CARRERA DE ANÁLISIS DE SISTEMAS

TEMA:

"PROPUESTA DE MANUAL DE SEGURIDAD BASADO EN LA NORMA ISO/IEC 27034 PARA EL DESARROLLO DE PÁGINAS WEB"

AUTOR:

MENDOZA DÁVILA YAJAIRA ELIZABETH.

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

TECNÓLOGO EN ANÁLISIS DE SISTEMAS

TUTORES:

• MGS. GALO HURTADO

CUENCA – ECUADOR, 2019

DICTAMEN DE ACEPTACIÓN DEL TRABAJO.

RESUMEN.

El significado de seguridad se ha ampliado con el tiempo, por el desarrollo de nuevos sistemas tecnológicos de información, protegiendo la confidencialidad y el proceso de la información, los mismo que se han convertido en estrategias que garantizan la seguridad de las páginas web, y también las de las empresas.

Para poder minimizar estos problemas de seguridad, las empresas deben desarrollar un plan de seguridad que ayuden a detectar las vulnerabilidades de la página web, uno de estos es la norma ISO/IEC 27034, la cual es una guía importante para proteger la información.

Para la actualidad en la ciudad de Cuenca se investigó tres empresas, viendo si al momento de desarrollar páginas web, se implementa el buen funcionamiento del CID en los sistemas informáticos, y saber si aplican la norma ISO/IEC 27034, siguiendo pasos para revisar la seguridad de páginas web con el objetivo de ayudar a los procesos comerciales que tienen, mediante las investigaciones se dio a conocer que las empresas tienen algunos problemas de seguridad, incluyendo vulnerabilidades y ataques lo que puede llevar a una filtración de información importante del usuario.

En este trabajo se propone un manual de seguridad para páginas web, el cual ayuda a garantizar que una página web cumpla con los requisitos requeridos para tener un desarrollo correcto, el cual tiene como objetivo final determinar si una página web cumple los pasos de seguridad necesarios que impone la norma ISO/IEC 27034.

ABSTRACT.

The meaning of security has expanded over time, due to the development of new technological information systems, protecting confidentiality and the information process, which have become strategies that control the security of web pages, and also those of the companies.

In order to minimize these security problems, companies must develop a security plan that helps detect vulnerabilities on the website, one of these is the ISO / IEC 27034 standard, which is an important guide to protect information.

For the present in the city of Cuenca, investigate three companies, see if the time to develop web pages, implement the proper functioning of the CID in computer systems, and know if it develops the ISO / IEC 27034 standard, following the steps to analyze the Web page security in order to help the commercial processes they have, through investigations it was announced that companies have some security problems, including vulnerabilities and attacks, which can lead to a leak of important user information.

This paper proposes a security manual for web pages, which helps determine that a web page meets the requirements required to have a correct development, which aims to determine if a web page meets the necessary security steps which imposes the ISO / IEC 27034 standard.

PALABRAS CLAVE.

Implementación, seguridad, información, riesgo, análisis.

KEY WORDS.

Implementation, security, information, risk, analysis.

DEDICATORIAS.

Dedico este trabajo de titulación a mi madre, por ser mi mejor amiga, consejera y ejemplo a seguir, por ser la persona más importante y darme siempre su cariño y apoyo incondicional sin importar nuestras diferencias de opiniones.

A mi padre, que a pesar de la distancia física que tenemos, me apoyo para poder formarme como profesional y aunque nos faltan muchas cosas por vivir, sé que este momento es tan especial para él como lo es para mí.

A mis hermanos, por compartir momentos muy emotivos conmigo y porque siempre estaban dispuestos a escucharme y ayudarme.

De igual manera, agradezco a mi tutor el MGS. Galo Hurtado, quien confió en mi capacidad y entrega para seguir adelante, y con paciencia, conocimientos y correcciones, hoy puedo terminar este trabajo.

INDICE GENERAL.

INDICE DE IMAGENES.

INDICE DE TABLAS.

INTRODUCCIÓN.

En la actualidad la tecnología de información ha impactado directamente a la seguridad de la información y se ha permitido el desarrollo de páginas web innovadoras, las que se han convertido en las más utilizadas e importante en la sociedad. Debido a que permite comunicar y compartir información en tiempo real entre usuarios finales, tanto a nivel laboral además del personal.

A medida que el software se convierte en algo completo, el riesgo de no descubrir vulnerabilidades de forma rápida y precisa en las páginas web aumenta, para identificar los riesgos se ha utilizado OWASP, su principal objetivo es dar a conocer sobre las consecuencias de las debilidades más comunes e importantes de las seguridades de las páginas web, proporcionando técnicas básicas para protegerse contra las áreas con problemas de alto riesgo.

Con el fin de precautelar la información de los usuarios, La organización Internacional de Normalización (ISO) publicó ISO/IEC 27034, que consiste en técnicas de seguridad de administración de información para aplicaciones con el fin de proteger la información que se maneja y llegar a tener el nivel deseado o adecuado de funcionamiento de las mismas. (ISO 27000.es, 2019)

Por este motivo se genera una Propuesta de manual de seguridad basado en la norma ISO/IEC 27034 para el desarrollo de páginas web, con la finalidad de ayudar a minimizar los riesgos y a establecer pasos requeridos para que se cumpla esta norma al momento de desarrollar páginas web, tomando en cuenta que en las investigaciones realizadas se ha visto que las empresas solo se adaptan a las necesidades del cliente, sin implementar la debida seguridad que necesitan las páginas webs realizadas.

En el presente proyecto se realizó la debida investigación para poder general la Propuesta de manual de seguridad basado en la norma ISO/IEC 27034 para el desarrollo de páginas web.

OBJETIVOS DE LA INVESTIGACIÓN.

OBJETIVO GENERAL.

Realizar un manual técnico de seguridad utilizando el estándar ISO/IEC 27034, para la validación y corrección de vulnerabilidades de las páginas web.

OBJETIVOS ESPECÍFICOS.

- Realizar un análisis de las vulnerabilidades de páginas web por medio de OWASP.
- Determinar los tipos más comunes de vulnerabilidades en páginas web.
- Elabora una guía de buenas prácticas para la seguridad en páginas web.

PREGUNTAS DE LA INVESTIGACIÓN.

¿Qué tipo de metodología utiliza para el desarrollo de páginas web, la ágil o la predictiva?

¿Cuáles son las páginas web más solicitadas?

¿Cuáles son las vulnerabilidades más frecuentes halladas en el desarrollo de las páginas webs?

¿Qué medidas tomaría ante un ataque?

¿Cuáles son los pasos que sigue a la hora de desarrollar una página web?

JUSTIFICACIÓN.

Al desarrollar una página web se debe considerar el impacto que generaría hacia su información, usuarios, recursos TI, los desarrolladores deben ser conscientes de los riesgos y las vulnerabilidades que implicaría dicha acción. Para poder reducir los riesgos, los desarrolladores deben probar el nivel de confianza, que se ofrece al usuario.

Por lo tanto, se ve la facilidad de realizar un manual de seguridad para aplicaciones web, con el fin de proporcionar confiabilidad a los usuarios mediante pruebas realizadas en Owasp. Basados en la norma ISO/IEC 27034, en la cual indica definiciones, técnicas, validaciones y control de seguridad para páginas web, la cual permitirá reducir los riesgos de la información de los usuarios.

CAPITULO I.

1. PROBLEMÁTICA.

En algunos casos los desarrolladores le restan importancia a la seguridad que ofrecen al momento de desarrollar páginas web, porque solo se enfocan en lo que el cliente pide y en lo rápido que puedan entregar, no consideran las normas de seguridad necesarias que se deben tener al momento de desarrollar una página web.

Con el fin de proteger la información de los usuarios, la ISO/IEC 27034, desea proteger la información que se utiliza y poder llegar a tener el nivel adecuado de funcionamiento, generando debidos procesos a seguir para tener la seguridad necesaria en el desarrollo de páginas webs.

CAPÍTULO II.

2. MARCO REFERENCIAL.

1.1.MARCO TEORICO.

5.1.1 ¿Qué es un activo?

Los activos son los componentes más importantes, como el hardware, software y base de datos, deben ser protegidos para el buen funcionamiento de un sistema informático, caso contrario se podrían ocasionar fallos en el sistema informático, las personas que se encargan en proteger los activos tienen que identificar, definir y valorar todos los activos. (SGSI, 2015)

5.2.1 Definición de ataque.

Un ataque, es un daño o problema en un sistema, se realiza mediante las fallas que se encuentren en el software o hardware, para obtener beneficios económicos afectando los activos con la propagación de virus que pueden dañar o eliminar datos. (Lucia D'Adamo, 2017)

Hay varios tipos de ataques, entre los más reconocidos están los siguientes.

2.1.2.1 Cross-Site Scripting.

Cross-Site Scripting, es un tipo de vulnerabilidad de seguridad informática encontrada en aplicaciones web, permite la inyección de código por usuarios maliciosos, las fallas que permiten que estos ataques tengan éxito están bastante extendidas y ocurren en cualquier lugar donde una aplicación web utiliza la entrada de un usuario sin validarla o codificarla.

Debido a que se cree que el script proviene de una fuente confiable, el script malicioso puede acceder a cualquier cookie, tokens de sesión u otra información confidencial, estas secuencias de comando pueden incluso reescribir el contenido de la página HTML. (MDN, 2019)

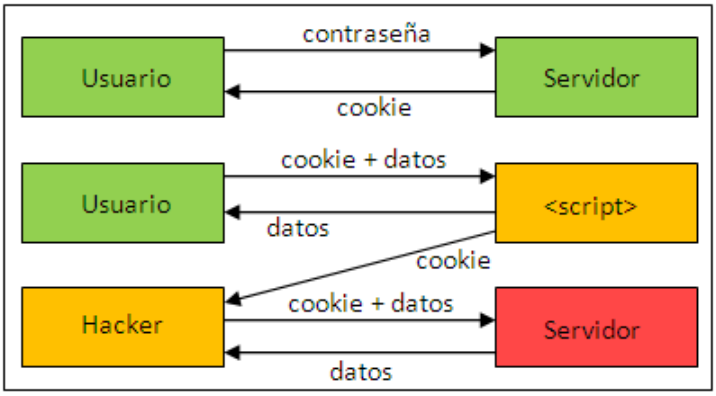


Imagen 1 Operación de un ataque

Fuente: (Domínguez, 2015)

2.1.2.2 Inyección SQL.

El ataque de tipo SQL, inyecta códigos para determinar las vulnerabilidades, se colocan sentencias SQL maliciosas que se inyectan en los campos de entrada del usuario, permitiendo el acceso al contenido de la base de datos. (MDN, 2019)

2.1.2.3 Broken Access Control.

Los errores en la configuración de los sistemas de control de acceso pueden permitir a un atacante acceder de forma no autorizada a datos y archivos para los que no debería tener permiso.

Las restricciones de control de acceso indican que los usuarios solo pueden actuar bajo los permisos previstos, si un usuario no aprobado puede acceder a cualquier página, significa que esto es una falla. (OWASP, 2017)

2.1.2.4 Insufficient Logging & Monitoring.

Debido al monitoreo insuficiente, y la falta de respuesta ante incidentes, que suele tardar hasta 200 días en detectar una vulnerabilidad, los atacantes manipulan, extraen y destruyen

datos, si el tiempo se pudiera reducir se configurarían mayores controles con mejor monitorización.

Para evitar este riesgo se debe asegurar que todos los errores de inicio de sesión, de control de acceso y validación de datos se registren desde el servidor para así poder realizar un análisis forense ante cualquier riesgo. (OWASP, 2017)

5.3.1 Definición de vulnerabilidad.

Una vulnerabilidad es una debilidad en la seguridad de un sistema informático, la cual coloca en peligro la confidencialidad y veracidad de la información; se pueden producir por el mal diseño de un software, y se siguen encontrando problemas constantes en la seguridad de los sistemas, suelen quedar expuestos, dejando que muchos hackers y ciberdelincuentes se aprovechen. (INCIBE, 2017)

5.4.1 ¿Qué es un riesgo?

Un riesgo es un fallo en el cumplimiento de un objetivo, que genera consecuencias de perdida hacia la empresa, generalmente se plantea como amenaza cuando el grado de perdida es alto, para saber la dificultad que tiene, se recomienda realizar un análisis de riesgo. (SGSI, 2019)

5.5.1 Análisis de riesgo en la seguridad de las aplicaciones.

El análisis de riesgos es la actividad que permitirá determinar cuán comprometido está un activo. El principal objetivo es proveer la información necesaria para tomar las decisiones sobre qué debe protegerse, ¿de qué? y ¿cómo?

Es conveniente emplear medidas de seguridad que ayuden a los usuarios a entender, que mientras más compleja sea la aplicación web, aumentara el riesgo de que se sufra un ataque, es por eso se debe considerar opciones de seguridad sencillas pero eficientes que ayuden a eliminar cualquier vulnerabilidad. (OWASP, 2017)

5.6.1 Estrategias de evitación de la gestión de riesgos.

Una vez analizado los riesgos, se debe identificar las amenazas y los beneficios, eligiendo la estrategia de evitación de riesgo más adecuada. Existen cuatro estrategias que abordan los riesgos que pueden tener consecuencias negativas sobre los objetivos del proyecto, y son:

- **Evitar:** seleccionar medios alternativos que logren el mismo resultado con cambios significativos por mejoramiento y así eliminar el riesgo.
- **Transferir:** se refiere a transferir el riesgo de un lugar a otro, pero no lo elimina
- **Mitigar:** busca reducir la existencia de un riesgo por medio de controles de gestión, y procedimientos que reduzcan la existencia de un error.
- **Aceptar:** reducir el impacto de los riesgos o no hacer nada y dejar el riesgo identificado.

Según (Barà, 2019), las estrategias de evitar, mitigar y transferir, son eficaces para riesgos críticos de magnitud alta, mientras que la estrategia aceptar es buena para amenazas menos críticas y con menos impacto.

5.7.1 Fundación de OWASP.

La Fundación OWASP inicio el 1 de diciembre de 2001, se estableció como una organización sin fines de lucro en los Estados Unidos el 21 de abril de 2004, dedicada a permitir a lar organizaciones concebir, desarrollar, adquirir, operar y mantener aplicaciones en las que se pueda confiar. La Fundación OWASP es una entidad sin fines de lucro que garantiza el éxito a largo plazo del proyecto. (OWASP, 2019)

Todas las herramientas y documentos de OWASP son gratuitos y están abiertos a cualquier persona interesada en mejorar la seguridad de las aplicaciones, OWASP no está afiliado a ninguna compañía de tecnología y produce muchos tipos de materiales.

5.8.1 Definición de OWASP.

OWASP (proyecto abierto de seguridad en aplicaciones Web) es una comunidad abierta dedicada a mantener aplicaciones confiables. Todas la herramientas, documentos, foros y

capítulos de OWASP son gratuitos y ayudan a resolver la seguridad de aplicaciones como un problema de gente, procesos y tecnología. (OWASP, 2014)

Imagen 2 OWASP

Fuente: (OWASP, 2019)

5.9.1 CID.

Considerados como los tres principios de la seguridad, que se encuentran relacionados con la seguridad, cada riesgo que se mitiga es desde la perspectiva de la CID

Imagen 3 CID

Fuente: (Guazaman, 2016)

2.1.9.1 Confidencialidad.

Se refiere a que la información solo debe llegar a la persona correcta, la perdida de confidencialidad puede llevar efectos negativos, se puede implementar controles físicos, técnicos y procesos que restrinjan el acceso.

Se puede usar diversos controles para la protección, como la encriptación, identificación, autorización y autenticación.

2.1.9.2 Integridad.

Se encarga de proteger la información de cambios ya sean intencionales o accidentales, se debe confiar en que la información es precisa y que no fue manipulada de manera no autorizada, ya que en el momento en que se altera la información, se pierde la credibilidad, lo cual nos puede dar documentos con errores.

Los controles de seguridad como lo es un criptográfico puede proteger la integridad de la información.

2.1.9.3 Disponibilidad.

Consiste en que la información y los recursos relacionados estén disponible para los usuarios autorizados cuando lo requieran, incluso en momentos de emergencia o alto tráfico.

Garantizar la disponibilidad de la información es de vital importancia en el proceso de la búsqueda de la seguridad informática, esta se refiere a que una vez que nos aseguramos que la información está correcta y llega a los usuarios adecuados, la información debe de llegar en el momento oportuno.

2.1.MARCO CONCEPTUAL.

2.2.1 Definición de Seguridad de información.

La información o base de datos de una empresa, es el activo más importante, se puede definir a la seguridad de la información como el fin de protección de la información con medidas preventivas para evitar la divulgación, destrucción no autorizada de la misma. (SGSI , 2017)

2.2.2 Introducción a la seguridad en páginas web.

Los desarrolladores deben tener en cuenta los riesgos y de las vulnerabilidades que se generan al desarrollar una página web. Para minimizar riesgos, debería demostrar que la página web este mayormente sin vulnerabilidades.

Según (Ogata, Franklin, Voas, Sritapan, & Stephen, 2015) mencionan que los avances de la tecnología se generan que también existan nuevas vulnerabilidades. Las organizaciones deben desarrollar requisitos que especifiquen como deben protege los datos según el entorno en el cual se desarrolla.

2.2.3 Definición Norma ISO 27001.

ISO 27001, es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan, permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para eliminarlos.

La aplicación de ISO-27001 mejora la competitividad y la imagen de una organización, el cumplimiento de los requerimientos de esta norma, permite que una organización pueda obtener la certificación internacional. (ISOTools, 2019)

2.2.4 Introducción Estándar ISO/IEC 27034.

ISO/IEC 27034, es un estándar desarrollado por sistema especializado de norma mundial conformado por ISO. La misma que establece una guía sobre seguridad de la información enfocados a aplicaciones, dirigidas a administradores TI, desarrolladores o usuarios.

En la mencionada guía proporciona orientación sobre diseño, programación, implementación de controles de seguridad de la información a través de un conjunto de procesos integrados y orientados. (ISO 27000.es, 2019)

2.2.5 Estructura de ISO/IEC 27034.

ISO/IEC 27034, implementa controles de seguridad de la información mediante procesos, los cuales se detallan a continuación:

Tabla 1

Estructura de ISO/IEC 27034.

PROCESO.	DETALLE.
ISO/IEC 27034-1: 2011 Descripción y conceptos.	Seguridad de la aplicación, con definiciones, conceptos, principios y procesos involucrados. Define un nivel de confianza para diseñar una aplicación y luego validarla.
ISO/IEC 27034-2: 2015 Marco normativo de la organización.	Explicación del Marco Normativo de la Organización, sus componentes y procesos para poder gestionarlo. Se detalla las relaciones entre procesos y actividades que apoyan la gestión de seguridad de la aplicación.

ISO/IEC 27034-3: 2018 Proceso de gestión de seguridad de aplicaciones.	Determina los requisitos y el entorno de la aplicación, evaluando los riesgos de seguridad. Opera la aplicación y valida la seguridad, explicando las relaciones entre los procesos.
ISO/IEC 27034-5: 2017 Protocolos y estructura de datos de control de seguridad de la aplicación.	Ayuda a las organizaciones a validar y actualizar la estructura de atributos esenciales y el ciclo de vida del CSA.
ISO/IEC 27034-5-1: 2018 Estructura de datos de protocolos y control de seguridad de la aplicación, esquemas XML.	Implementa protocolos y esquemas XML para el CSA y determina como se debe utilizar la información en el desarrollo de software.
ISO/IEC 27034-6: 2016 Estudios de casos.	Proporciona ejemplos del desarrollo de los CSA, y adaptar a los requisitos específicos de aplicaciones.
ISO/IEC 27034-7: 2018 Marco de predicción de aseguramiento.	Ofrece la seguridad necesaria al momento de realizar funciones de seguridad. El CSA asignado a un PAR define el nivel de confianza para una aplicación, y es aplicable a los equipos que tienen definido un Marco de Referencia Normativo.

Fuente: (ISO/IEC 27034, 2018)

CAPÍTULO III.

3. METODOLÓGIA. DE LA INVESTIGACIÓN.

3.1.METODOLOGÍA USADA.

Se realizará una investigación exploratoria con el objetivo de obtener información y determinar los aspectos más importantes que se necesitan para la elaboración del manual de seguridad basado en la norma ISO/IEC 27034.

Mediante una exhaustiva investigación sobre el tema con el método deductivo, se realizarán entrevistas y pruebas de las páginas webs mediante el programa OWASP para poder realizar un análisis de vulnerabilidades y después de varias pruebas poder desarrollar el manual de seguridad.

Se utilizará una metodología cuantitativa, basado en el método deductivo, para permitir una medición del porcentaje de riesgo que tienen las páginas webs desarrolladas por las empresas entrevistadas, permitiendo un mayor nivel de control y obtener soluciones basadas en la norma ISO/IEC 27034.

Tabla 2

Comparación de las ISO relacionadas con la ISO 27034.

ISO/IEC 27034-3 (2018)	ISO/IEC 27034-5 (2017)
Es el proceso de gestión de seguridad de aplicaciones.	Son los protocolos y estructura de datos de control de seguridad de la aplicación.
Determina los requisitos y el entorno de la aplicación, evaluando los riesgos de seguridad.	Proporciona requisitos, representaciones gráficas y esquemas XML para el modelo de datos. Ayuda a las organizaciones a validar y actualizar la estructura de atributos esenciales y el ciclo de vida del CSA.
Proceso general para administrar la seguridad en cada aplicación específica y valida la seguridad, explicando las relaciones entre los procesos.	

Fuente: (Autor propio)

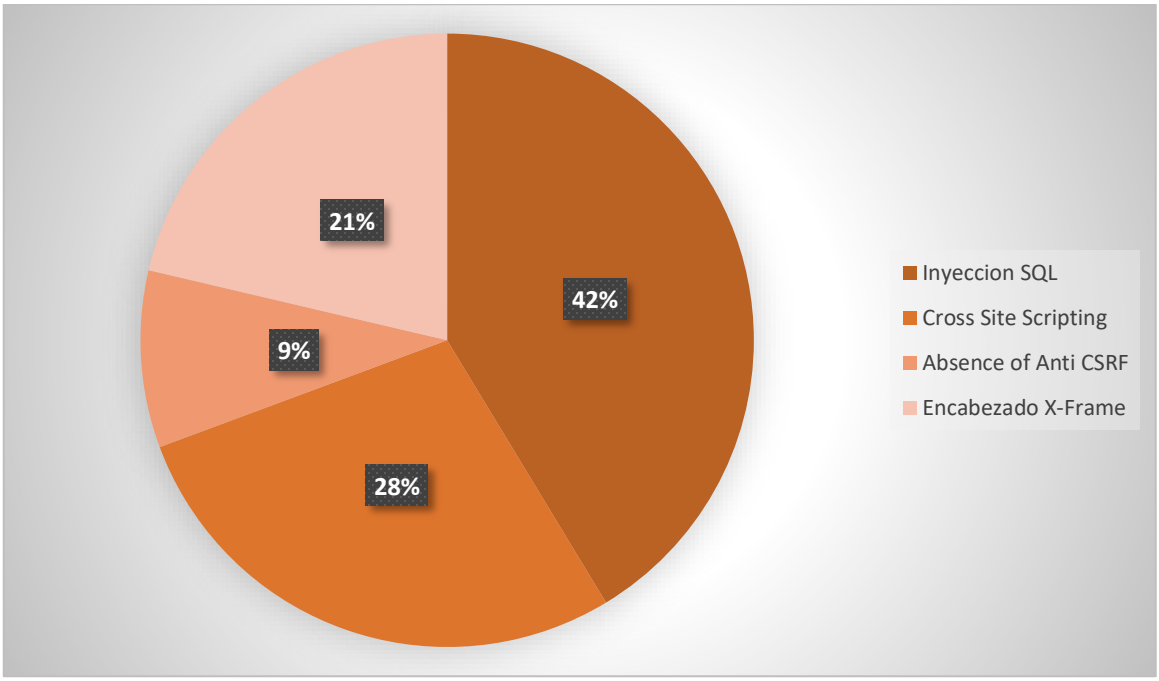


Imagen 4 Vulnerabilidades más frecuentes en páginas web probadas.

Fuente: (Autor propio)

- **Inyección SQL (42%),** esta vulnerabilidad permite al atacante, enviar petiviones en lenguaje SQL, el cual permite tener acceso a la base de datos, permitiendo ejecutar acciones privilegiadas para hacer o deshacer en la base de datos.
- **Cross-Site scripting (28%),** es un tipo de vulnerabilidad, que puede permitir a personas inyectar código JavaScript o cualquier otro lenguaje similar, teniendo acceso a su información e incluso ejecutando otros ataques en su nombre.
- **Encabezado X-Frame,-Ootions** puede ser usado para evitar ataques clickjacking, asegurándose que el contenido no esta conectado con otros sitios.
- **Absence of Anti CRF Tokens,** este ataque envía una petición a una página web vulnerable, y abusa de la confianza entre el navegador y el servidor, ataca mediante formularios web, apoderándose de la información.

3.2.INSTRUMENTOS DE INVESTIGACIÓN.

Los instrumentos que se utilizaron para la investigación fueron:

- Documentos.
- Internet.
- Manuales técnicos.

CAPÍTULO IV.

4. ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS.

4.1.LEVANTAMIENTO DE INFORMACIÓN.

Se realizó un análisis actual de páginas web, entre estas, se encuentras tres páginas web de empresas en concretos como lo son: “RIVERMIND”, “SONEXT” y “MYCODEDMIND”, dedicadas al desarrollo de páginas web.

Para analizar las vulnerabilidades de las páginas web se instaló la aplicación OWASP ZAP, que se dedica a identificar vulnerabilidades y clasificarlas dependiendo el nivel de riesgo.

Tabla 3

Cumplimiento del Marco Normativo

MARCO NORMATIVO.	SONEXT	RIVERMINDS	MYCODEDMINDS
Contexto empresarial,	**X**	**X**	**X**
Contexto regulatorio.			
Contexto tecnológico.		**X**	**X**
Especificaciones de aplicaciones y repositorios de funcionalidades.			
Repositorios de roles, responsabilidades y calificaciones.	**X**	**X**	**X**
Controles de seguridad de aplicaciones.			**X**
Biblioteca de los controles de seguridad de aplicaciones.			
Matriz de trazabilidad de seguridad de aplicaciones.			
Modelo de referencia del ciclo de vida de seguridad de la aplicación.		**X**	**X**
Modelo de ciclo de vida de seguridad de la aplicación.			
Marcos normativos de la aplicación.			

La organización del marco normativo del comité de gestión.			
La gestión de la organización del marco normativo.			
La gestión de riesgos de seguridad de aplicaciones.			
La gestión de seguridad de aplicaciones.			
La conformidad de seguridad de la aplicación.	**X**	**X**	**X**

Fuente: (Autor propio)

Revisando la prueba y la entrevista realizadas a las empresas se puede asumir que las empresas en cuestión no poseen.

- Análisis de vulnerabilidades.
- Control de Vulnerabilidades documentadas.
- Políticas documentadas relacionada a la seguridad de la información, para garantizar la confidencialidad, Integridad y Disponibilidad.
- Control de acceso.
- Pasos a seguir para el control de riesgos.

4.1.ANÁLISIS DE LA SITUACION ACTUAL.

Para la verificación de la metodología se realizó un análisis actual a tres empresas que se dedican al desarrollo de páginas webs, siendo estas las siguientes.

4.2.1. RIVERMINDS.

A un desarrollador de la empresa pequeña tecnológica “RIVERMINDS”, que cuenta con 7 empleados y se encarga del desarrollo e implementación de soluciones informáticas, se le realizo una entrevista para poder descubrir los pasos que sigue al momento de desarrollar una página web, una vez recopilada la información nos dio el siguiente diagrama.

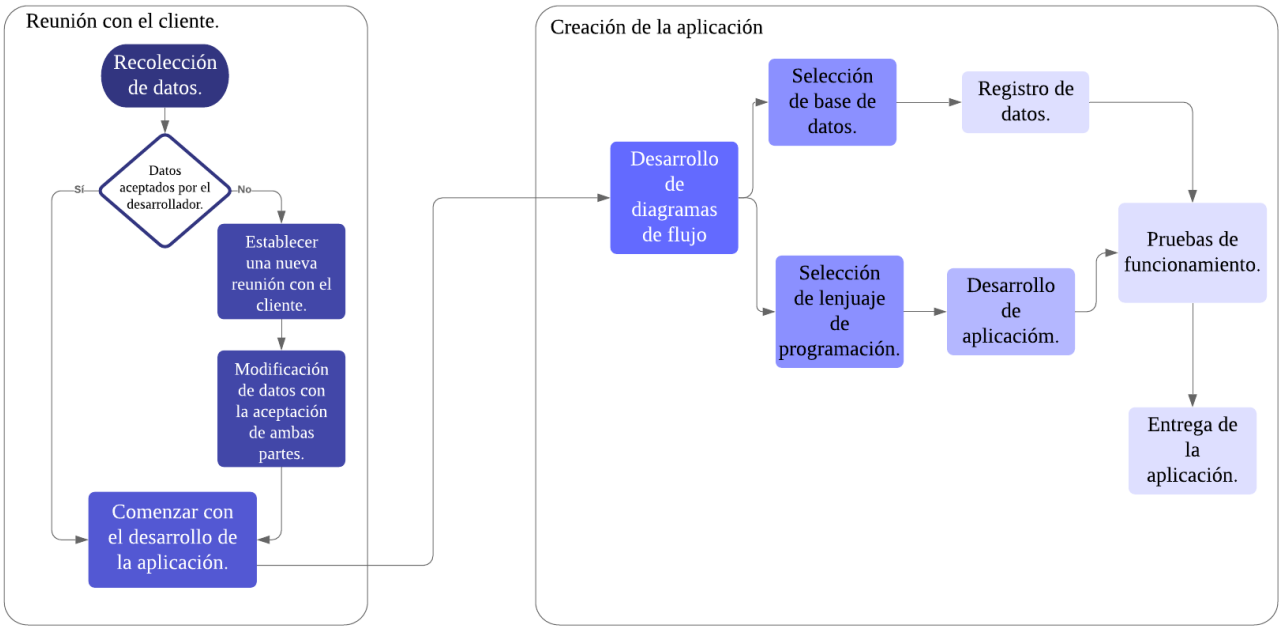


Imagen 5 Diagrama de la empresa RIVERMINDS

Fuente: (Autor propio)

También se realizó pruebas de vulnerabilidades a la página web de la empresa, dándonos como resultado 2 riesgos de alto nivel, 1 riesgo de nivel medio y 6 de bajo nivel.

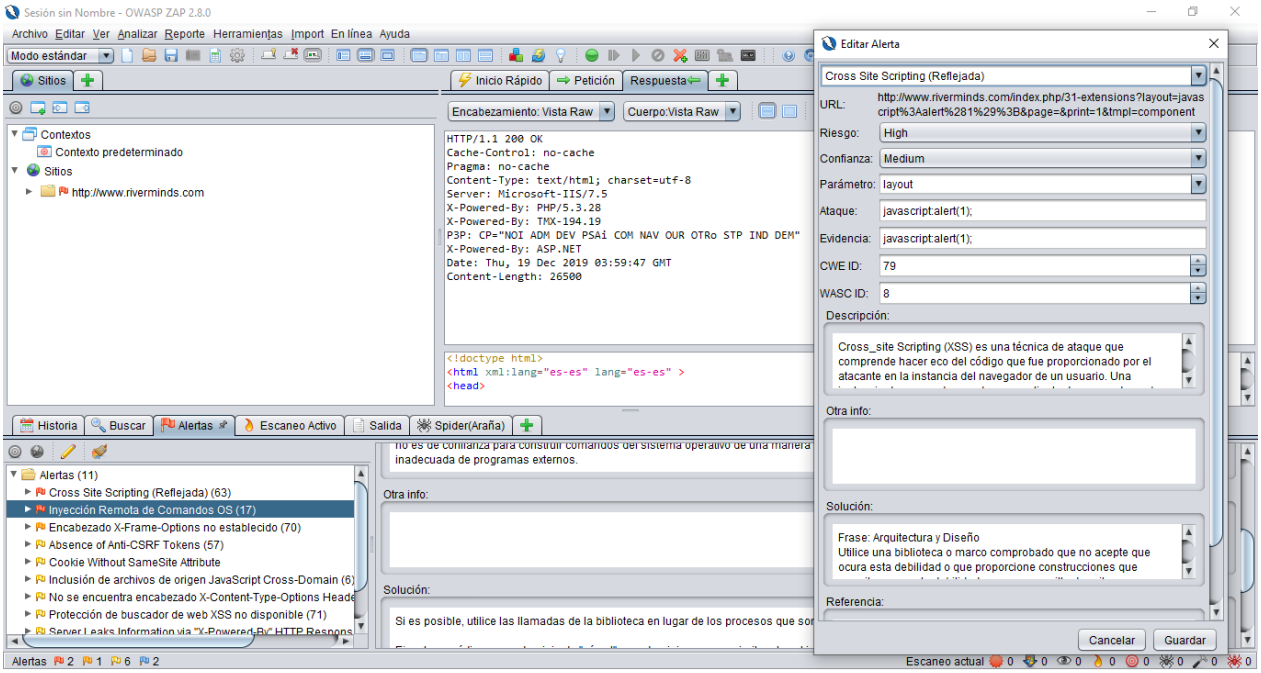


Imagen 6 Análisis de vulnerabilidades de la página web de RIVERMINDS.

Fuente: (Autor propio)

Al observar que la página web de la empresa RIVERMINDS, tiene 2 riesgos de vulnerabilidades de alto nivel, y su vez es la página que tiene más riesgos de las tres que se analizaron, por esta razón se llegó a la conclusión que es una página muy propensa a sufrir ataques maliciosos.

4.2.2. SONEXT.

Esta empresa es pequeña y se encarga del desarrollo de páginas y aplicaciones web, por medio de los datos recolectados se pudo descubrir los pasos que siguen al momento de desarrollar una página web.

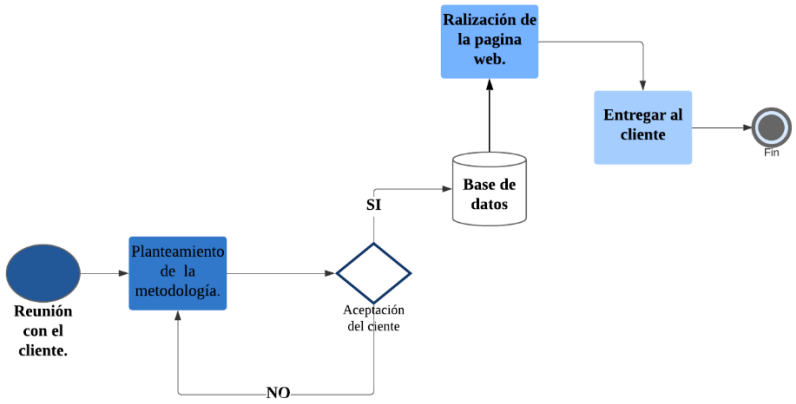


Imagen 7 Diagrama de la empresa SONEXT

Fuente: (Autor propio)

Se realizó pruebas de vulnerabilidades a la página web de la empresa, dándonos como resultado 2 riesgos de nivel medio y 6 riesgos de bajo nivel.

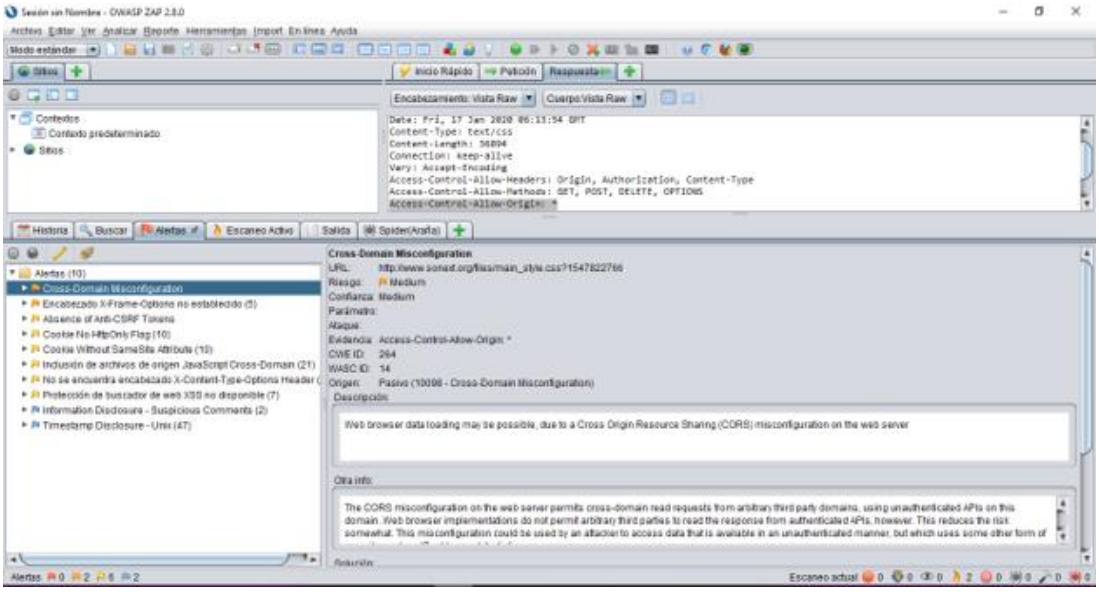


Imagen 8 Análisis de vulnerabilidades de la página web de SONEXT.

Fuente: (Autor propio)

4.2.3. MYCODEDMIND

La empresa MyCodedMind cuenta con 10 empleados, siendo una empresa pequeña, la cual brinda servicios integrales de comunicaciones corporativas y publicitarias en medios digitales, se pudo realizar un diagrama, en el cual se observa el procedimiento que siguen en el momento en que desarrollan una página web.

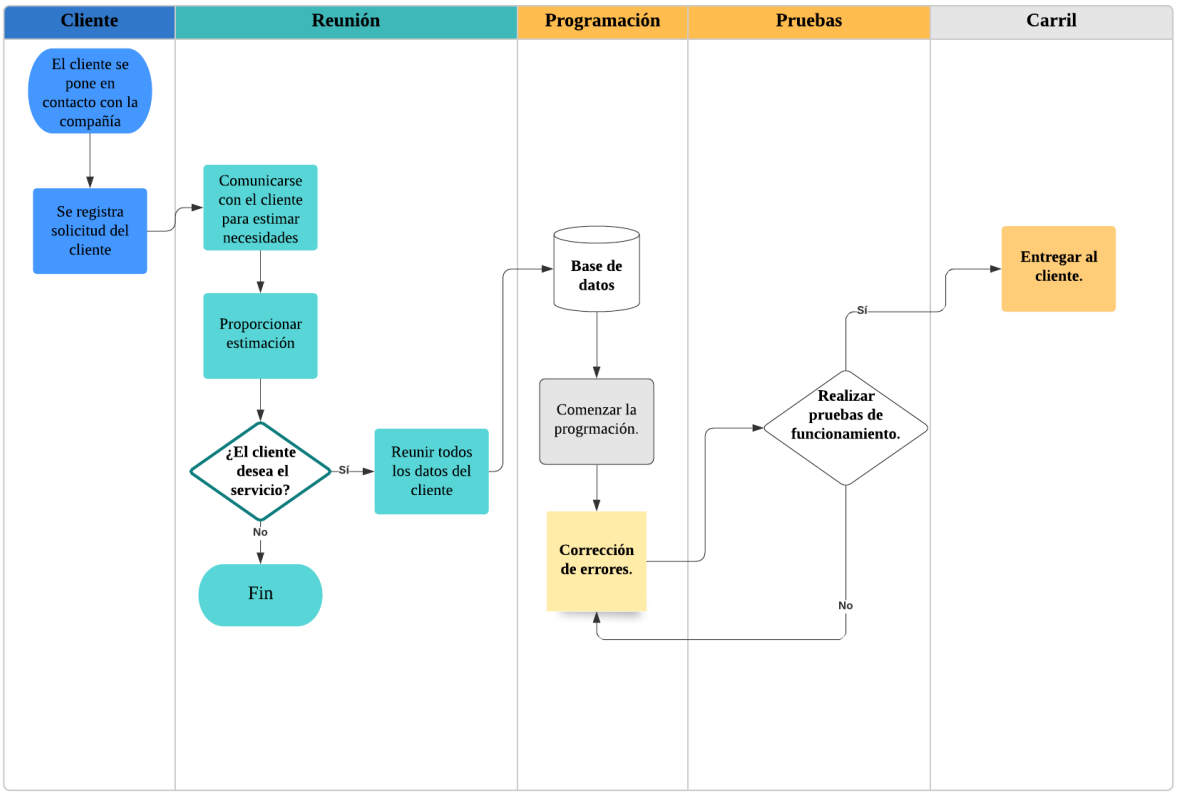


Imagen 9 Diagrama de la empresa MYCODEDMIND.

Fuente: (Autor propio)

Esta fue la última empresa a la que se le realizaron pruebas de vulnerabilidad en la aplicación de OWASP ZAP, y fue la página con menos riesgos de vulnerabilidad, ya que comparado con las otras páginas esta solo tuvo 7 riesgos de bajo nivel.

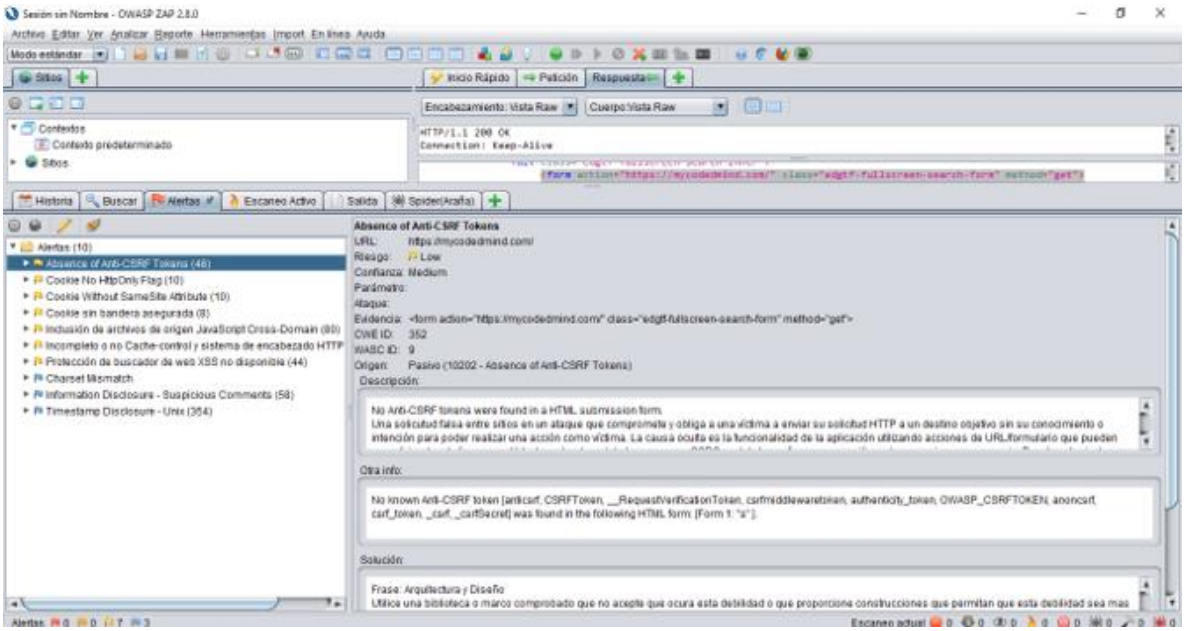


Imagen 10 Análisis de vulnerabilidades de la página web de MYCODEDMIND.

Fuente: (Autor propio)

CAPÍTULO V.

5. PROPUESTA DE INVESTIGACIÓN.

5.1.IMPLEMENTACIÓN DEL MANUAL.

5.1.1. GESTIÓN DE RIESGOS EN PÁGINAS WEB.

En la actualidad las empresas, dependen de los datos e información que se encuentran registrado en sus sistemas, por esta razón es importante poner en conocimiento a los clientes de cual es el impacto del problema relacionado con la seguridad de la información, a través de gráficos, también evitando el tecnicismo para facilitar el entendimiento a personas que no están involucradas tanto en el tema.

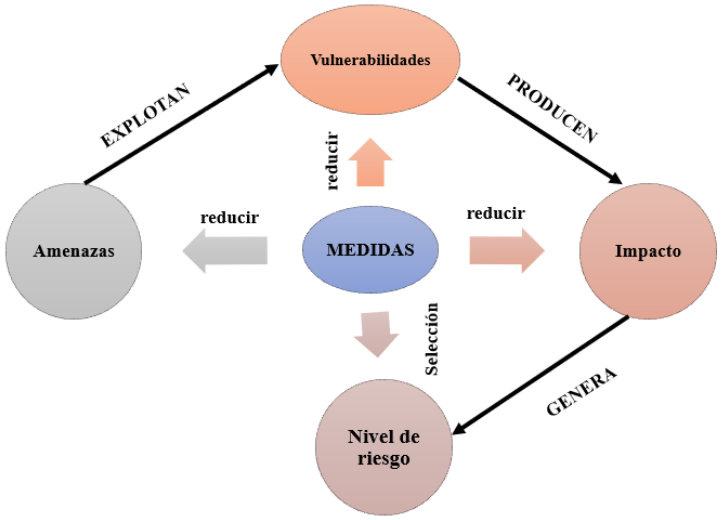


Imagen 11 Gestión de riesgo.

Fuente: (Autor propio)

Para llevar a cabo la implementación de seguridad en una empresa, es importante considerar diferentes requisitos que ayudaran a obtener confianza superior, como las siguientes.

- Políticas de seguridad.
- Organización y división de responsabilidades.
- Seguridad física y contra incendios.

- Políticas del personal.
- Seguros.

5.1.2. Auditoria de seguridad.

Ayuda a mejorar la seguridad de la información, la cual permite detectar fraudes, errores o atentados a la página web a través de revisiones oportunas, esto se debe revisar durante el desarrollo de la página web, para verificar las actividades y el cumplimiento de normas y estándares que permitan generar un código fiable.

Una vez que se termina el producto, y ya se encuentra en la etapa de la implementación, se deben realizar tareas de verificación de funcionamiento, mediante las siguientes herramientas:

- Observación.
- Cuestionarios.
- Entrevistas.
- Pruebas de seguridad.

5.2.FUNCIONALIDAD DEL DIAGRAMA.

Debido a que las empresas no contaban con un manual técnico de seguridad, este se implemento en el diagrama general, el manual se utilizara siempre que el cliente quiera, ya que por el hecho de ser una seguridad más a la página web, el costo y el tiempo de entrega pueden aumentar dependiendo el criterio del desarrollador.

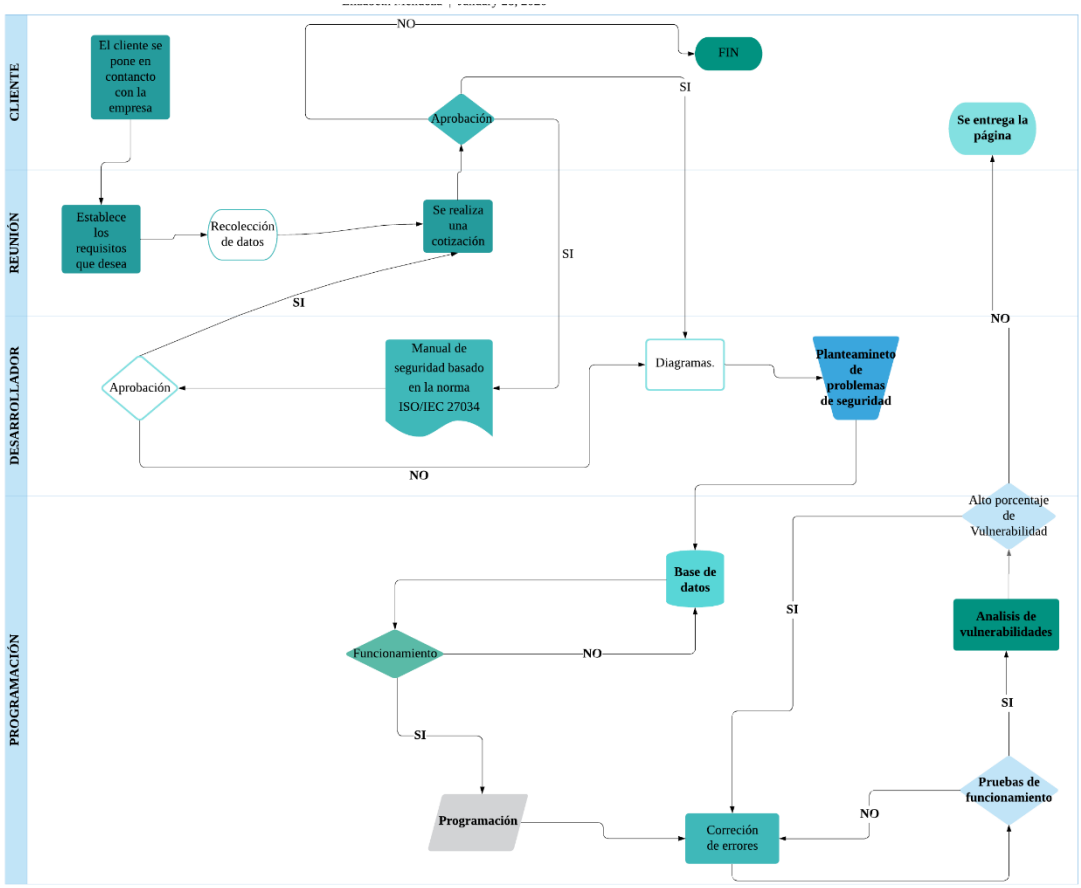


Imagen 12 *Diagrama del Manual de seguridad basado en la norma ISO/IEC 27034*

Fuente: (Autor propio)

6. CRONOGRAMA DE ACTIVIDADES.

ACTIVIDADES	SEPTIEMBRE.				OCTUBRE.				NOVIEMBRE.				DICIEMBRE.				ENERO.			
	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4
Presentación, revisión y aprobación de Tema de Trabajo de Titulación.																				
Ajustes al anteproyecto del Trabajo de Titulación.																				
Desarrollo de la introducción y el problema.																				
Marco Teórico y conceptual.																				
Metodología de la Investigación.																				
Pruebas en el OWASP ZAP.																				
Predefensa.																				
Análisis e interpretación de los resultados.																				
Propuesta de investigación.																				
Recepción del documento final del Trabajo de Titulación.																				

7. CONCLUSIONES.

Como resultado de la investigación realizada, se puede decir que la propuesta de manual de seguridad basado en la norma ISO/IEC 27034 para el desarrollo de páginas web, se considera una herramienta de ayuda para identificar los requerimientos que se deben tener en cuenta al momento de realizar una página web y a su vez poder disminuir los riesgos que se puedan generar. Mediante el proceso de análisis e identificación de vulnerabilidades se pudo conocer los tipos de vulnerabilidades más frecuentes de las páginas web en estudio y plantear una forma de minimizar el riesgo a un ataque.

Se logró analizar las seguridades de páginas web basándose en la norma ISO/IEC 27034 y se realizaron pruebas en OWAS ZAP para evaluar las vulnerabilidades que contienen las páginas web, esto nos puede ayudar a tener una visión más comprensiva para garantizar una seguridad efectiva, promoviendo en las empresas la integración de un manual de seguridad para páginas web, esto ayudaría reducir los riegos en la seguridad y la resistencia a cambios futuros.

ISO/IEC 27034 ayuda a las empresas a plantear y administrar controles de seguridad y niveles de confianza, respecto a los recursos y prioridades de la empresa.

La seguridad de la información es basada en la administración del riesgo. El mismo que no puede ser eliminado, pero puede solo ser minimizado a un nivel aceptable, se debe definir los requerimientos de seguridad que significa como se va a mitigar el riesgo.

Dentro de los requerimientos se debe diseñar e implementar un manual de seguridad para páginas web que debe proporcionar confianza cuando se realice la reducción de riesgos.

8. RECOMENDACIONES.

Se recomienda, definir las especificaciones de seguridad más claras para así poder desarrollar una página web que cumpla con los parámetros y requisitos propios de la empresa.

Para evitar vulnerabilidades no detectadas en una página web. Se recomienda realizar pruebas de vulnerabilidad de la página web y de la base de datos y poder proceder con las respectivas correcciones.

La seguridad es de gran importancia, y se debe tener en cuenta en una empresa, debido a que cada día aparecen o se desarrollan nuevos tipos de amenazas, por tanto, se recomienda capacitar a los miembros de la organización sobre conceptos básicos de seguridades.

Es necesario seguir los estándares que siguen otros países para el desarrollo de páginas web, e identificar áreas que manejan información crítica o sensible.

9. BIBLIOGRAFÍA.

Barà, M. (2019). *Estrategias ante las Amenazas en Proyectos*. Obtenido de Estrategias ante las Amenazas en Proyectos: https://www.obs-edu.com/es/blog-investigacion/project-management/estrategias-ante-las-amenazas-en-proyectos

Domínguez, A. A. (21 de Agosto de 2015). *¿Qué es y cómo opera un ataque de Cross-Site Scripting (XSS)*. Obtenido de ¿Qué es y cómo opera un ataque de Cross-Site Scripting (XSS): https://www.seguridad.unam.mx/historico/documento/index.html-id=35

Guazaman, M. y. (28 de Agosto de 2016). *CIA Modelo de Seguridad*. Obtenido de CIA Modelo de Seguridad: https://camendoz.wordpress.com/2016/08/28/cia-modelo-de-seguridad/

INCIBE. (20 de Marzo de 2017). *Amenaza vs Vulnerabilidad*. Obtenido de Amenaza vs Vulnerabilidad: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

ISO 27000.es. (2019). *El portal de ISO 27001 en Español*. Obtenido de El portal de ISO 27001 en Español: http://www.iso27000.es/iso27000.html

ISO/IEC 27034. (2018). *Seguridad de la aplicación*. Obtenido de Seguridad de la aplicación: https://www.iso27001security.com/html/27034.html

ISOTools. (2019). *ISO 27001*. Obtenido de ISO 27001: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

Lucia D'Adamo, M. P. (18 de Octubre de 2017). *Qué es y en qué consiste un ataque informático*. Obtenido de Qué es y en qué consiste un ataque informático: https://www.consulthink.it/es/que-es-y-en-que-consiste-un-ataque-informatico/

MDN. (12 de abril de 2019). *Seguridad de Sitios Web*. Obtenido de Seguridad de Sitios Web: https://developer.mozilla.org/es/docs/Learn/Server-side/Primeros_pasos/seguridad_sitios_web?fbclid=IwAR041dgeAEmof5Czlr-y7PCD7w2Z3s0rp0oOwRdTowB0m8UuEjMdexWj0Jk

Nmap. (2019). *Nmap.org*. Obtenido de GUI de Zenmap: https://nmap.org

Nmap.org. (2019). *Capítulo 15. Guía de referencia de Nmap*. Obtenido de Capítulo 15. Guía de referencia de Nmap: https://nmap.org/

Ogata, M., Franklin, J., Voas, J., Sritapan, V., & Stephen. (enero de 2015). *Vetting the Security of Applications*. Obtenido de Vetting the Security of Applications: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-163.pdf

OWASP. (11 de noviembre de 2014). *Sobre OWASP*. Obtenido de Sobre OWASP: https://www.owasp.org/index.php/Sobre_OWASP

OWASP. (2017). *Los diez riesgos más críticos en Aplicaciones Web*. Obtenido de Los diez riesgos más críticos en Aplicaciones Web: https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

OWASP. (21 de agosto de 2019). *La Fundación OWASP*. Obtenido de La Fundación OWASP: https://www.owasp.org/index.php/About_The_Open_Web_Application_Security_Project

OWASP. (01 de octubre de 2019). *OWASP™ Foundation*. Obtenido de OWASP™ Foundation: https://www.owasp.org/index.php/Main_Page

SGSI . (26 de Enero de 2017). *¿Seguridad informática o seguridad de la información?* Obtenido de ¿Seguridad informática o seguridad de la información?: https://www.pmg-ssi.com/2017/01/seguridad-de-la-informacion/

SGSI. (30 de Marzo de 2015). *ISO 27001: Los activos de información*. Obtenido de ISO 27001: Los activos de información: https://www.pmg-ssi.com/2015/03/iso-27001-los-activos-de-informacion/

SGSI. (6 de junio de 2019). *Análisis y evaluación de riesgos en ISO 27001*. Obtenido de Análisis y evaluación de riesgos en ISO 27001: https://www.pmg-ssi.com/2019/06/analisis-y-evaluacion-de-riesgos-en-iso-27001-amenazas-consecuencias-y-criticidad/

10.GLOSARIO.

CID: Confidencialidad, Integridad y Disponibilidad.

COOKIE: Son pequeños archivos que almacenan información sobre el usuario y que algunos sitios web guardan en el ordenador

CSA: Control de Seguridad de la Aplicación.

GUI: Interfaz Gráfica de Usuario, es un programa informático que utiliza un conjunto de imágenes y objetos gráficos para representar la información y acciones disponibles en la interfaz.

HOST: es un ordenador que funciona como el punto de inicio y final de las transferencias de datos, tiene una dirección de Internet única y un nombre de dominio único.

MARCO NORMATIVO: Conjunto de normas, metodologías, lineamientos y sistemas, que establecen la forma en que deben desarrollarse las acciones para alcanzar los objetivos propuestos.

PAR: Solicitud de Acción Preventiva.

REPOSITORIO: Es un sitio donde se almacena y mantiene información digital, habitualmente bases de datos o archivos informáticos.

SGSI: Sistema de Gestión de Seguridad de la información, se debe realizar mediante un proceso sistémico, documentado y conocido por toda la empresa.

TI: Tecnología de la Información, se refiere al uso de equipos de telecomunicaciones y computadoras para la transmisión, el procesamiento y el almacenamiento de datos.

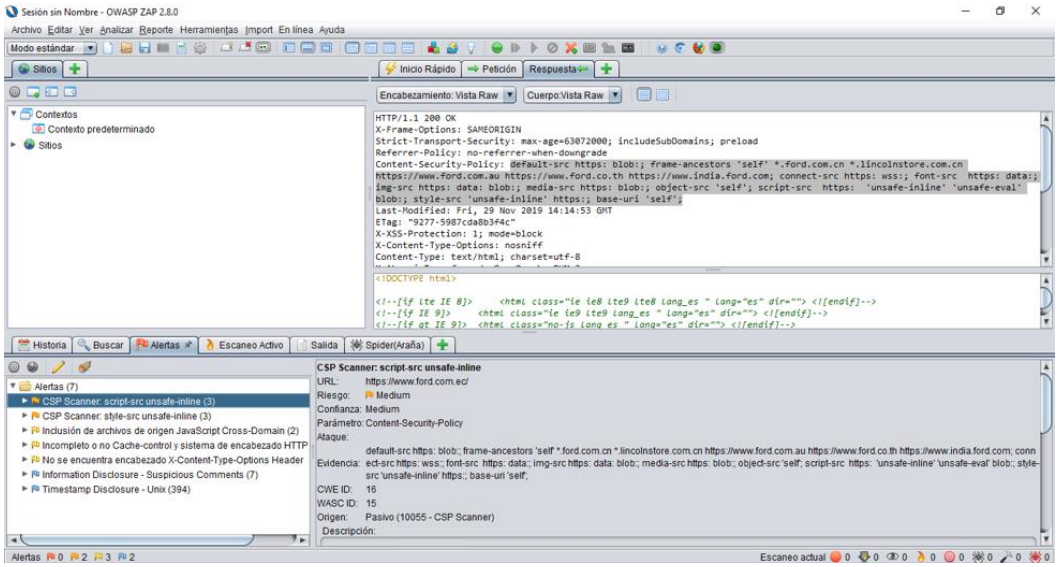
TIC: Tecnología de la Información y Comunicación, son el conjunto de tecnologías desarrolladas para gestionar información y enviarla de un lugar a otro.

TOKEN: Es una cadena de caracteres que tiene un significado coherente, podrían ser palabras clave, identificadores, números, signos, o un operador de varios caracteres.

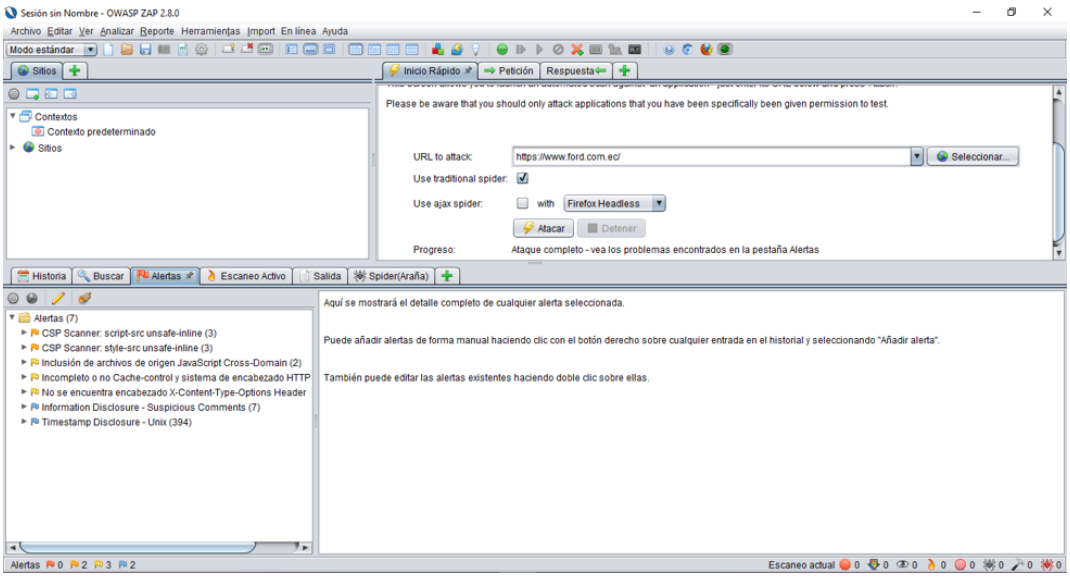
XML: Lenguaje de Marcas Extensible.

11.ANEXOS.

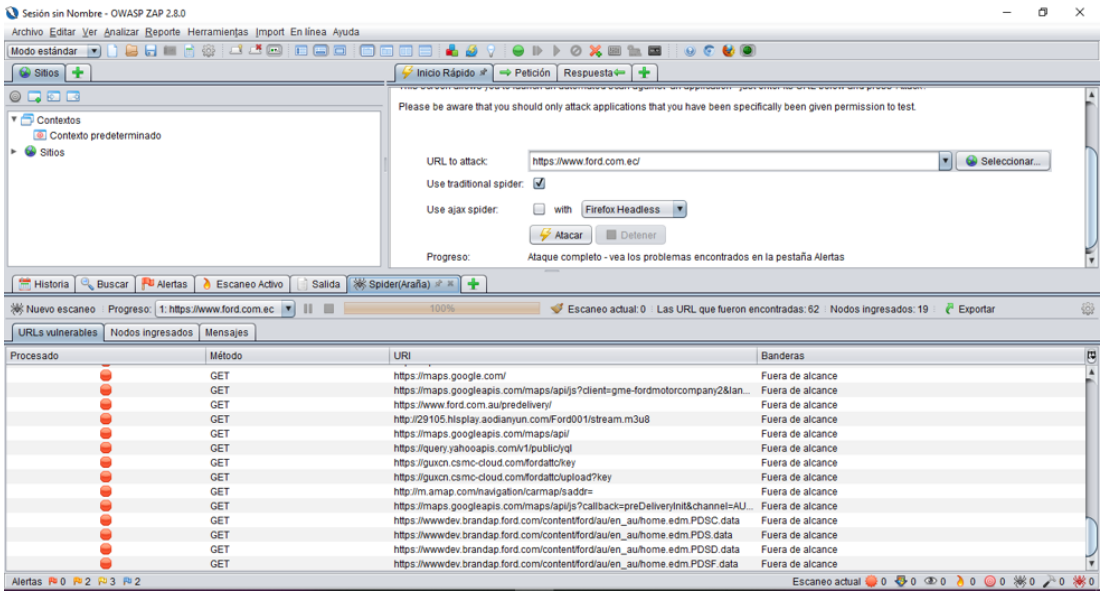
Anexo 1. Análisis de vulnerabilidades de la página web de FORD.



Fuente: (Autor propio)

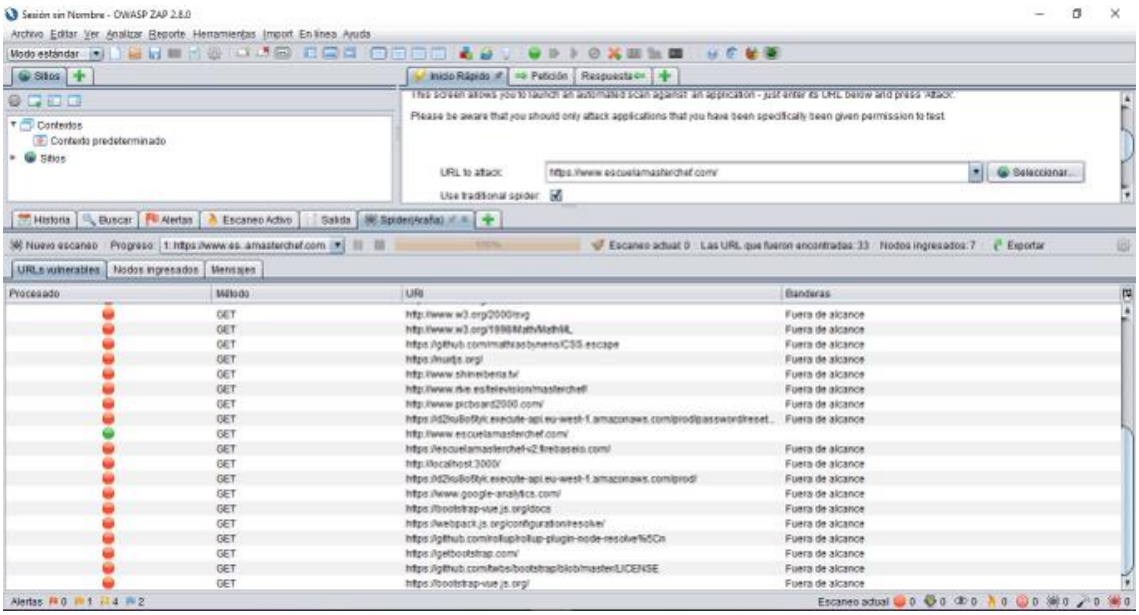


Fuente: (Autor propio)

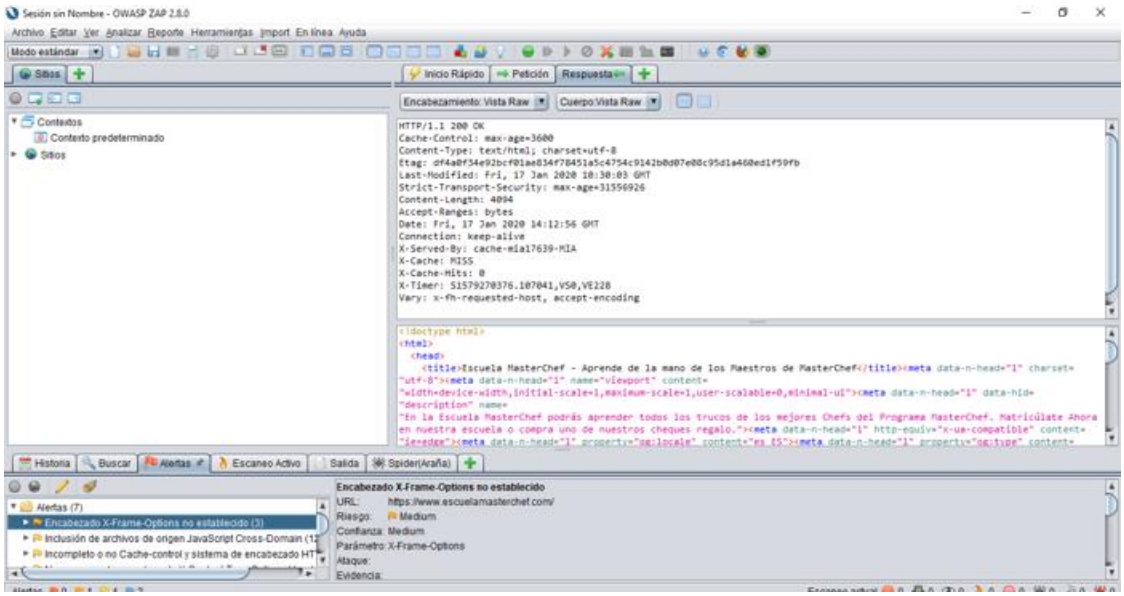


Fuente: (Autor propio)

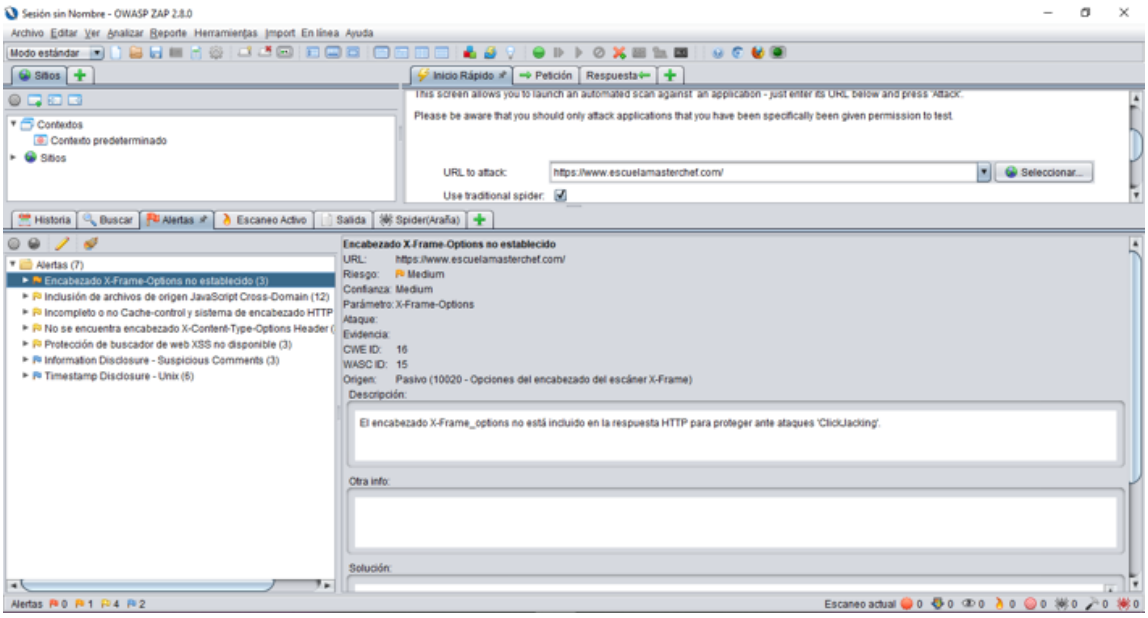
Anexo 2. Análisis de vulnerabilidades de la página web de MASTER CHEF.



Fuente: (Autor propio)

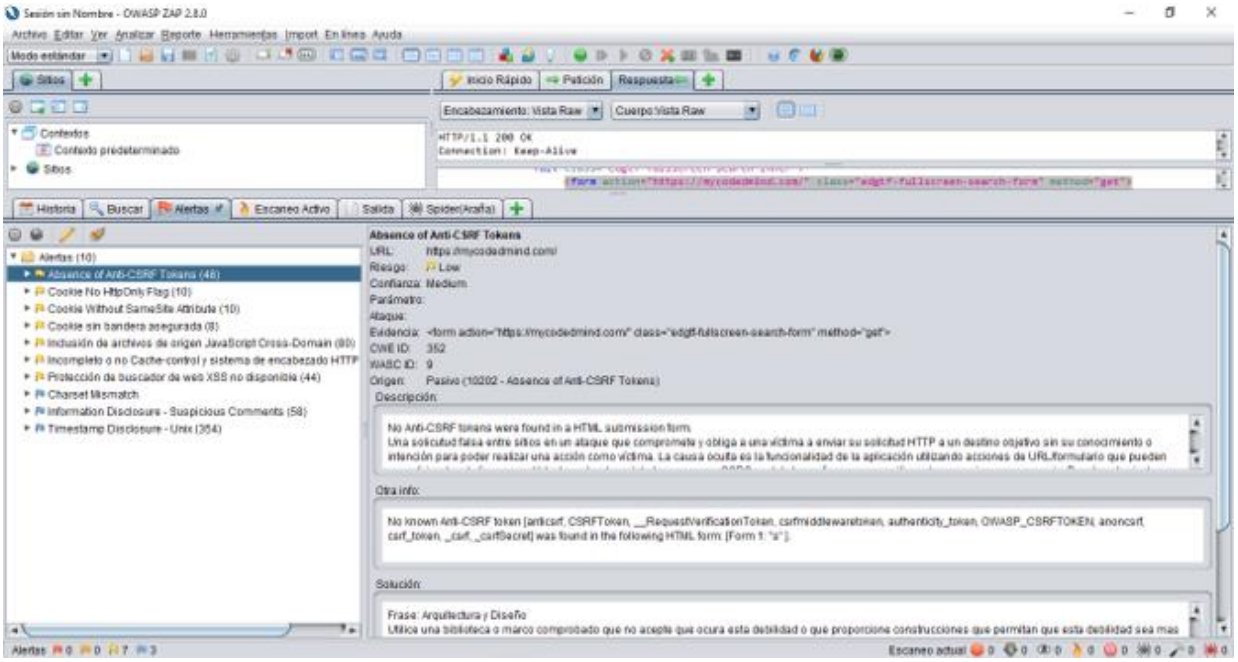


Fuente: (Autor propio)

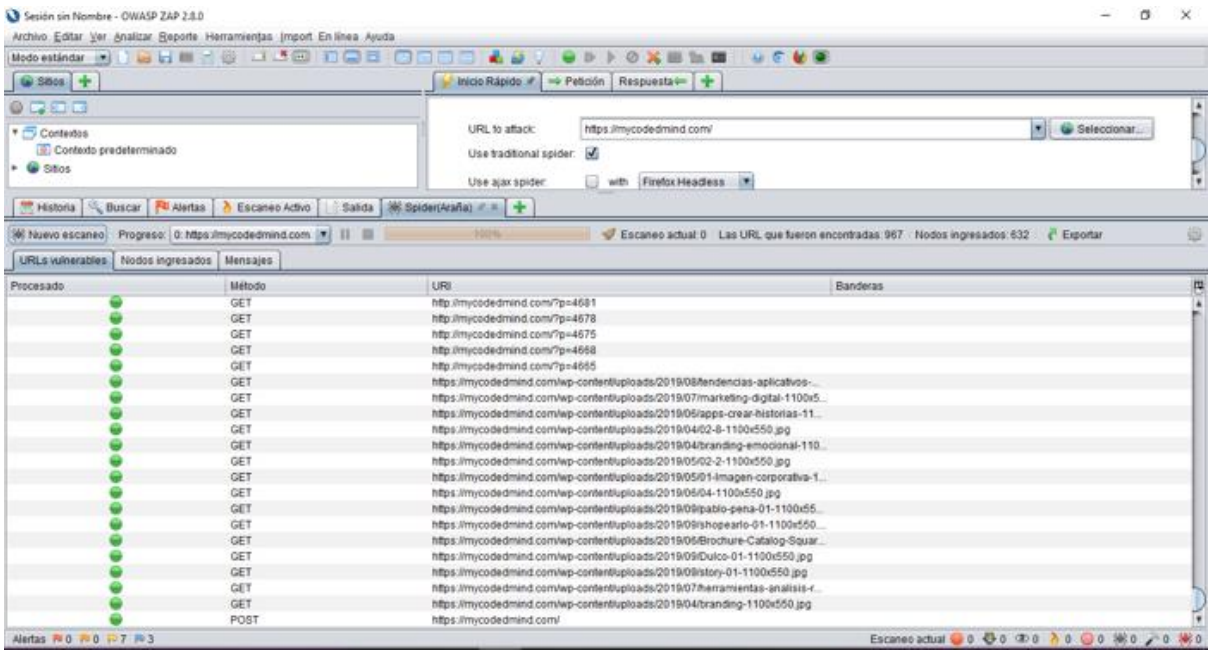


Fuente: (Autor propio)

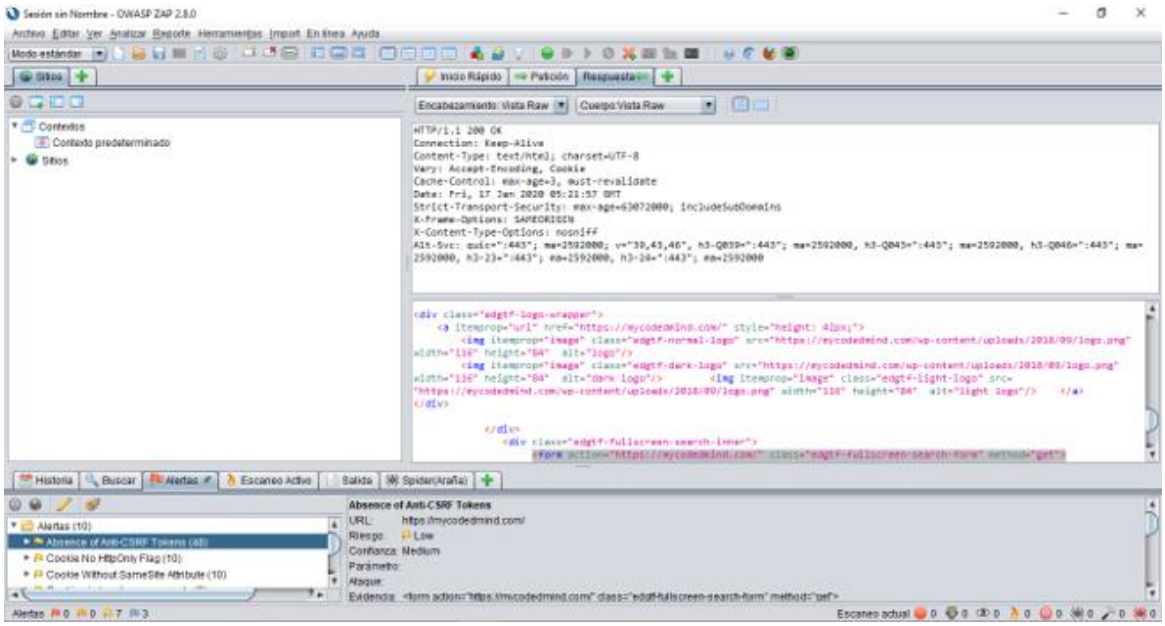
Anexo 3. Análisis de vulnerabilidades de la página web de MYCODEDMIND.



Fuente: (Autor propio)

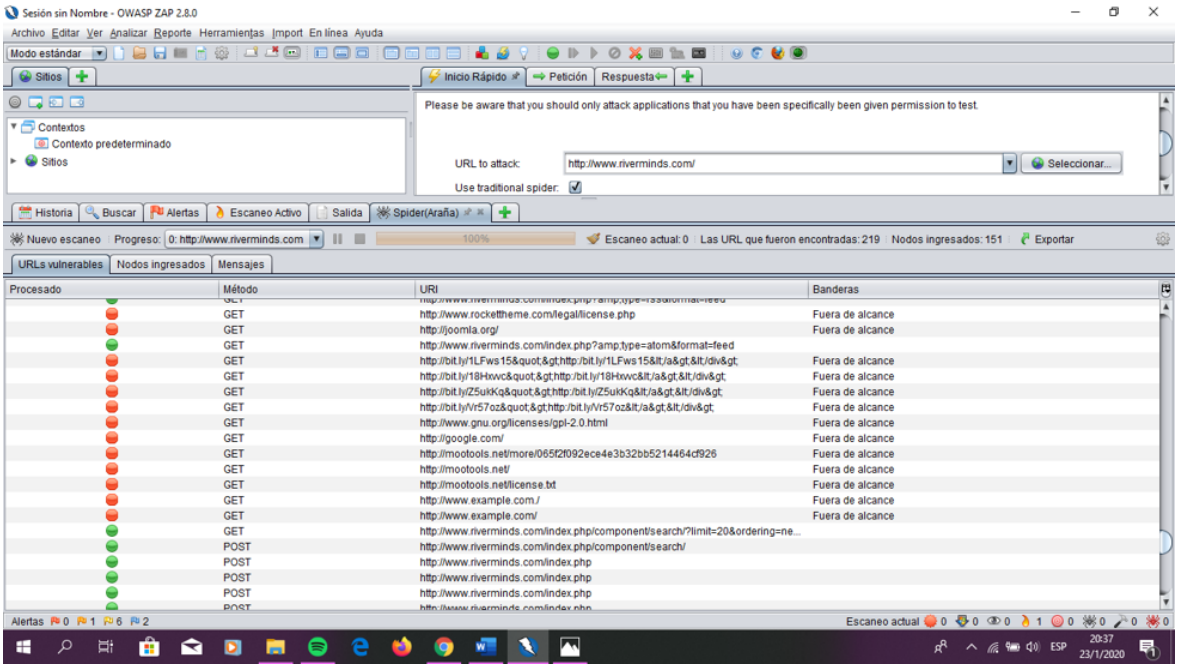


Fuente: (Autor propio)

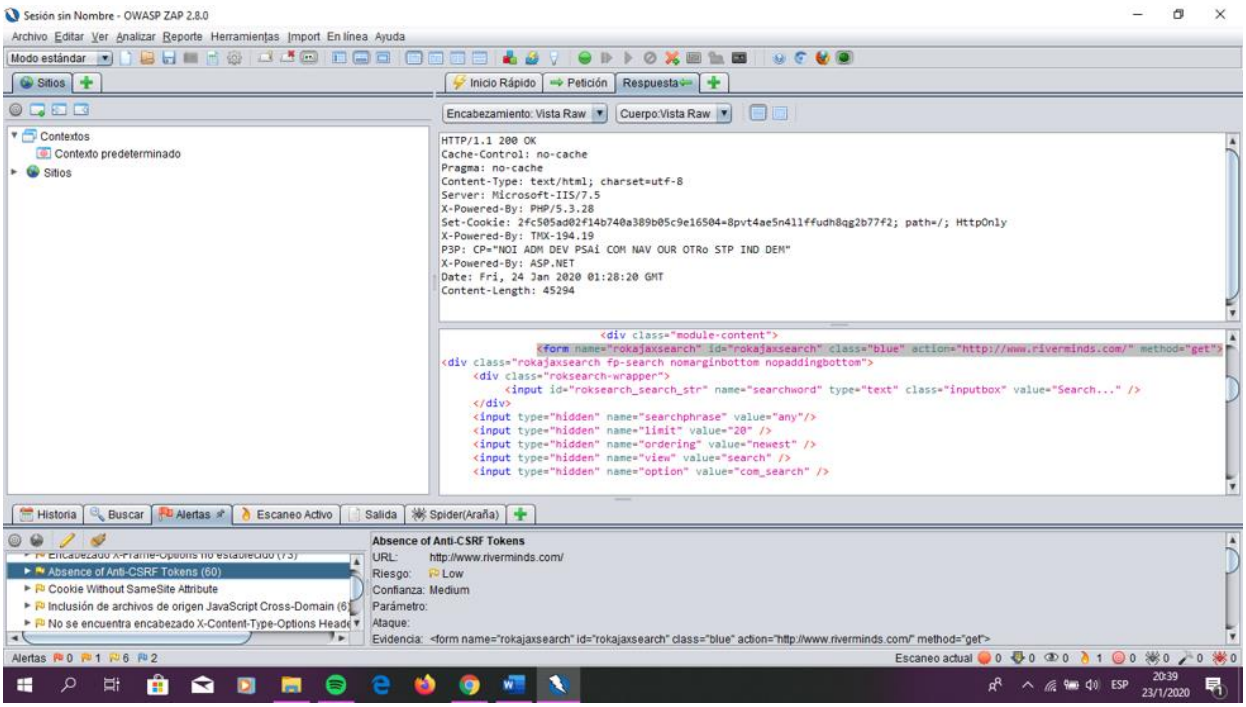


Fuente: (Autor propio)

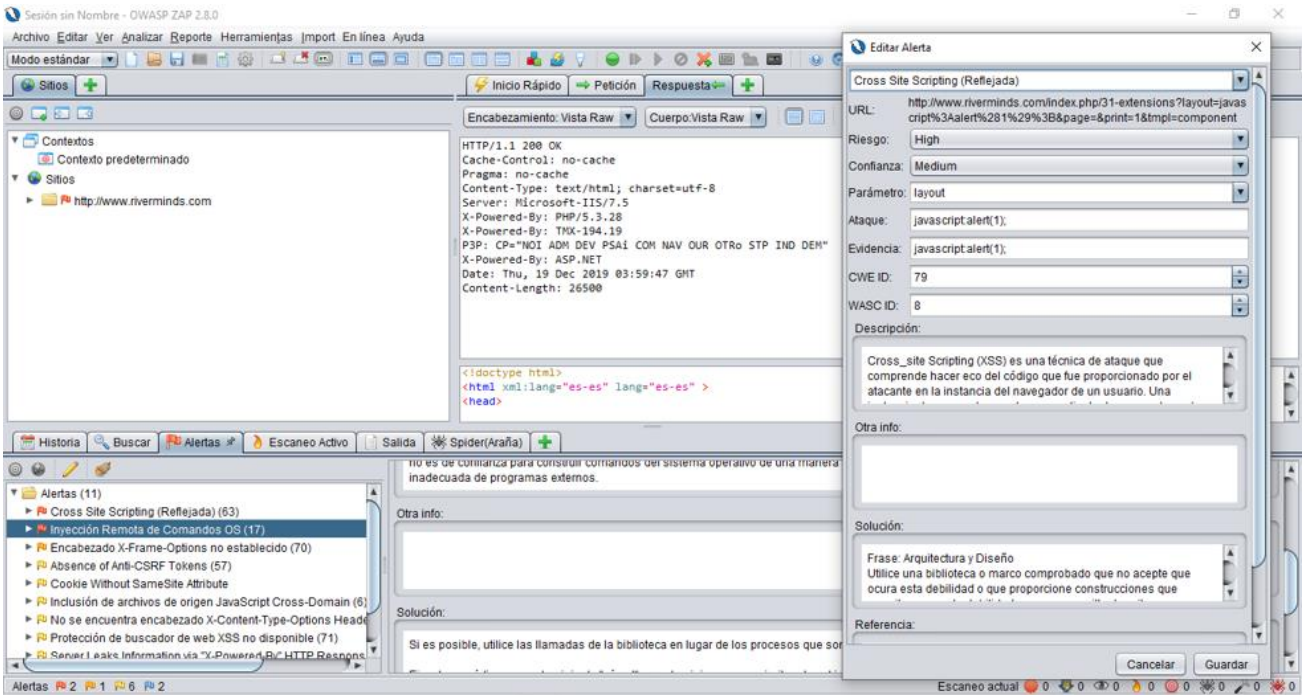
Anexo 4. Análisis de vulnerabilidades de la página web de RIVERMINDS.



Fuente: (Autor propio)

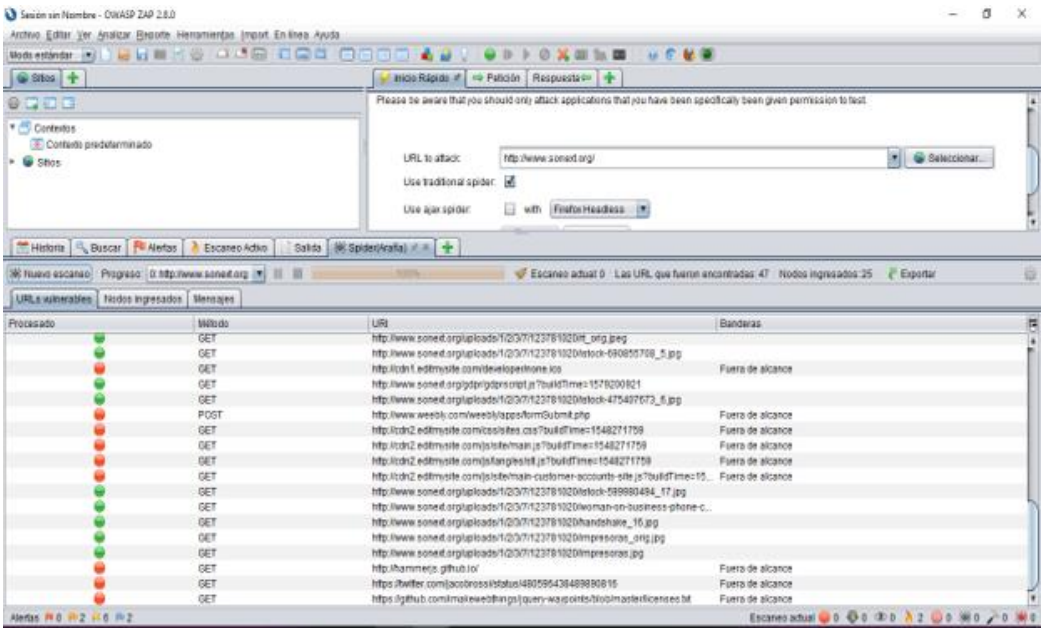


Fuente: (Autor propio)

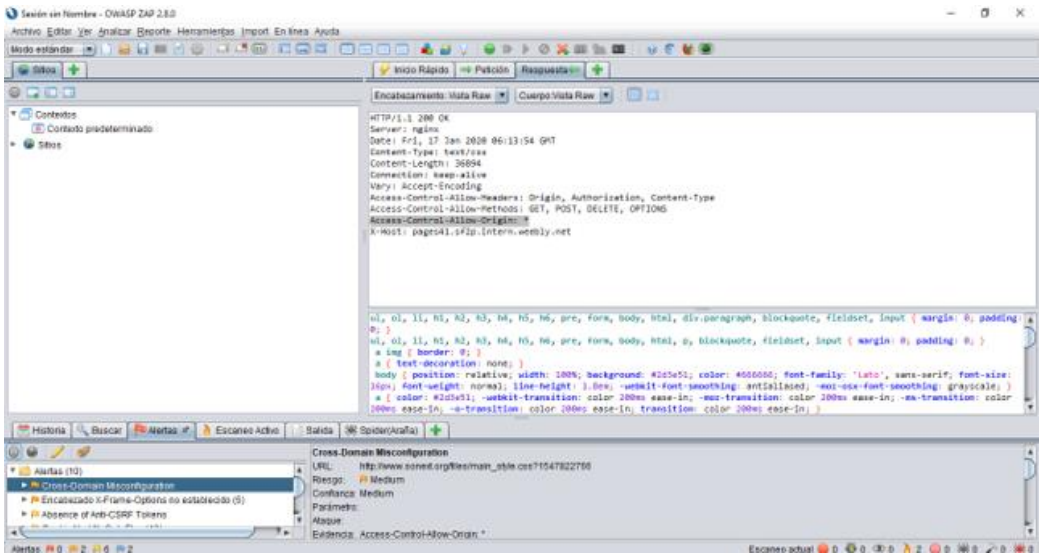


Fuente: (Autor propio)

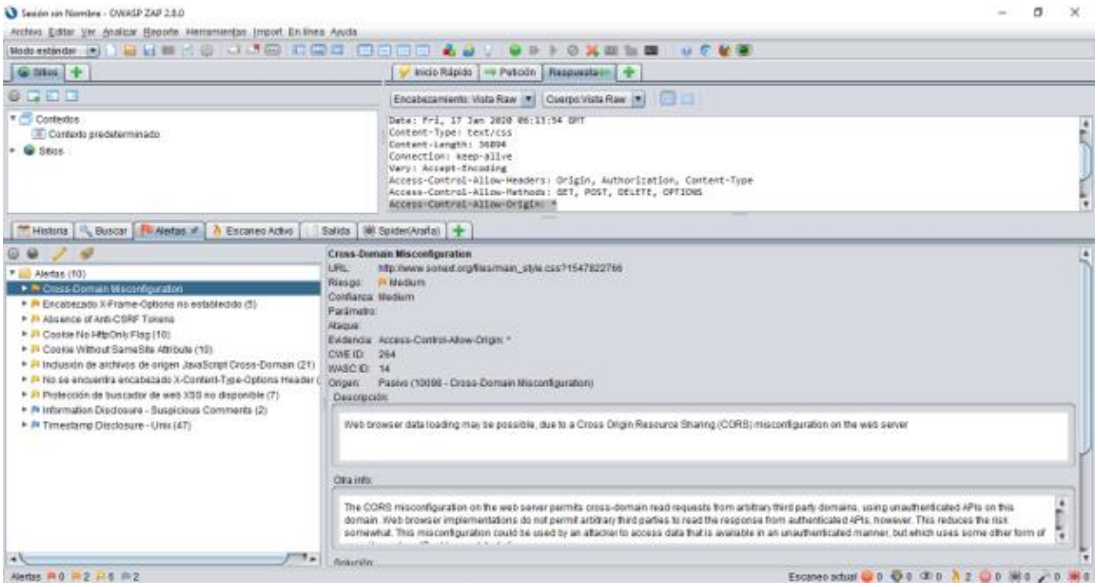
Anexo 5. Análisis de vulnerabilidades de la página web de FORD



Fuente: (Autor propio)

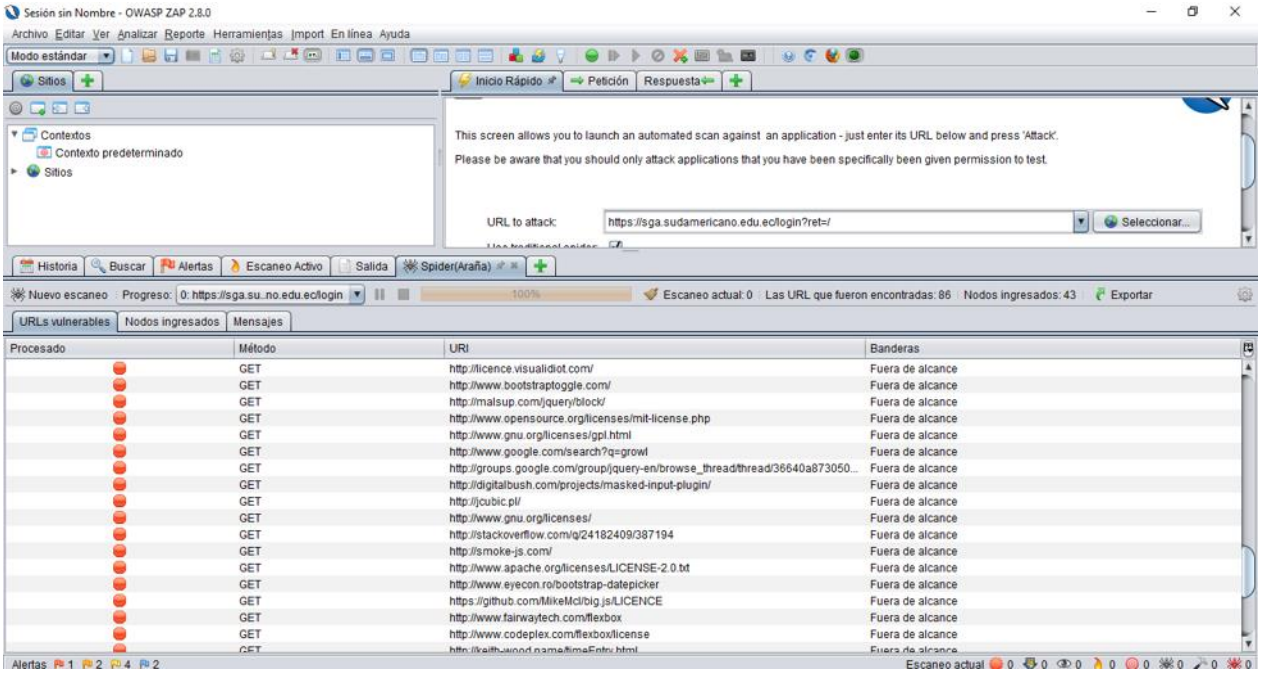


Fuente: (Autor propio)

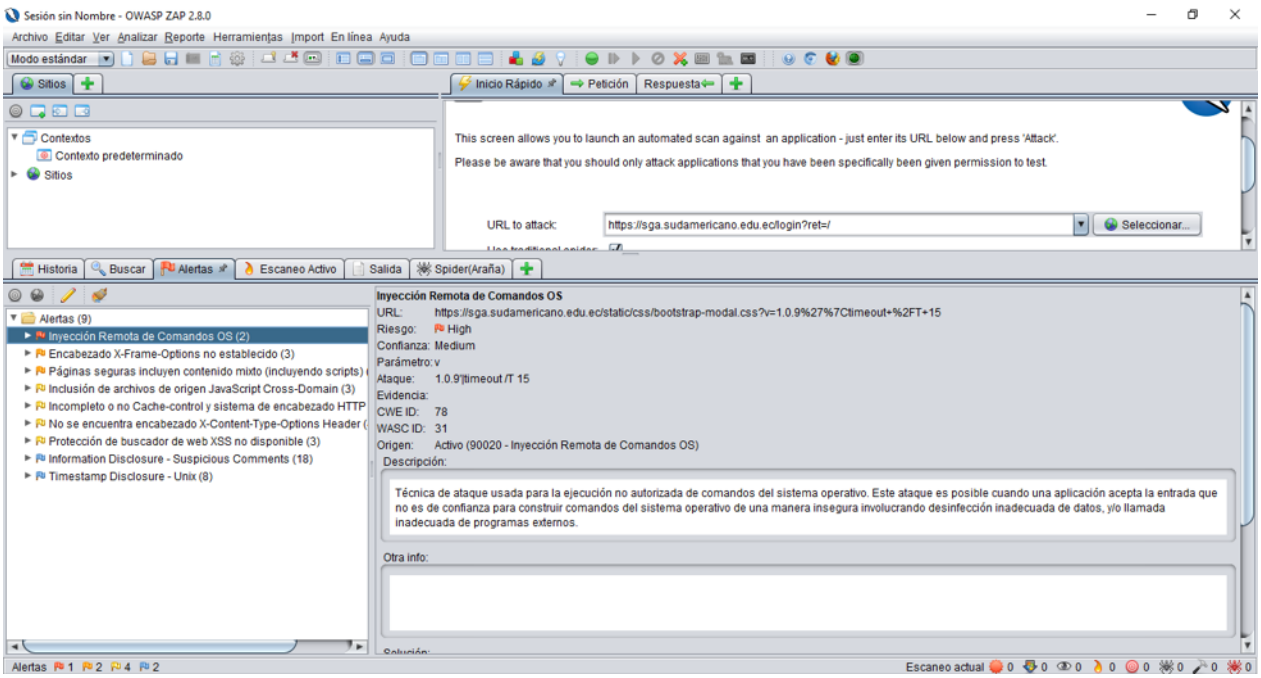


Fuente: (Autor propio)

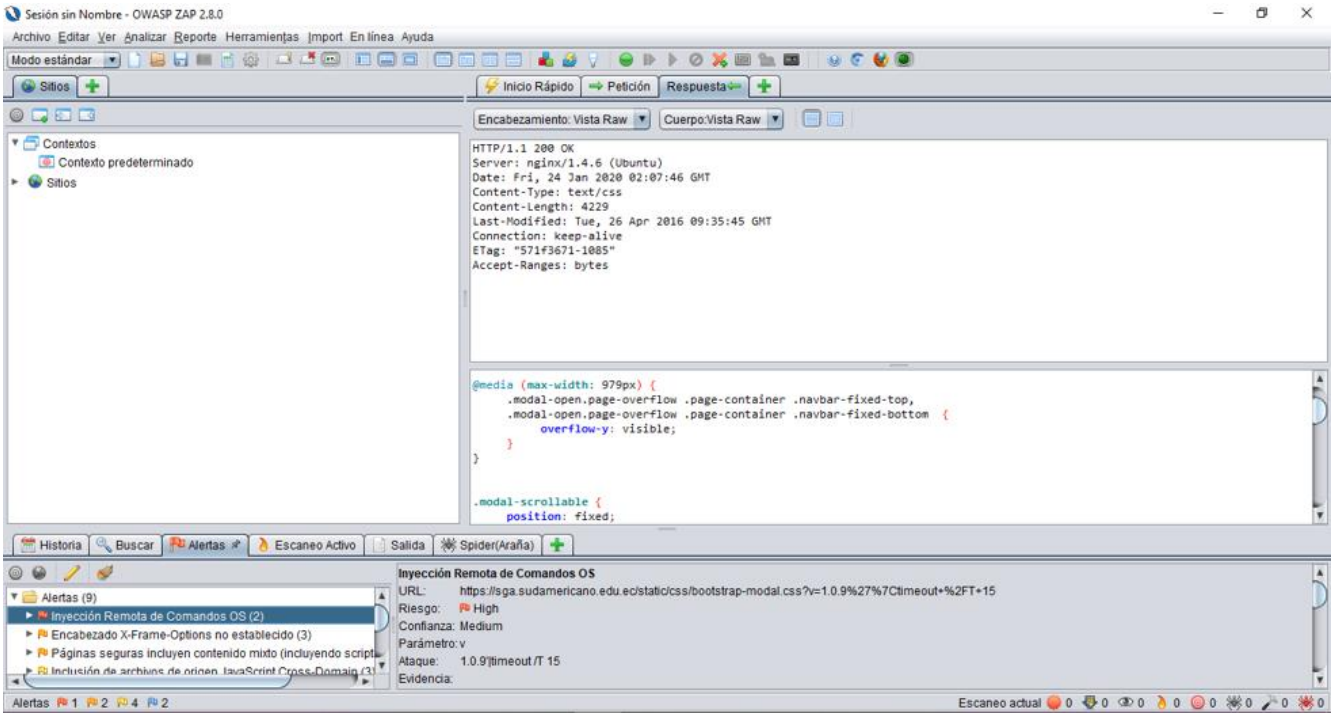
Anexo 6. Análisis de vulnerabilidades de la página web de SUDAMERICANO.



Fuente: (Autor propio)

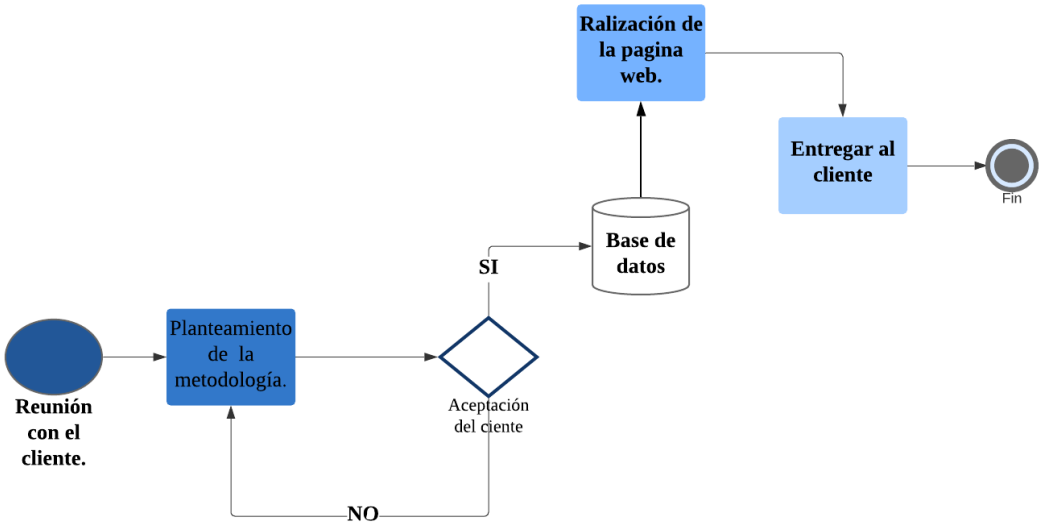


Fuente: (Autor propio)



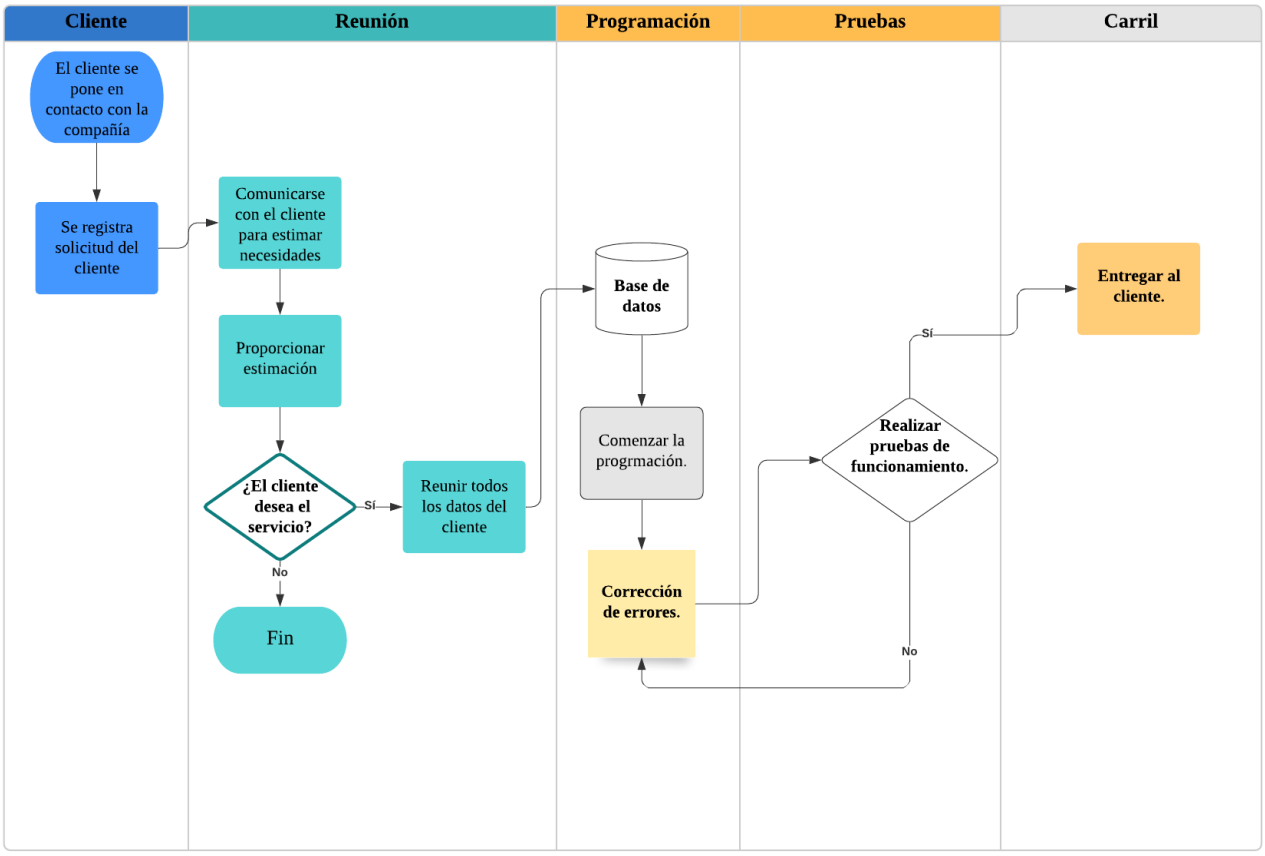
Fuente: (Autor propio)

Anexo 7. Diagrama de flujo de la página web de SONEXT.



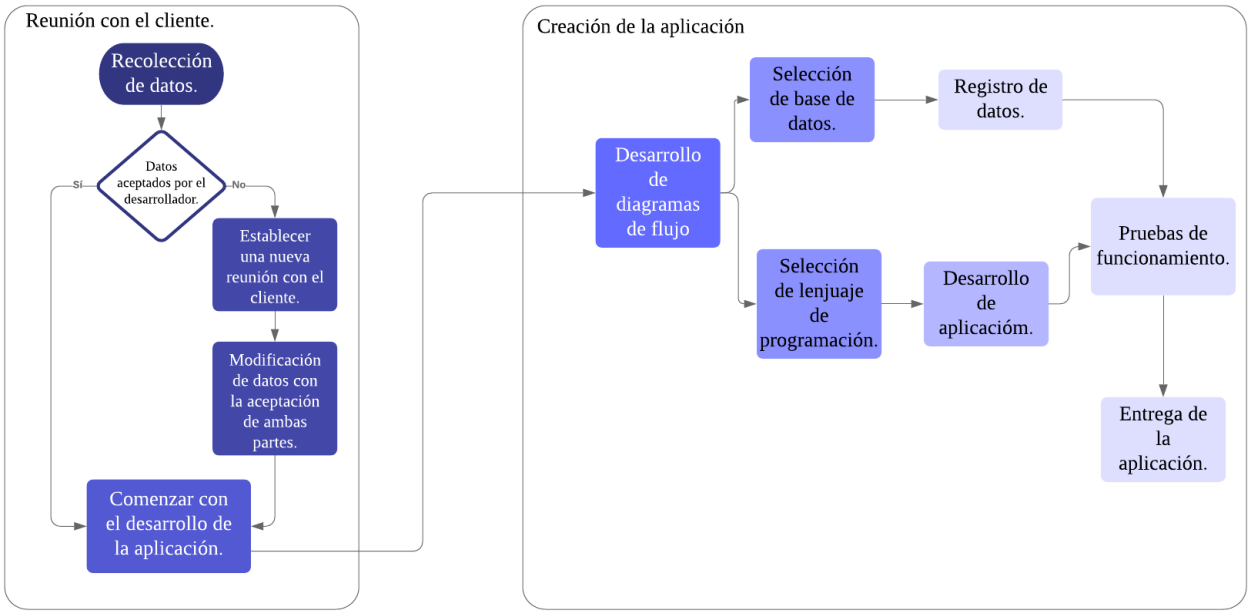
Fuente: (Autor propio)

Anexo 8. Diagrama de flujo de la página web de MYCODEDMIND



Fuente: (Autor propio)

Anexo 9. Diagrama de flujo de la página web de RIVERMIND.



Fuente: (Autor propio)