aplicaciones web. California: OWASP, 2017. 25 p. (Disponible en internet): <https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_Top_10

_____. Guía de pruebas OWASP Versión 3.0. California: OWASP, 2008. 371 p. (Disponible en internet): < https://owasp.org/www-pdf-archive/Gu%C3%ADa_de_pruebas_de_OWASP_ver_3.0.pdf>

_____. Estándar de Verificación de Seguridad en Aplicaciones 3.0.1. California: OWASP, 2017. 75 p. (Disponible en internet): <https://owasp.org/www-pdf-archive/Est%C3%A1ndar_de_Verificaci%C3%B3n_de_Seguridad_en_Aplicaciones_3.0.1.pdf>

_____. OWASP Application Security Verification Standard (ASVS) 4.0. California: OWASP, 2019. 68 p. (Disponible en internet): <https://owasp.org/www-project-application-security-verification-standard/>

_____. Guía de revisión de código OWASP 1.0 California: OWASP, 2007. P. (Disponible en internet): <http://www.owasp.org/index.php/Category:OWASP_Code_Review_Project>

_____. OWASP ZAP Desktop user guide. California: OWASP, 2020. P. (Disponible en internet): <https://www.zaproxy.org/docs/desktop/>

UNIÓN EUROPEA. SECRETARIADO FUNDACIÓN DML FORUM. Modelo de Requisitos para la gestión de documentos electrónicos de archivo. Bruselas: Unión, 2001. (Disponible en internet): <

UNIVERSIDAD POLITECNICA SALECIANA SEDE CUENCA. Auditoría de seguridad informática ISO 27001 para la empresa de alimentos “Italimentos CIA. LTDA”. Ecuador: Universidad, 2011. (Disponible en internet) : <http://dspace.ups.edu.ec/bitstream/123456789/2644/16/UPS-CT002441.pdf>

REVISTA ESPAÑOLA DE DOCUMENTACIÓN CIENTÍFICA. Procesos de gestión de documentos. Metadatos para la gestión de documentos. Parte 2: Aspectos conceptuales y de implementación. ISO 23081-2. España: Revista, 2008. (Disponible en internet): < https://www.uma.es/media/tinyimages/file/ISO.23081.Parte_2.pdf>