DESARROLLO DE UN MODELO PARA CALCULAR EL NIVEL DE SEGURIDAD EN SITIOS WEB, BASADO EN EL TOP 10 DE VULNERABILIDADES MÁS EXPLOTADAS EN 2017 SEGÚN EL MARCO DE REFERENCIA OWASP

RAFAEL ENRIQUE RODRÍGUEZ RODRÍGUEZ

ANDRÉS FELIPE SÁNCHEZ SÁNCHEZ

UNIVERSIDAD CATÓLICA DE COLOMBIA

FACULTAD DE INGENIERÍA

PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

BOGOTÁ D.C 2018

DESARROLLO DE UN MODELO PARA CALCULAR EL NIVEL DE SEGURIDAD EN SITIOS WEB, BASADO EN EL TOP 10 DE VULNERABILIDADES MÁS EXPLOTADAS EN 2017 SEGÚN EL MARCO DE REFERENCIA OWASP

RAFAEL ENRIQUE RODRÍGUEZ RODRÍGUEZ

ANDRÉS FELIPE SÁNCHEZ SÁNCHEZ

Trabajo de grado para obtener el título de especialista en seguridad de la información

ASESOR: HÉCTOR JAIMES

INGENIERO DE SISTEMAS

UNIVERSIDAD CATÓLICA DE COLOMBIA

FACULTAD DE INGENIERÍA

PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

BOGOTÁ D.C 2018

Nota de aceptación

_____
_____
_____

_____
Presidente del Jurado

_____
Jurado

_____
Jurado

Bogotá D., Diciembre de 2018.

DEDICATORIA

Dedicamos este proyecto primeramente a Dios por ser nuestro faro en cada paso en nuestras carreras profesionales, a nuestros padres por ser nuestro apoyo y fortaleza en cada nuevo reto que tomamos en nuestras vidas y con los que contamos en todo momento; a nuestros parejas, quienes nos han apoyado de manera incondicional en el desarrollo de nuestra especialización, a todos los profesores que compartieron su conocimiento con nosotros cuyo trabajo nos ayuda en la formación como especialistas y a nuestros compañeros que nos apoyaron y crecimos como especialistas en seguridad de información durante este año.

AGRADECIMIENTOS

Este trabajo de grado es el consolidado de un proceso de crecimiento personal, intelectual y profesional en nuestras vidas. Agradecemos a Dios el creador del universo que me permite construir otros mundos mentales. A nuestras familias por el apoyo incondicional y su acompañamiento en este proceso de crecimiento. A los profesores de la especialización, que con su profesionalismo lograron transmitir sus mejores conocimientos. A nuestro asesor de trabajo de grado HECTOR DARIO JAIMES, por su apoyo y colaboración en la consolidación de los conocimientos adquiridos en este trabajo de grado. A todas aquellas personas que de una u otra manera participaron y nos acompañaron en este proceso tan significativo para nosotros.

TABLA DE CONTENIDO

RESUMEN 12

ABSTRACT 13

INTRODUCCIÓN 14

1. Generalidades 16

1.1. Línea de Investigación 16

1.2. Alcance del proyecto 16

1.3. Planteamiento del Problema 17

1.3.1. Antecedentes del problema 17

1.3.2. Formulación de problema 21

1.3.3. Pregunta de investigación 21

1.3.4. Variables del problema 21

1.4. Justificación 22

1.5. Objetivos 23

1.5.1. Objetivo general 23

1.5.2. Objetivos específicos 23

2. Marcos de referencia 24

2.1. Marco conceptual 24

2.1.1. CVE 24

2.1.2. CVSS 24

2.1.3. Oswasp 24
2.1.4. Isaca 24
2.1.5. Cobit 25
2.1.6. ISO 27001 25
2.1.7. ISO 27005 25
2.1.8. Iso 27004 25
2.1.9. Riesgo 25
2.1.10. Amenaza 26
2.1.11. vulnerabilidad 26
2.1.12. Probabilidad 26
2.1.13. Frecuencia 26
2.1.14. seguridad de la información 26
2.1.15. Sitio web 26
2.1.16. Nist 800-55 27
2.1.17. ISO 27004 27
2.1.18. activo 27
2.2. Marco teórico 27
2.2.1. Owasp. 27
2.2.2. CVE. 30
2.2.3. CVSS. 31

2.2.4. Nist 800-55 32

2.2.5. ISO 27004 33

2.3. Marco jurídico 34

2.3.1. Derechos de Autor 34

2.4. Marco geográfico 34

2.5. Estado del arte 35

3. Metodología 38

3.1. FASES DEL TRABAJO DE GRADO 38

4. desarrollo de la propuesta 40

4.1. modelos aplicables para evaluar las vulnerabilidades de la ciber seguridad..... 40

4.2. Análisis de marcos de referencia en cuanto a la evaluación de vulnerabilidades de sitios web……..42

4.3. Definición del modelo para calcular el nivel de seguridad en sitios web. 47

4.4. Caso de Prueba 51

5. PRODUCTOS POR ENTREGAR 61

6. conclusiones 62

7. Recomendaciones 63

8. Trabajos futuros 64

9. Estrategias de comunicación 65

10. Bibliografía 66

LISTA DE TABLAS

TABLA 1: VARIABLES DEL PROBLEMA FUENTE: LOS AUTORES. 22

TABLA 2. MATRIZ E CATEGORIZACIÓN DE LOS MARCOS REFERENCIALES. FUENTE LOS AUTORES. 40

TABLA 3. VARIABLES DE LA FÓRMULA PARA CALIFICAR LA VULNERABILIDAD. 49

TABLA 4. VARIABLES PARA EL IMPACTO DE NEGOCIO 49

TABLA 5. ESCALA DE CALIFICACIÓN DE VULNERABILIDADES SEGÚN CVSS. 51

TABLA 6. RESUMEN DE LAS VULNERABILIDADES ENCONTRADAS CON LA HERRAMIENTA 56

Lista de Figuras

Figura 1: distribución de sitios web hackeados en 2017. 18
Figura 2: plataformas desactualizadas. 19
Figura 3: distribución de las familias de malware. 19
Figura 4: relación de metodología de owasp 28
Figura 5:cambios de las versiones de owasp 29
Figura 6: fases de las vulnerabilidades en Owasp 29
Figura 7:codificación de CVE. 30
Figura 8: modelo de CVSS. 31
Figura 9: mapa de Bogotá. 34
Figura 10. Componentes de CVSS. 43
Figura 11 Modelo propuesto para calificación de vulnerabilidades. Fuente los Autores 48
Figura 12. Prueba con owasp-zap 53
Figura 13. Imagen de relacionada a X-Frame-Options. 54
Figura 14. Prueba 2 con owasp-zap 54
Figura 15. Prueba con ironwasp 55
Figura 16. Clasificación A4 de Owasp 201. 57
Figura 17. CVE 2012-1961 57
Figura 18. Análisis con el modelo propuesto de la vulnerabilidad 1. 58
Figura 19. Calificación de OWASP para A9 59
Figura 20. Calificación de CVE-2016-6145 59
Figura 21. Análisis con el modelo de la vulnerabilidad 2. 60
Figura 22. Resultado del sitio web. 61

RESUMEN

En la actualidad la seguridad de la información es una prioridad para las grandes, medianas y pequeñas empresas, por este motivo se han desarrollado técnicas, marcos de referencia y metodologías para hacer un análisis de vulnerabilidades, con el motivo de evitar la difusión de amenazas dentro de las organizaciones. Para el desarrollo del proyecto se investigó sobre las marcos de referencia, metodologías y buenas prácticas con el fin de gestionar un modelo para calificar y evaluar las vulnerabilidades de los sistemas, buscando las más alineadas, lo anterior con el fin de realizar un diagnóstico de selección de los marcos de referencia aplicables para la evaluar vulnerabilidades, así mismo se identificaran las características de los marcos utilizadas en la gestión de riesgos y vulnerabilidades con sus características, para continuar con el análisis de los resultados de las metodologías y marcos de referencia y así plantear un modelo para evaluar la vulnerabilidades de los sitios web según Owasp top 10 2017.

Palabras clave: Owasp, CVSS, vulnerabilidades, sitios web, modelo, calificación, evaluación.

ABSTRACT

Currently, information security is a priority for large, medium and small companies, for this reason techniques, frameworks and methodologies have been developed to analyze vulnerabilities, with the purpose of preventing the spread of threats within of the organizations. For the development of the project, research was carried out on reference frameworks, methodologies and good practices in order to manage a model to assess and assess the vulnerabilities of the systems, looking for the most aligned ones, in order to make a selection diagnosis. of the applicable reference frameworks for evaluating vulnerabilities, as well as identifying the characteristics of the frameworks used in the management of risks and vulnerabilities with their characteristics, in order to continue with the analysis of the results of the methodologies and reference frameworks and thus raise a model to assess the vulnerabilities of websites according to Owasp top 10 2017.

Keywords: Owasp, CVSS, vulnerabilities, websites, model, rating, evaluation.

INTRODUCCIÓN

En las organizaciones la información es un activo muy importante, por ello su protección de forma eficaz y eficiente resulta ser trascendental para la continuidad de los negocios.

La mayoría de las organizaciones generan desarrollo de software continuo y estos sistemas de información los están alojando en la nube, esto genera vulnerabilidades y riesgos para sus procesos (Control, 2015).

El continuo cambio sin la adecuada supervisión y falta de buenas prácticas de desarrollo de software dejan abiertas puertas que pueden ser explotadas maliciosamente.

Aunque existen procesos de calidad de software, en la actualidad hay grandes falencias ya que en muchas ocasiones se centran en pruebas funcionales, pero dejan a un lado las pruebas de haking etico o pruebas de seguridad en la información sobre plataformas web, lo que contribuye a la indisponibilidad de los servicios, al robo y a la no confidencialidad de la información (Control, 2015).

La Seguridad de la Información tiene como fin la protección de la información, uso, divulgación, interrupción o destrucción no autorizada (Ballestas, 2016). Conviene aclarar que la seguridad absoluta no es posible, no existe un sistema 100% seguro, de forma que los elementos vulnerables están ahí siempre presentes, independiente de los controles que se tomen, por lo que se tienen los niveles de seguridad y de niveles de vulnerabilidad.

Es aquí donde se debe entrar a evaluar y calificar las vulnerabilidades que tiene un sistema por lo que se encuentran modelos y metodologías orientadas a evaluar el impacto que están pueden tener en las organizaciones.

Por lo que diferentes organizaciones de TI (Isaca, Owasp, Iso 27005) que generan modelos para evaluar las vulnerabilidades y clasificarlas. Una de estas es Owasp que es una organización la cual genera cada año un ranking de vulnerabilidades y las clasifica según su tipo y el nivel de riesgo que tiene según los casos ocurridos y documentados en el transcurso del año (MinTic, 2016).

Por todo lo anterior el presente proyecto muestra un modelo para calcular el nivel de seguridad en aplicaciones web, basado en el top 10 de vulnerabilidades más explotadas en 2017 según el marco de referencia owasp (Moyano, 2017).

1. GENERALIDADES

1.1. LÍNEA DE INVESTIGACIÓN

El proyecto se en marca en la modalidad de “Software inteligente y convergencia tecnológica”, toda vez que, al realizar el desarrollo y estudio de esta problemática, se pueden identificar diferentes variables que evidencian alguna falencia que hay en los procesos de la de la seguridad de TI.

De la misma forma, el proyecto está desarrollado en torno a la necesidad de los las compañías y del personal de la seguridad de la información de mejorar el proceso para calificar o evaluar numéricamente una vulnerabilidad de un sitio web.

Por otro lado, se analizarán herramientas que hagan este proceso para definir los requerimientos y cálculos para realizar el desarrollo del modelo calcular el nivel de seguridad en Sitios web.

1.2. ALCANCE DEL PROYECTO

Este proyecto está sujeto al desarrollo de un modelo que evalúa y califica las vulnerabilidades de sitios web con el fin de poderlas clasificar y clasificar, así poder evaluar su impacto. Dicho Modelo tendrá un tiempo estimado de cuatro meses para su desarrollo.

En el proyecto se identificarán las metodologías aplicables para la identificación de vulnerabilidades en ciber seguridad y los modelos que manejan dichas metodologías y como

las clasifican, para generar una matriz con las características de cada metodología. Por consiguiente, se identifica las metodologías para calificar y clasificar las vulnerabilidades y su impacto, con el fin de analizar qué características de cada metodología se puede aplicar al modelo que se va a desarrollar y el valor agregado que este puedes brindar en el entorno colombiano.

En el desarrollo del modelo se tendrán en cuenta modelo matemáticos probabilísticos con el fin de adaptar el modelo con las características necesarias al entorno colombiano. Por último, se validará el dicho modelo por medio de una prueba piloto en la empresa Mac Center en Bogotá Colombia.

1.3. PLANTEAMIENTO DEL PROBLEMA

1.3.1. Antecedentes del problema

El origen de la seguridad de la información surge con la necesidad de asegurar los procesos y actividades de las compañías y por la incapacidad de invertir en los procesos tanto productivos como comerciales (School, 215).

Por estas razones surge la necesidad de buscar personas capacitadas, de preferencia externas (imparciales), para que se desarrollen mecanismos de supervisión, vigilancia y control que integran y desempeñan funciones relevantes para la empresa (Control, 2015).

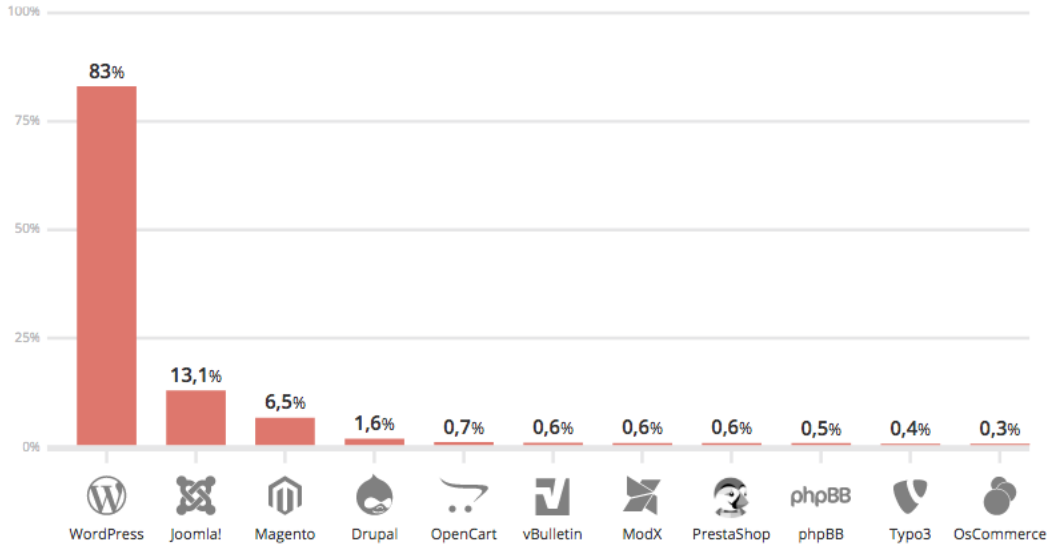
Hoy en día con los avances de las tecnologías de la información e internet, la seguridad de la información ha tomado gran importancia para las empresas ya que la información que

estas tienen de su negocio es un activo de los más importantes. En este sentido las organizaciones día a día se enfrentan a diversos problemas.

La seguridad de la informática es de vital importancia para el buen desempeño de los sistemas de información, esta deberá comprender no sólo la evaluación de los equipos de cómputo, de un sistema o procedimiento específico, sino que además deberá evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información (Ballestas, 2016).

En la figura 1se muestran las plataformas web hackeadas y el porcentaje de ellas más expuestas en el año 2017.

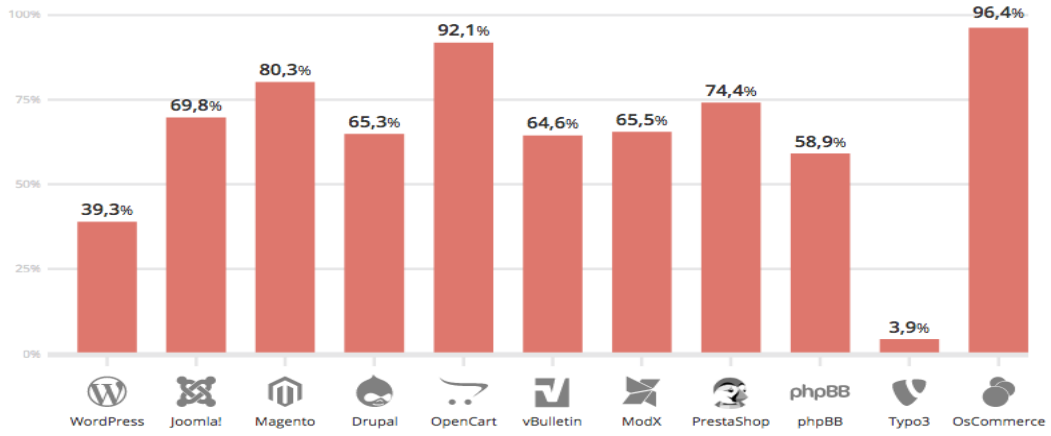
Figura 1: distribución de sitios web hackeados en 2017.



Fuente: http://www.computing.es/seguridad/informes/1101962002501/consecuencias-de-ciberataques-mas-afectan-empresas.1.html

Por otro lado, se identificó que las plataformas más desactualizadas son opencart y oscommerce según la figura 2.

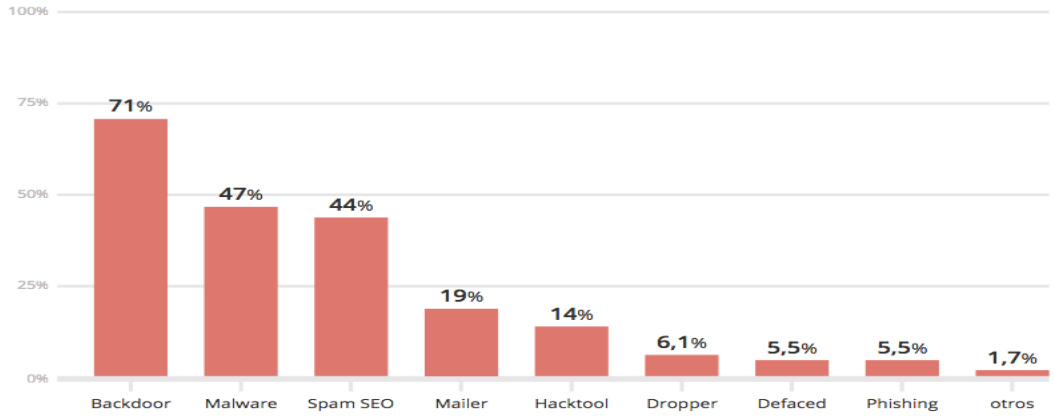
Figura 2: plataformas desactualizadas.



Fuente: http://www.computing.es/seguridad/informes/1101962002501/consecuencias-de-ciberataques-mas-afectan-empresas.1.html

Con respecto a las plataformas más vulnerables se tienen los malware mas comunes como se ve en la figura 2.

Figura 3: distribución de las familias de malware.



Fuente: http://www.computing.es/seguridad/informes/1101962002501/consecuencias-de-ciberataques-mas-afectan-empresas.1.html

Por lo tanto, como la seguridad de la informática se ha vuelto un proceso que se ejecuta de manera global, se han venido desarrollando herramientas y metodologías para gestionarla, una de estas es Owasp.

Por lo anterior, se busca realizar un modelo para el cálculo del nivel de seguridad en sitios web, basado en el top 10 de vulnerabilidades de Owasp de 2017 para la ejecución y validación de pruebas de seguridad aplicadas a los controles establecidos para la tecnología, promoviendo la seguridad en los procesos de TI (Control, 2015).

Ningún país u organización está exento de sufrir un ataque cibernético y Colombia no es la excepción; en agosto del 2016 hasta el mismo mes de este año del 2017 "*se han presentado un total de 198 millones de ataques, según lo revela un informe de la firma de ciberseguridad Digiware. De acuerdo con la compañía, diariamente se registran en promedio 542.465 incidentes y el impacto de los delitos informáticos ha generado pérdidas por 6.179 millones de dólares en el país*".

El sector financiero es el más afectado por los delitos informáticos en el país, con 214.600 ataques por día, seguido de telecomunicaciones, con 138.329; Gobierno, con 83.756 e industria, con 51.263 casos. Casos como el del ransomware de 2017 en Colombia genero grandes pérdidas pero son pocas las empresa que reconocieron que fueron atacadas (Moyano, 2017).

Por todo lo anterior se ha vuelto de gran importancia los análisis previos de las vulnerabilidades y amenazas que se puedan convertir en riesgos potenciales para una organización.

1.3.2. Formulación de problema

La seguridad informática en internet es algo determinante, así como las aplicaciones y sitios web que están en internet que en este momento son una de las mayores preocupaciones de los desarrolladores, dado las deficiencias en seguridad y vulnerabilidades de código que se presentan.

No obstante, se han desarrollado herramientas que apoyan la seguridad dentro de las organizaciones, pero son pocas las herramientas que ayudan a calificar las vulnerabilidades en las aplicaciones web en Colombia, por lo que surge la idea de plantear un modelo para calcular el nivel de seguridad en aplicaciones web.

1.3.3. Pregunta de investigación

¿Cómo debe ser y que características tiene un modelo para el cálculo del nivel de seguridad en un sitio web ayudara a optimizar la evaluación de las vulnerabilidades?

1.3.4. Variables del problema

Teniendo en cuenta la importancia que está tomando la seguridad de la información en Colombia y la necesidad de gestionar correctamente las buenas prácticas y modelos en las compañías se establecen las variables descritas a continuación.

Tabla 1: variables del problema Fuente: los autores.

Variable	Descripción
Modelo	Pautas o buenas prácticas para mejorar un entorno.
Vulnerabilidad	Es una debilidad del sistema informático que puede ser utilizada para causar un daño.
Amenaza	Es una entidad externa que se aprovecha de una vulnerabilidad para causar daño.
Activos	Son los bienes, derechos y otros recursos de los que dispone o dispondrá una empresa.
Información	Es un conjunto organizado de datos procesados.
seguridad	Es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información.

Fuente: los autores.

1.4. JUSTIFICACIÓN

Los avances tecnológicos han sido de gran importancia para las compañías ya que facilitan la gestión de muchos procesos existentes y han optimizado tiempos y calidad de estos, pero todo el apogeo que está teniendo la tecnología, también ha llevado a descuidar un poco la ciberseguridad, permitiendo aprovechar las vulnerabilidades del software para realizar daños a las organizaciones (Definiciones.es, 2015).

En el desarrollo del proyecto se tiene como objetivo crear un modelo para categorizar las vulnerabilidades de los sitios web según el entorno en que se en cuenta para así poderlas calificar, no obstante, en la actualidad se encuentran modelos que realizan esta labor, pero no se encuentra un modelo que tenga encuentra variables geográficas y el sector empresarial. Este Modelo ayudará a la calificación de las vulnerabilidades en el entorno

colombiano y según el sector empresarial al que pertenezca cierta empresa con su sitio web (Control, 2015).

La seguridad de la información en la actualidad presenta un reto para las compañías por lo que han desarrollado diferentes herramientas y buenas prácticas para mejorarla al interior de estas. Este proyecto tiene la finalidad ayudar en la calificación de vulnerabilidades en sitios web, para crear nuevas formas de abordar el análisis de las vulnerabilidades de ciber seguridad, basándonos en los parámetros de Owasp.

1.5. OBJETIVOS

1.5.1. Objetivo general

Desarrollar un modelo para calcular el nivel de seguridad en sitios web, basado en el top 10 de vulnerabilidades en 2017 por owasp.

1.5.2. Objetivos específicos

- Identificar los modelos aplicables para evaluar las vulnerabilidades de la ciber seguridad.

- Analizar los resultados de los marcos de referencia en cuanto a la evaluación de vulnerabilidades de sitios web.

- Desarrollar un Modelo que evalué y califiqué las vulnerabilidades de los sitios web.

- Verificar el modelo propuesto para la evaluación y calificación de vulnerabilidades de sitios web por medio de una prueba piloto.

2. MARCOS DE REFERENCIA

2.1. MARCO CONCEPTUAL

2.1.1. CVE

Es una lista de vulnerabilidades de seguridad de la información públicamente conocidas. Es quizás el estándar más usado. Permite identificar cada vulnerabilidad, asignando a cada una un código de identificación único (CVE, 2017).

2.1.2. CVSS

Es un sistema de puntuación de vulnerabilidad que proporciona una forma de capturar las características principales de una vulnerabilidad y producir una puntuación numérica que refleje su gravedad (CVSS, 2017).

2.1.3. OSWASP

OWASP es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro. La Fundación OWASP es un organismo sin ánimo de lucro que apoya y gestiona los proyectos e infraestructura de OWASP (owasp, 2017).

2.1.4. ISACA

Organización que ayuda a los profesionales globales a liderar, adaptar y asegurar la confianza en un mundo digital en evolución ofreciendo conocimiento, estándares, relaciones, acreditación y desarrollo de carrera innovadores y de primera clase. Establecida en 1969, ISACA es una asociación global sin ánimo de lucro de 140 000 profesionales en 180 países (ISACA, 2016).

2.1.5. COBIT

Es el marco aceptado internacionalmente como una buena práctica para el control de la información, TI y los riesgos que conllevan. COBIT se utiliza para implementar el gobierno de IT y mejorar los controles de IT. Contiene objetivos de control, directivas de aseguramiento, medidas de desempeño y resultados, factores críticos de éxito y modelos de madurez (ISACA, 2016).

2.1.6. ISO 27001

Es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa (ISOTools, 2014).

2.1.7. ISO 27005

La norma ISO 27005 contiene diferentes recomendaciones y directrices generales para la gestión de riesgo en Sistemas de Gestión de Seguridad de la Información. Puedes conocer más sobre la norma ISO 27005 en el siguiente post ISO/IEC 27005. Gestión de riesgos de la Seguridad la Información (ISOTools, 2014).

2.1.8. ISO 27004

Medición de la Seguridad de la Información facilita una serie de mejores prácticas para poder medir el resultado de un SGSI basado en ISO 27001 (ISOTools, 2014).

2.1.9. RIESGO

La posibilidad de que suceda algo que tendrá un impacto sobre los objetivos. Se lo mide en términos de consecuencias y probabilidades (Definiciones.es, 2015).

2.1.10. AMENAZA

Se define como un peligro potencial a la información a sistema. Una amenaza se presenta cuando un atacante identifica una vulnerabilidad sobre un activo y es usada para generar daños que afectan la compañía (Mendoza, 2015).

2.1.11. VULNERABILIDAD

Una vulnerabilidad es una debilidad a nivel de software, hardware, procedimientos o error humano que permite a un atacante aprovecharla para causar daño. La vulnerabilidad de caracteriza por ausencia en controles de seguridad que permite ser explotada (Mendoza, 2015).

2.1.12. PROBABILIDAD

La probabilidad de un evento específico o resultado, medido por el coeficiente de eventos o resultados específicos en relación con la cantidad total de posibles eventos o resultados. La probabilidad se expresa como un número entre 0 y 1, donde 0 indica un evento o resultado imposible y 1 indica un evento o resultado cierto (Mendoza, 2015).

2.1.13. FRECUENCIA

Una medida del coeficiente de ocurrencia de un evento expresado como la cantidad de ocurrencias de un evento en un tiempo dado (Mendoza, 2015).

2.1.14. SEGURIDAD DE LA INFORMACIÓN

Cuando existe una información y la misma tiene una relevancia especial en un contexto determinado y que, por tanto, hay que proteger (Definiciones.es, 2015).

2.1.15. SITIO WEB

Es un conjunto de archivos electrónicos y páginas web referentes a un tema en particular, alojada en el ciber espacio, a los cuales se puede acceder a través de un nombre de dominio y dirección en Internet específicos (MinTic, 2016).

2.1.16. NIST 800-55

Describe un enfoque para el desarrollo e implementación de la seguridad de la información, contiene un programa de medición para desarrollar, seleccionar e implementar sistemas de información y si seguridad, guía a una organización sobre cómo identificar la idoneidad de la seguridad en el lugar Controles, políticas y procedimientos mediante el uso de medidas (NIST, 2008).

2.1.17. ISO 27004

La norma ISO27004 posibilita una variedad de mejores prácticas para la medición de los resultados de un Sistema de Gestión de la Seguridad de la Información (SGSI) en ISO 27001. Este estándar especifica cómo estructurar el sistema de medición, cuáles son los parámetros a medir, cuándo y cómo medirlos. Además, ayuda a las empresas al establecimiento de objetivos relacionados con el rendimiento y los criterios de éxito.

2.1.18. ACTIVO

Se considera un activo a aquello que es de alta validez y que contiene información de vital la cual es importante proteger (Ballestas, 2016).

2.2.MARCO TEÓRICO

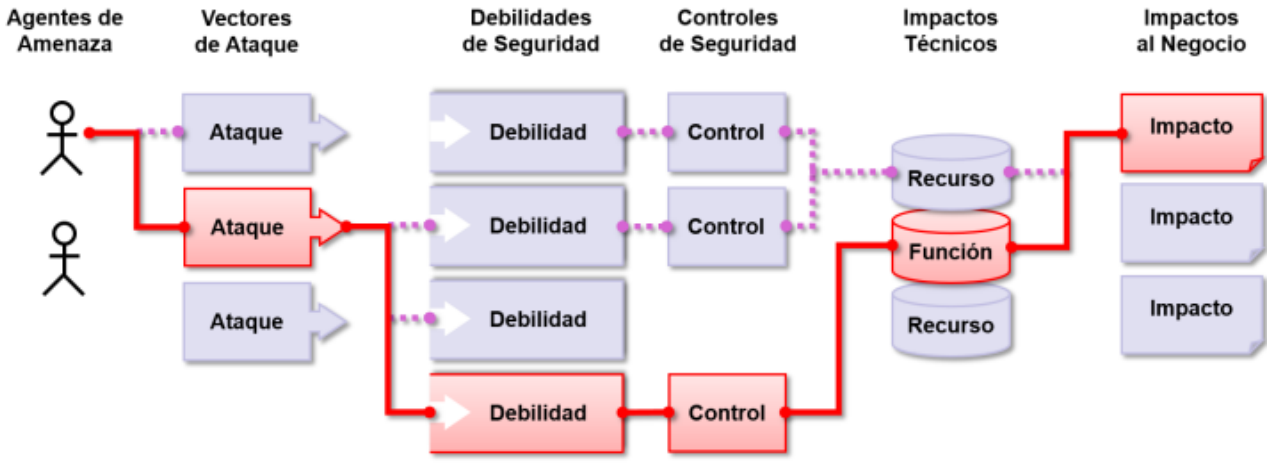
2.2.1. OWASP.

El Proyecto Abierto de Seguridad en Aplicaciones Web (OWASP por sus siglas en inglés) es una comunidad abierta dedicada a permitir que las organizaciones desarrollen, adquieran y mantengan aplicaciones y APIs en las que se pueda confiar (School, 215).

OWASP, tiene herramientas y estándares de seguridad en aplicaciones. Dentro de estas está el análisis de vulnerabilidades que se presenta como el top 10 de vulnerabilidad en cada año. El sistema que se da para aplicar el top 10 y el análisis de vulnerabilidades tiene en cuenta

lo mostrado en la figura 4.

Figura 4: relación de metodología de owasp



Fuente: https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

Se investigan los vectores de ataque según lo reportado por las organizaciones y caso que se tengan establecidos de ataques, paso siguiente se analiza que debilidad se aprovechó o que controles se traspasaron con el ataque, para finalmente evaluar los impactos que genero este ataque a nivel técnico y del negocio.

Los continuos cambios en la tecnología y la entrada del internet se han acelerado en los últimos cuatro años, por lo que el top 10 de owasp cambio. Se estructuro un modelo actualizado completamente el Top 10 de OWASP, se modernizo la metodología utilizada, se trabajó con la comunidad de especialistas para reorganizamos los riesgos por lo que se el top se actualizo como se muestra en la figura 5.

Figura 5:cambios de las versiones de owasp

OWASP Top 10 - 2013 (Versión anterior)	⇒	OWASP Top 10 - 2017 (Versión actual)
A1-Inyección	⇒	A1: 2017-Inyección
A2-Broken Authentication y Session Management	⇒	A2: 2017-Autenticación rota
A3-Cross-Site Scripting (XSS)	⇘	A3: exposición a datos sensibles a 2017
Referencias de objetos directos no seguros A4 - [Fusionada + A7]	∪	A4: Entidades Externas 2017-XML (XXE) [NUEVO]
A5-Misconfiguración de seguridad	⇘	A5: 2017-Control de acceso roto [Fusionada]
Exposición de datos sensibles a A6	⇗	A6: 2017-Misconfiguración de seguridad
Control de acceso del nivel de función A7-Missing - [Merged + A4]	∪	A7: 2017-Cross-Site Scripting (XSS)
A8-Cross-Site Request Forgery (CSRF) [Abandonado]	☒	A8: 2017-Deserialización insegura [NUEVO, Comunidad]
A9: uso de componentes con vulnerabilidades conocidas	⇒	A9: 2017: uso de componentes con vulnerabilidades conocidas
A10-Redirecciones y reenvío no validados [Abandonado]	☒	A10: 2017-Insufficient Logging & Monitoring [NUEVO, Comunidad]

Fuente: https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

La temática de análisis de vulnerabilidades de owasp es realizar un levantamiento de información con el que se interpreta el negocio, analizar las vulnerabilidades para ver que podría llegar a afectar los sistemas, definir lo objetivos base para evitar el riesgo, verificar los posibles ataques y que riesgos conllevan y así analizar los resultados del proceso y sus mitigaciones con el fin de generar un documento sobre dichas falencias del sistema como se muestra en la figura 6.

Figura 6: fases de las vulnerabilidades en Owasp

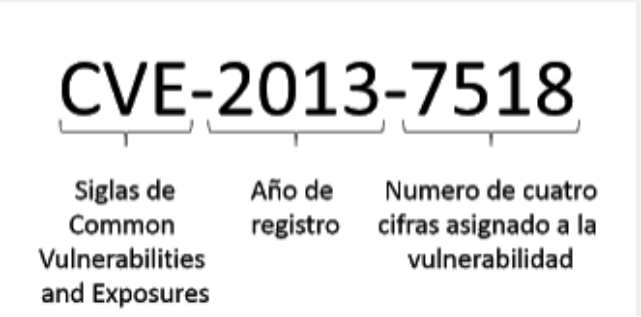
Fuente: https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

2.2.2. CVE.

CVE (Common Vulnerabilities and Exposures) es una lista de vulnerabilidades de seguridad de la información públicamente conocidas. Es quizás el estándar más usado. Permite identificar cada vulnerabilidad, asignando a cada una un código de identificación único. Se conoce como identificador CVE (CVE-ID) y está formado por las siglas de este diccionario seguidas por el año en que es registrada la vulnerabilidad o exposición y un número arbitrario de cuatro dígitos (CVE, 2017).

CVE basa su investigación y calificación de vulnerabilidades en los estándares de CVSS para dale un valor tangible a las vulnerabilidades que se registran en su sistema usa la lógica y la forma de valorar cada vulnerabilidad. Cuya consecución es un punto a favor para todas las comunidades de ciber seguridad y CVE (CVE, 2017)platea un código para las vulnerabilidades encontradas como se muestra en la figura 7.

Figura 7:codificación de CVE.



Fuente: https://cve.mitre.org/cve/cna.html

2.2.3. CVSS.

CVSS (Common Vulnerability Score System). Como su nombre lo indica es un Sistema de puntuación para las vulnerabilidades comunes en el contexto de la ciber seguridad. En este contexto, una vulnerabilidad se define como una debilidad que se encuentra en un activo o en un control y que puede ser explotada por una o más amenazas, lo que deriva en un riesgo de seguridad (CVSS, 2017).

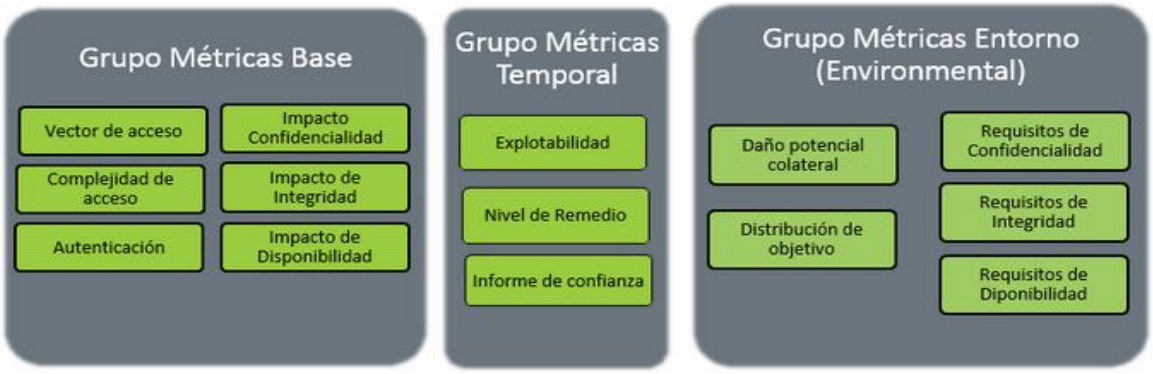
Por lo tanto, el CVSS es un sistema que está diseñado para proveer un estándar que permite medir el impacto derivado de las vulnerabilidades tecnológicas, puede estimar cuantificar el impacto que puede representar dichas vulnerabilidades.

CVSS es un framework abierto y se ha utilizado mundialmente, contiene métricas para comunicar las características, impacto y la severidad de las vulnerabilidades en la parte TI

La organización responsable de este marco es el Forum Incident response and Security Teams (FIRST) en los últimos años han trabajado para dar a conocer la nueva versión del marco de referencia ya que ayudará a las compañías para mejoras sus políticas de seguridad y dar valor a las organizaciones (CVSS, 2017).

En la figura 8 se muestra un grupo de métricas base, grupo de métricas temporales y grupo de métricas del entorno que utiliza el modelo del CVSS

Figura 8: modelo de CVSS.



Fuente: https://www.welivesecurity.com/la-es/2014/08/04/vulnerabilidades-que-es-cvss-como-utilizarlo/

Las métricas base se usan para todo tipo de vulnerabilidades, que indican valores estándar que afectan el entorno y la seguridad de un sistema de información, las métricas temporales son valores que afectan directamente el sistema, pero pueda cambiar en el tiempo o ser afectada por un evento externo o interno, por último, están las métricas de entorno que evalúan las variables del entorno del sistema y el impacto que pueden tener.

2.2.4. NIST 800-55

Da un alcance del programa de medición de seguridad de la información. El alcance del programa de medición de seguridad de la información puede adaptarse a una variedad de contextos (NIST, 2008), Cuantificando el rendimiento del nivel de seguridad del sistema de información para verificar y analizar los siguientes puntos:

- Cuantificar la integración de la seguridad de la información en el SDLC durante la información.

- Analiza los procesos de desarrollo de sistemas y software.
- Cuantificación el rendimiento de seguridad de la información en toda la empresa
- El alcance puede abarcar unidades organizativas, sitios u otras construcciones organizativas como:
    - necesidades de los interesados
    - metas y objetivos estratégicos
    - Entornos operativos
    - Prioridades de riesgo
    - Madurez del programa de seguridad de la información.

2.2.5. ISO 27004

El estándar concreto cómo configurar el programa de medición, qué parámetros medir, asegurando y cómo medirlos, y ayuda a las empresas a crear objetivos de rendimiento y criterios de éxito.

La medición de la seguridad aporta protección a los sistemas de la organización y da respuesta a las amenazas de la misma. (Tools, 2016)

Expone que el tipo de medidas requeridas dependerá del tamaño y complejidad de la organización, de la relación coste beneficio y del nivel de integración de la seguridad de la información en los procesos de la propia organización. La norma **ISO27004** establece cómo se deben constituir estas medidas y cómo se deben documentar e integrar los datos obtenidos en el SGSI. (Tools, 2016)

2.3.MARCO JURÍDICO

2.3.1. DERECHOS DE AUTOR

La normalización con respecto a los derechos que adquiere el autor de soporte lógico o de software, y las consecuencias jurídicas que sobrevienen a su licenciamiento, transferencia, distribución, reproducción o, en general, cualquier utilización que se haga de ellos, están contempladas en la Ley 23 de 1982, la Decisión 351 del Acuerdo de Cartagena y el Decreto 1360 de junio 23 de 1989 (Definiciones.es, 2015).

Según el Acuerdo de Cartagena, tanto los programas operativos como a los aplicativos, ya sea en forma de código fuente o código objeto, están cobijados por la Ley, que establece, entre otras, las siguientes normas: El propietario de un ejemplar de programa de computador de circulación lícita, puede realizar copias o adaptaciones del mismo, siempre y cuando sean indispensables para su utilización o se realicen con fines de archivo o sustitución del original en caso de daño o pérdida (Definiciones.es, 2015).

Por lo que en nuestro desarrollo del prototipo estamos seguros de que los derechos que sobre él tiene se respetarán a nivel nacional e internacional.

2.4.MARCO GEOGRÁFICO

El area geografica en el cual se realizará la investigacion es en la capital de Bogotá D.C., sobre sitios web en diferentes organizaciones y tomando como caso de estudio el sitio Web de Mac Center Ubicado en la Cra 14 No 81-19 Barrio El Retiro como se ilustra en la figura 9.

Figura 9: mapa de Bogotá.

Fuente: https://www.google.com/maps/place/Bogot%C3%A1/@4.6482837,-74.2478965,11z/data=!3m1!4b1!4m5!3m4!1s0x8e3f9bfd2da6cb29:0x239d635520a33914!8m2!3d4.7109078!4d-74.0720558

2.5. ESTADO DEL ARTE

El internet es la red mundial de comunicaciones formada por miles de redes telefónicas e informáticas, que están conectadas entre sí. "*El inicio de Internet se remonta a los años 60. En plena guerra fría, Estados Unidos crea una red exclusivamente militar, con el objetivo de que, en el hipotético caso de un ataque ruso, se pudiera tener acceso a la información militar desde cualquier punto del país"*. El objetivo de internet es ser él medio para compartir información o recursos. Desde la aparición del internet los ataques o incidentes de seguridad a los sistemas de información han incrementado un 13% en 2015. De acuerdo con una investigación realizada por ESET, esto ha aumentado en gran medida la necesidad

de las organizaciones de proteger sus sistemas de información y minimizar riesgos (Etico, 2014). Es importante tener en cuenta que ningún sistema es infalible ya que todo sistema por más sofisticado que sea puede ser vulnerado de alguna manera. El reto es asignar estratégicamente los recursos para cada equipo de seguridad y bienes que intervengan, basándose en el impacto potencial del negocio, respecto a los diversos incidentes que se deben resolver. Según Pontus Johnson y Robert Lagerstr¨om en su artículo ¿Puede confiar el sistema de puntuación de vulnerabilidad común?, se realiza un análisis sobre el sistema CVSS para analizar la confiabilidad del mismo, ya que ha sido criticado por la falta de validez y relevancia profesional. Se concluye que, con la excepción de algunas dimensiones, el CVSS es bastante confiable y las bases de datos son relativamente consistentes no obstante algunas son más consistentes que otras como por ejemplo la NVD es la mejor y OSVDB es la peor de las bases evaluadas (tor, 2016). Por otro lado, en una contenéis del CVSS se evidencia que es más relevantes de la versión 2 del CVSS y la versión 3 del CVSS y de qué forma las organizaciones las deben tomar para sacarles el mejor provecho y poderlas entender según menciona la publicación titulada Generaciones del Sistema de Puntuación de Vulnerabilidades Comunes (CVSS) - utilidad y deficiencias (CVSS, 2017).

históricamente las compañías de TI usan sus propios métodos para la calificación de vulnerabilidades de software sin detallar sus criterios o procesos, por lo tanto, genera un problema importante para los usuarios. Por lo que se debe promover el por qué se debe manejar el CVSS que empresas lo manejan y que beneficios se tienen al implementarlo.

Las etapas propuestas por **ISO 27004** con el objetivo de medir la eficacia de la seguridad de la información son:

- Selección procesos y objetos de medición.

Las empresas deben definir lo que hay que medir y el alcance de la medida. Sólo se consideran en la medición los procesos bien documentados que son consistentes y repetibles. Objetos de medición puede ser el rendimiento de los controles o de procedimientos, el comportamiento del personal (ISOTools, 2014).

- Definición de las líneas base.

Los valores base que muestran el punto de referencia deben definirse para cada objeto que se está midiendo.

- Recopilación de datos.

Los datos deben ser dimensionales precisos y oportunos. Se pueden emplear técnicas automatizadas de recogida de datos para lograr una recolección estandarizada y presentar informes.

- Desarrollo de un método de medición.

Según **ISO 27004**, la secuencia lógica de operaciones se aplica en diversos atributos del objeto seleccionado para la medición. Se usan indicadores como fuentes de datos para mejorar el rendimiento de los programas de seguridad de la información (Tools, 2016).

- Interpretación de los valores medidos.

Mediante procesos y la tecnología para el análisis y la interpretación de los valores se deben identificar las brechas entre el valor inicial y el valor de medición real.

- Comunicación de los valores de medición.

Los resultados de medición del SGSI se comunicarán a las partes interesadas. Se puede hacer en forma de gráficos, cuadros de mando operacionales, informes o boletines de noticias.

3. METODOLOGÍA

3.1.FASES DEL TRABAJO DE GRADO

Con el fin de cumplir los objetivos de esta investigación y alcance, se definen las siguientes etapas: la primera es la etapa de planeación, luego la etapa de ejecución, siguiendo con la etapa de verificación. En la primera se desarrolla la propuesta y el anteproyecto, la segunda fase que consolida en el desarrollo de las tareas para cumplir cada uno de los objetivos planteados. La fase final correspondiente a la verificar la implementación del trabajo, se aplica desde la fase de planeación con el fin de tomar acciones correctivas sobre el desarrollo de las tareas.

3.2.INSTRUMENTOS O HERRAMIENTAS UTILIZADAS

Los instrumentos que se tendrán en cuenta para esta investigación y alcanzar desarrollar cada uno de los objetivos son el análisis de los marcos de referencia, normas o metodologías asociadas al análisis de vulnerabilidades y su respectiva documentación. Lo primero se debe a la información obtenida mediante las consultas e investigaciones de los marcos teóricos y conceptual. También se investigaciones puntuales para conocer los procesos y modelos que se tengan en el análisis y evaluación de vulnerabilidades en las organizaciones. Por último, se aplicará el modelo obtenido en la empresa MAC center para establecer si el modelo se adecua a los requerimientos actuales de las organizaciones.

4. DESARROLLO DE LA PROPUESTA

4.1. MODELOS APLICABLES PARA EVALUAR LAS VULNERABILIDADES DE LA CIBER SEGURIDAD.

Las vulnerabilidades siempre están presentes y tener un sistema 100% seguro es muy difícil por eso descubrirlas importante, pero poder calificarlas y evaluarlas es importante para el negocio. Por lo que se revisaran los principales marcos de trabajo en lo que se tuvo en cuenta el marco teórico de este proyecto.

Tabla 2. Matriz e categorización de los marcos referenciales. Fuente los autores.

Item	Iso 27004	CVSS	OwasP	Nist 800-55
Concepto del marco de referencia	Incentiva la búsqueda de los factores para analizar las vulnerabilidades, pero no establece como hacerlo.	Establece una serie de métricas para facilitar la búsqueda de vulnerabilidades	Clasifica las vulnerabilidades y amenazas para establecer el riesgo.	Cuantifica el rendimiento de seguridad a nivel del sistema de información.
Detectabilidad de las vulnerabilidades	Gestiona las reglas para encontrar las vulnerabilidades	Gestiona y ayuda a establecer una serie de pasos para evaluar y encontrar las vulnerabilidades	Fomenta la investigación de casos y nuevos patrones para evaluar nuevas vulnerabilidades.	establece la probabilidad que puede tener la vulnerabilidad
Gestión de métricas para reaccionar ante la explotación de vulnerabilidades	Nos da un criterio para poder establecer el grado de explotación.	Se apoya en el criterio y documentación de CVE para ver antecedentes.	Establece un criterio para identificar como se pueden explotar más fácilmente las vulnerabilidades y cómo actuar en dicho caso.	Cuantificación del rendimiento de seguridad de la información en toda la empresa.

Medición del impacto técnico de la vulnerabilidad	Establecer que se debe hacer para el desarrollo de la gestión de riesgos y de planes de continuidad del negocio.	Califica la vulnerabilidad con forme a el impacto de en la seguridad de la información.	Establecer directrices de para identificar los vectores de ataque y recolecta información del manejo que se ha tenido en casos puntuales conforme a una vulnerabilidad.	Establecer criterios para gestionar el impacto técnico con el fin establecer acciones para combatir la explotación de la vulnerabilidad.
Medición de los factores de impacto en el negocio	Indica que hay que gestionar y verificar el impacto a los objetivos del negocio.	Establece un modelo para calificar el posible impacto.	Establecer un criterio general para cada vulnerabilidad que contemplen.	Indica la gestión del impacto y la probabilidad que tenga cada vulnerabilidad para con el negocio.
Impacto en la seguridad de la información	Indica que se debe gestionar cada tema por separado, pero se apoya en otros marcos para completar dicho punto	Establecer un criterio y calificador exclusivo para la disponibilidad, integridad y confidencialidad	Califica la vulnerabilidad después de establecer el vector de ataque.	Fomenta la clasificación de riesgos en torno a la disponibilidad, integridad y confidencialidad de la información.
Alcance	Guiar a una organización sobre qué hacer para identificar las vulnerabilidades en seguridad de la información.	Desarrolla un sistema de puntación para calificar las vulnerabilidades técnicas en cualquier ambiente tecnológico.	Desarrolla un sistema para analizar las vulnerabilidades en sitios web.	Establece y sistema de puntos para calificar el nivel de seguridad de la información.
Componentes o estructura	Contiene 3 anexos el A que es un extracto de la ISO 27001 donde clasifica cada punto y vulnerabilidad el B que es un actuar en base a casos prácticos y el C que es una guía de prácticas y de normas anexas para manejar las vulnerabilidades.	Los componentes son básicos que evalúa el ambiente y la seguridad de la información, temporales donde se evalúa la explotabilidad y la confianza y finalmente el componente de entorno que evalúa los vectores de ataque.	Actúa sobre los vectores de ataque, la explotabilidad de la vulnerabilidad web, prevalecía detectabilidad e impacto técnico.	Su estructura está conformada por la gestión de riesgo y controles que actúan para la priorización y monitoreo continuo de cada riesgo y su respectivo control
Métricas de la norma	Incluye una Base lógica, monitorizar, quién y qué medir, cuándo monitorizarlo, medirlo y evaluarlo.	Gestiona la calificación de las métricas de explotabilidad, impacto, Nivel de curación, Confianza del anuncio, Daño	Identifica como métricas la explotabilidad de las vulnerabilidades, prevalecía en el tiempo y	Platea que las métricas deben ser gestionadas acordes con las políticas de seguridad y

		colateral potencial, Distribución de objetivos, Modificadores de las puntaciones de impacto.	defectibilidad, impacto técnico y del negocio	privacidad de la compañía, haciendo una evaluación de riesgos y calificando de 1 a 10

Fuente: los autores

4.2. ANÁLISIS DE MARCOS DE REFERENCIA EN CUANTO A LA EVALUACIÓN DE VULNERABILIDADES DE SITIOS WEB.

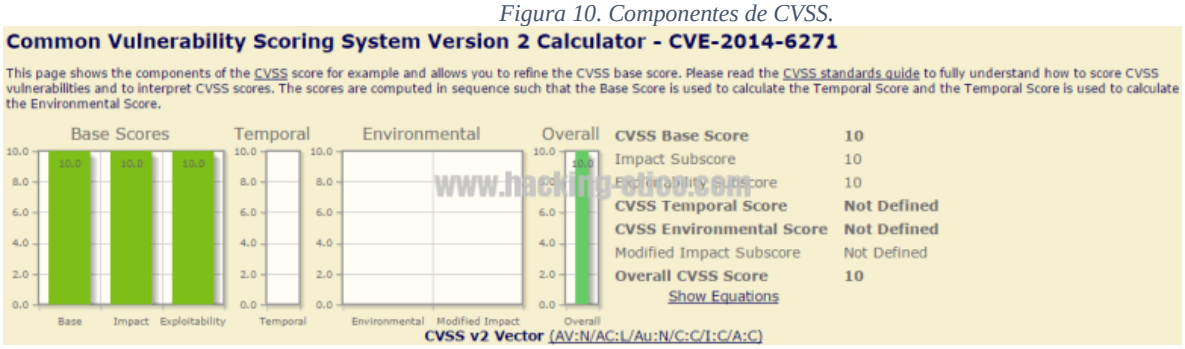
Según el punto anterior se pudo encontrar que la ISO 27004 es una norma para gestionar las vulnerabilidades de la tecnología, pero solamente se limita a dar guías y pautas para mejorar la seguridad en el ambiente empresarial en la web, CVSS es un estándar donde analiza y califica las vulnerabilidades de los sistemas de información y como pueden llegar a impactar directamente en un ambiente empresarial especifico, Owasp es un marco de trabajo para analizar y evaluar las vulnerabilidades más frecuentes y explotadas en aplicaciones web, pero analiza el ámbito de la seguridad de la información a nivel mundial, nist 800-55 es una normatividad compuesta de guías para establecer qué nivel de seguridad de la información tiene una organización pero no califica cada vulnerabilidad por aparte, califica los riesgos en las compañías.

Por lo anterior se torna fundamental revisar y tener en cuenta el modelo de calificación de las vulnerabilidades de Oswap y de CVSS ya que están orientados a tener una exactitud para cada una de las vulnerabilidades que se requieran (CVE, 2017).

En consecuencia, a esto se tiene que CVSS utiliza tres métricas básicas para medir el alcance que

puede tener una vulnerabilidad. Podemos verlas en la figura 10.

Figura 10. Componentes de CVSS.



Fuente: https://www.first.org/cvss/specification-document

Métrica Base: Dentro de la métrica base tenemos evaluados aquellos **parámetros que son constantes en el tiempo y el entorno**. Dicha métrica se suele expresar como un vector. Esto es lo que se conoce con el nombre de vector base y serían los siguientes (CVSS, 2017):

- **AV**: Vector de Acceso, es decir, la manera a través de la cual podemos acceder a la vulnerabilidad. En nuestro caso para explotar la vulnerabilidad podemos acceder **desde cualquier red**, no sólo en local (**N**:Network) (CVSS, 2017).
- **AC**: Complejidad de Acceso, es decir, la complejidad que requiere el atacante una vez ha accedido al sistema, en nuestro caso **complejidad baja** (**L**: Low) (CVSS, 2017).
- **Au**: Autenticación, es decir, cuantas veces debe autenticarse el usuario para poder hacer uso de la vulnerabilidad, en nuestro caso **ninguna** (**N**:None) (CVSS, 2017).
- **C**: Impacto de Confidencialidad, es decir, como afecta esta vulnerabilidad en cuanto a la confidencialidad. En este caso el impacto es total, porque podemos ejecutar cualquier código en el sistema, lo que conlleva acceso a cualquier archivo, rompiendo de manera **completa** la confidencialidad del sistema (**C**: Complete) (CVSS, 2017).

- **I**: Impacto de Integridad, es decir, como afecta esta vulnerabilidad en cuanto a la integridad. Al igual que en el caso anterior, tenemos acceso completo a modificar cualquier archivo de tal forma que se rompe este principio **completamente** (**C**: Complete) (CVSS, 2017).
- **A**: Impacto a la Disponibilidad, más de lo mismo, si podemos ejecutar en el sistema cualquier comando podemos echar abajo servicios entre otras cosas. Por tanto, afecta a la disponibilidad de manera **completa** (**C**: Complete) (CVSS, 2017).

Normalmente a la hora de evaluar una vulnerabilidad mediante el CVSS tan sólo se suele valorar la métrica base, ya que las dos siguientes son opcionales y cambiantes en el tiempo.

Métrica Temporal: Esta métrica varía en el tiempo, en ella podemos evaluar varios parámetros como vemos a continuación:

- **Explotabilidad:** se refiere a si existen exploits y si están disponibles, o sólo existen pruebas de concepto, si los exploit sólo existen en algún sistema o por el contrario existe código multiplataforma.
- **Nivel de curación:** hace referencia a la existencia o no de soluciones para corregir dicho bug, si estas provienen de fuentes oficiales o anónimas, o incluso si son soluciones temporales.
- **Confianza del anuncio:** trata de evaluar la veracidad en la existencia de dicha vulnerabilidad, si ha sido confirmada por fuentes oficiales (el responsable del software o sistema) o sólo por grupos independientes de seguridad.

Métrica del entorno: Esta métrica también varía en el tiempo, en ella podemos evaluar varios parámetros relacionados al entorno al cual afecta la vulnerabilidad. Los vemos a continuación (CVSS, 2017):

- **Daño colateral potencial:** hace referencia al daño que puede ocasionar a terceros, como a personas, bienes físicos, la productividad o beneficios.
- **Distribución de objetivos:** aquí medimos la proporción de sistemas vulnerables en el entorno, se suele dar valor numérico entre 0 y 10; y se expresa en intervalos de mínimo y máximo.
- **Modificadores de las subpuntaciones de impacto**: aquí se trata del grado de afectación dentro de los objetivos de la seguridad como son Confidencialidad, Integridad y Disponibilidad. Es decir, mediante estos valores podemos medir cuán importante es para esta vulnerabilidad cada uno de estos parámetros.

Como punto siguiente Owasp se enfoca en identificar los riesgos más críticos para un amplio tipo de organizaciones. Para cada uno de estos riesgos, se proporciona información genérica sobre la probabilidad y el impacto técnico, utilizando el siguiente esquema de evaluación, basado en la Metodología de Evaluación de Riesgos de propuesta por Owasp (owasp, 2017). Descubrir vulnerabilidades es importante, pero poder estimar el riesgo asociado para el negocio es igual de importante. Al inicio del ciclo de vida, uno puede identificar los problemas de seguridad en la arquitectura o el diseño mediante el uso de modelos de amenazas (CVSS, 2017). Más adelante, uno puede encontrar problemas de seguridad utilizando la revisión de código o las pruebas de

penetración . O es posible que los problemas no se descubran hasta que la aplicación esté en producción y esté realmente comprometida.

Para ponderar cada una de las vulnerabilidades del top 10, se desglosan los factores que conforman la "probabilidad" y el "impacto" para la seguridad de la aplicación. Se muestra al probador cómo combinarlos para determinar la gravedad que la vulnerabilidad sea explotada y cumple los siguientes pasos (owasp, 2017):

Paso 1: Identificación de un riesgo

Paso 2: Factores para estimar la probabilidad

Paso 3: Factores para estimar el impacto

Paso 4: Determinación de la gravedad del riesgo

Paso 5: Decidir qué arreglar

Paso 6: Personalización de su modelo de calificación de riesgo

Para finalizar se evidencio que Owasp y CVSS sería los modelos más idóneos para calificar una vulnerabilidad, por ello se utilizara el modelo de Owasp usando sus métricas y complementado con el parámetro base que nos ofrece CVSS.

Comprobando que el impacto de negocio no se aborda de manera concreta en OWASP ni en CVSS se recurre a NIST 800-55 en un apartado y documento acoplado por Mintic Colombia para analizar el riesgo, que puede correr una organización si una vulnerabilidad es explotada por lo que se analizan los siguientes ítem y se califican según lo que cada vulnerabilidad podría afectar (Mintic G. , 2015).

- Procesos
- Operación
- Procesos críticos
- Aplicaciones
- Bases de datos
- Comunicaciones
- Cuartos de maquinas
- equipos
- Recurso humano
- Objetivos Misionales, estratégicos y de negocio

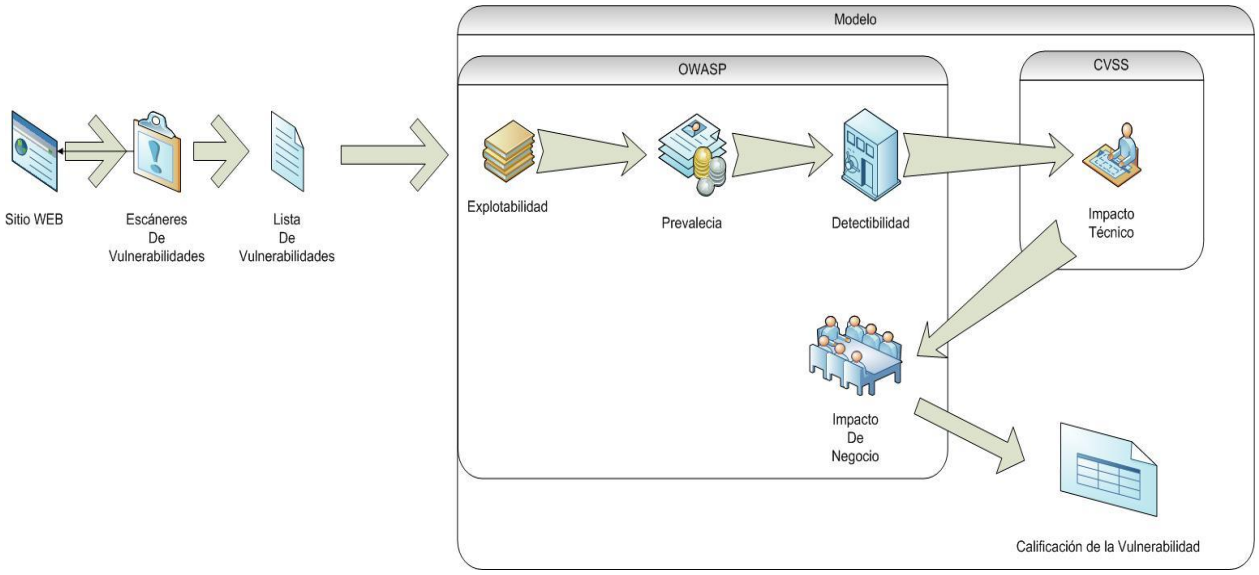
4.3. DEFINICIÓN DEL MODELO PARA CALCULAR EL NIVEL DE SEGURIDAD EN SITIOS WEB.

Este modelo enfoca sus esfuerzos en identificar las vulnerabilidades más críticas para un amplio tipo de organizaciones, para cada vulnerabilidad proporciona información sobre:

- Explotabilidad: revisa en el contexto de la seguridad de la información que tan fácil es explotar la vulnerabilidad detectada.
- Prevalencia de la vulnerabilidad: busca como se puede corregir la vulnerabilidad o que tanto puede proseguir en el tiempo aun con modificación y actualización en el sistema vulnerable.
- Detección de la vulnerabilidad: identifica que tan fácil puede ser detectada la vulnerabilidad en el ambiente de trabajo y en internet.
- Impacto técnico: busca calificar que impacto tendría en el sistema si la vulnerabilidad logra ser explotada.
- Impacto del negocio: Owasp deja este ítem abierto para que cada compañía lo acoja o interprete según la experiencia y objetivos de negocio, no lo incluye en el ámbito para la calificación final de la vulnerabilidad.

Por los puntos anteriores, es indispensable usar el modelo de Owasp para calificar las vulnerabilidades en un ambiente más condensado y específico por lo que el componente de impacto del negocio toma gran valor para incluirlo en la calificación, así como complementar el impacto técnico ya que en ese aspecto se encuentran muchas variables, por lo que en cuanto al impacto técnico se extraerá la calificación directamente de CVSS y adicional la calificación del impacto de negocio para cada vulnerabilidad encontrada en el sitio web se realizará de acuerdo a OWASP, como se muestra en la figura 11.

Figura 11 Modelo propuesto para calificación de vulnerabilidades. Fuente los Autores



Fuente: los autores.

Para evaluar cada vulnerabilidad encontrada en el sitio web a analizar se harán de la siguiente manera, donde se califica la explotabilidad, prevalencia y detectabilidad cada una en un rango de 0 a 3 y se promedian los 3 valores para después multiplicarlos por el impacto técnico que se califica según las métricas de CVSS que tienen una escala de 0 a 10 y luego por el impacto de negocio calificado de 0 a 30.

Tabla 3. Variables de la fórmula para calificar la vulnerabilidad.

No	VARIABLE	ESCALA
1	Explotabilidad	De 0 – 3
2	Prevalencia	De 0 – 3
3	Detectabilidad	De 0 – 3
4	Impacto técnico	De 0 – 10
5	Impacto de negocio	De 0 – 30

Fuente los autores.

El impacto de negocio se reconoce según las siguientes métricas basadas en el modelo NIST 800-55 implementado por Mintic en Colombia, y para el caso del modelo propuesto se califica cada variable de 0 a 3, para indicar cada el nivel para nulo se expresa con 0, para bajo se expresa con 1, medio se expresa con 2 y alto se expresa con 3 y el valor de cada variable se suma para dar un total máximo de 30 puntos.

Tabla 4. Variables para el impacto de negocio

No	VARIABLE	ESCALA
1	Procesos	0-3
2	Operación	0-3
3	Procesos críticos	0-3
4	Aplicaciones	0-3
5	Bases de datos	0-3
6	Comunicaciones	0-3
7	Cuartos de maquinas	0-3
8	equipos	0-3
9	Recurso humano	0-3
10	Objetivos Misionales, estratégicos y de negocio	0-3

Fuente los autores.

Para la implementación del modelo propuesto para calificar cada vulnerabilidad se inicia con un escaneo del sitio web a calificar donde se usan herramientas como IronWasp y OwaspZap que son escáneres de vulnerabilidades orientados a sitios web basados en OWASP, de este escaneo se obtienen las vulnerabilidades que serán insumo del modelo que se propone, posteriormente se buscan a que categoría pertenece la vulnerabilidad en el top 10 de vulnerabilidades de OWASP y

su código correspondiente en CVE que la documenta la califica. Se toman dichos valores para el modelo y se aplica siguiente formula es la para dar el resultado total de la calificación de una sola vulnerabilidad.

((explotabilidad + prevalencia+ detectabilidad) /3) * impacto técnico) + impacto de negocio) /6

Las variables explotabilidad, prevalencia y detectabilidad se evalúan exactamente igual que en Owasp calificando de 0 a 3 según su clasificación en el documento del top 10 de OWASP 2017 para después calificar el impacto técnico según CVSS cuya calificación se da de 0 a 10 teniendo en cuenta la calificación de la base de datos de CVE para cada vulnerabilidad según su código que se consulta en "https://cve.mitre.org/cve/search_cve_list.html" que documenta y califica la vulnerabilidad. Para el impacto de negocio se tiene una escala de 0 a 3 donde se califica cada variable de la tabla 4 y da un total máximo de 30.

Luego de obtener el resultado de la calificación de cada vulnerabilidad en una escala de 0 a 10 como se ve en la tala 5, se estable la calificación general del sitio que suma la calificación de las vulnerabilidades y las divide en el número de vulnerabilidades, se saca un promedio básico y se obtiene el nivel de vulnerabilidad del sitio como se ve en la siguiente formula.

$$(Vulnerabilidad\ 1 + vulnerabilidad\ 2 + \cdots + vulnerabildad\ n) \text{ / n}$$

Tabla 5. Escala de calificación de vulnerabilidades según CVSS.

Calificación	Escala
0	Nula
0.1 - 3.9	Baja
4.0 - 6.9	Media
7.0 - 8.9	Alta
9.0 - 10	Critica

Fuente. https://nvd.nist.gov/CVSS.

4.4. CASO DE PRUEBA

El proyecto está orientado en la zona del distrito de Bogotá, el modelo se aplicará en la compañía Mac Center ubicada su sede principal en la ciudad de Bogotá, ofrece una experiencia Premium en la compra de productos Apple en las tiendas se puede encontrar accesorios de las mejores marcas de tecnología, servicio técnico confiable y cursos de entrenamiento sin costo, en toda Colombia, tiene sus oficinas principales y administrativas en el sector de Usaquén. Uno de los procesos que maneja la empresa es la seguridad de la información, se aplicara el modelo propuesto en el sitio Web de la compañía que es una de las plataformas más importantes porque es el primer contacto que tienen los clientes con la compañía y además un punto muy relevante es que manejan por medio de este sitio Web compras Online, de este modo buscamos medir el nivel de seguridad de su sitio Web basado en el top 10 de OWASP.

Herramientas de Escaneo:

Owasp zap: Open Web Application Security Project (OWASP) OWASP ZAP es un escáner de seguridad web de código abierto. Pretende ser utilizado como una aplicación de seguridad y como una herramienta profesional para pruebas de penetración. Es uno de los proyectos más activos de

OWASP. y se le ha dado un estatus de desarrollo insignia, esta herramienta usa el top 10 de owasp para calificar y clasificar las vulnerabilidad en baja, media y alta.

IronWasp: IronWASP es una herramienta gratuita y de código libre que se encarga de realizar una completa auditoría de seguridad en servicios web. Algunas de las características de IronWASP es que tiene un motor de escaneo muy potente y efectivo basado en la clasificación de las vulnerabilidades del top 10 de owasp, además es capaz de grabar la secuencia de login de las páginas web y usarlo en escáneres de vulnerabilidades y otros test automatizados.

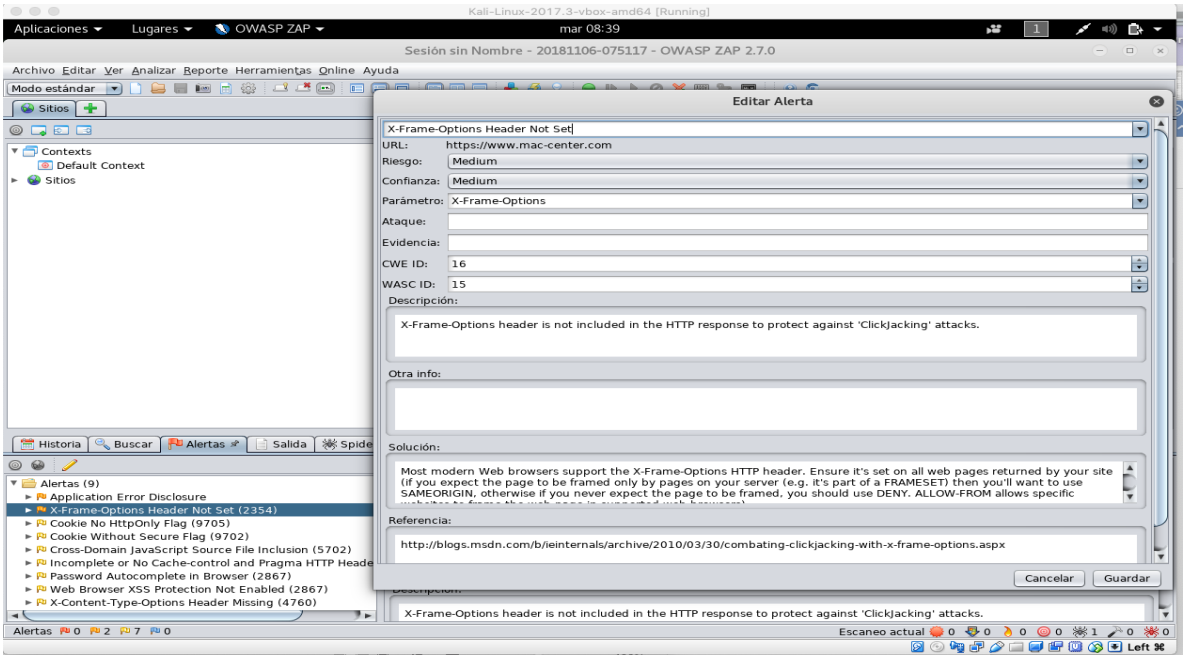
Inicio de la prueba:

Se realizan dos escaneos sobre la página https://www.mac-center.com con autorización de la compañía para el proyecto el cual se enfoca en alertas medias y altas las cuales son de relevancia para la compañía y establecer un alcance medible para el plazo del proyecto. Se corre la herramienta OwaspZap e IronWasps

Con la herramienta de Owasp-Zap se obtuvieron los siguientes resultados:

- X-Frame-Options, vulnerabilidad clasificada por la herramienta como de impacto como se muestra en la figura 12.

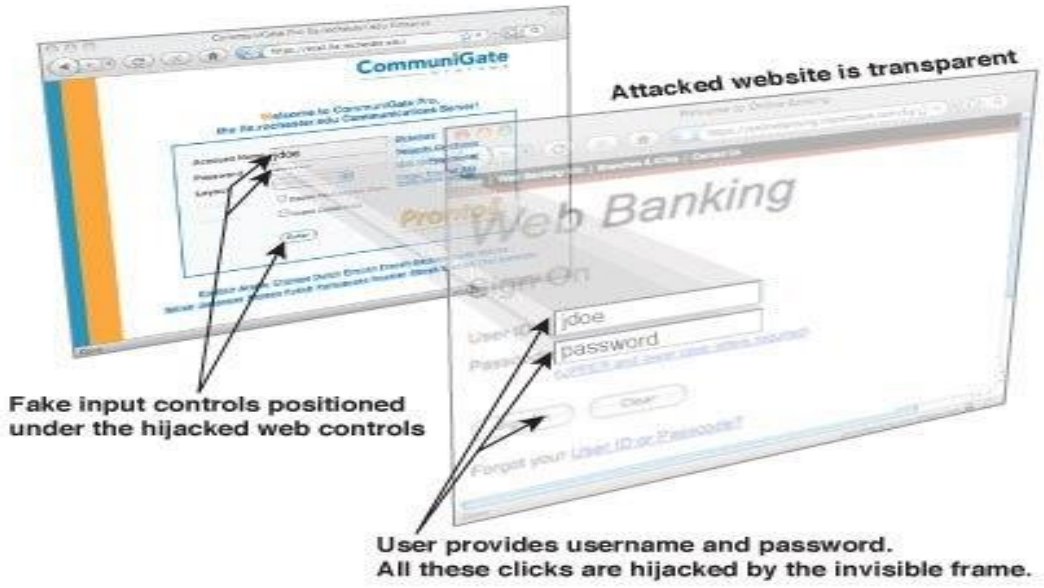
Figura 12. Prueba con owasp-zap



Fuente. Los autores Prueba con owasp-zap

La herramienta documenta que se puede ejercer un ataque de click Hacking hace creer al usuario que está realizando acciones sobre una aplicación web cuando en realidad está actuando sobre un marco superpuesto creado por un atacante (Etico, 2014) cómo se ilustra en la figura 13.

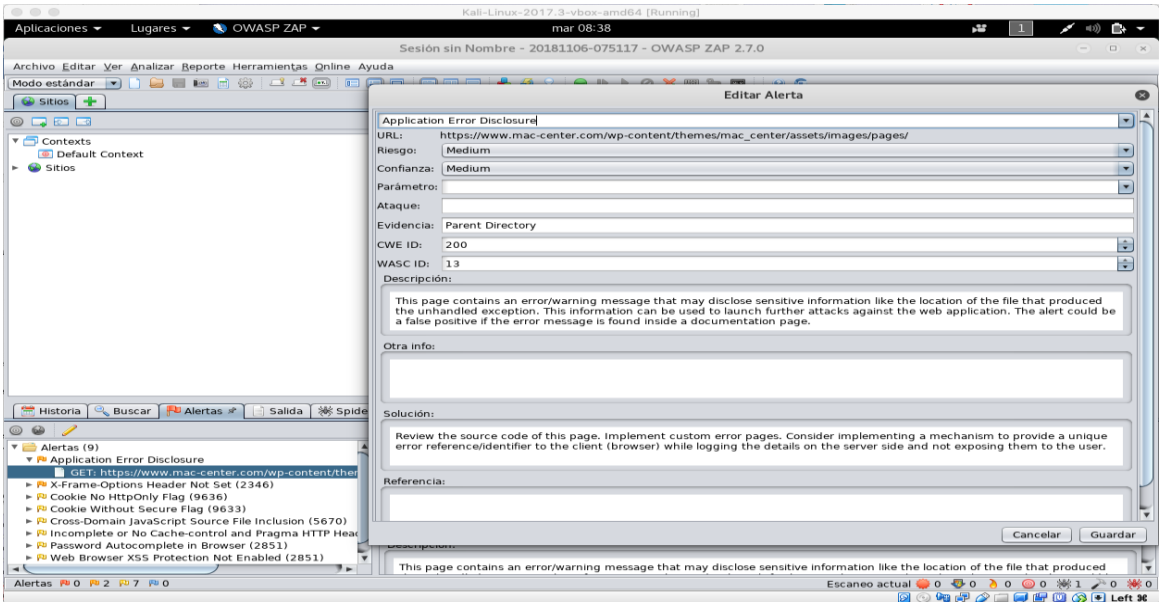
Figura 13. Imagen de relacionada a X-Frame-Options.



Fuente. https://clicksecurity.github.io/data_hacking/

- Application Error Disclosure vulnerabilidad clasificada por la herramienta como de nivel medio

Figura 14. Prueba 2 con owasp-zap



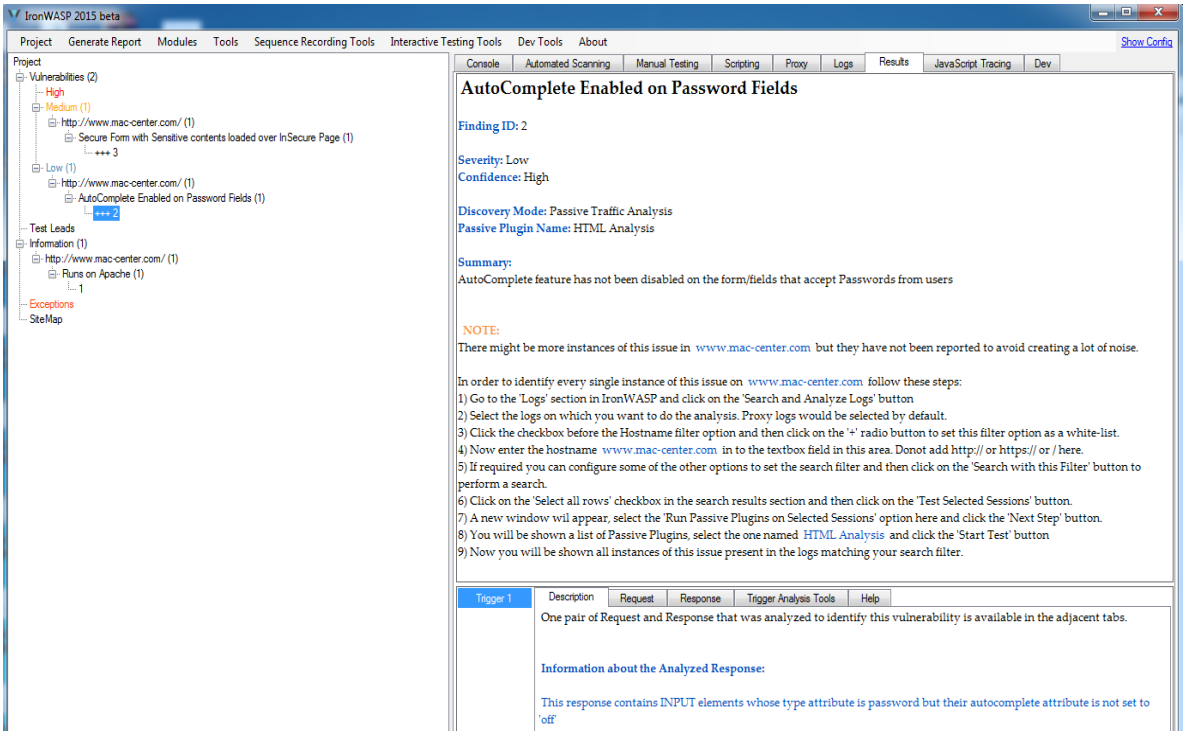
Fuente. Los autores Prueba con owasp-zap

Esta vulnerabilidad indica que se hace una declaración de errores de la aplicación. Esta página contiene un mensaje de error y advertencia que puede revelar información confidencial como la ubicación del archivo que produjo la excepción no controlada. Esta información se puede utilizar para lanzar más ataques contra la aplicación web. La alerta podría ser un falso positivo si el mensaje de error se encuentra dentro de una página de documentación (Etico, 2014).

IronWasp

Se realiza escaneo con la herramienta IronWasp a el sitio web de Mac Center obteniendo los resultados que se describen en la figura 15.

Figura 15. Prueba con ironwasp



Fuente. Los autores Prueba con IronWasp

Según lo anterior se obtienen como resultados principales las dos mismas vulnerabilidades X-Frame-Options y Application Error Disclosure.

Los resultados obtenidos se muestran en la tabla 6 que indica un resumen del análisis.

Tabla 6. Resumen de las vulnerabilidades encontradas con la herramienta

Herramienta	Vulnerabilidad	Nivel de la vulnerabilidad según el escáner	Clasificación en Owasp	Clasificación en CVE
IronWasp	X-Frame-Options	Medio	A4 entidad externa de XML	CVE-2016-9168
IronWasp	Application Error Disclosure	Medio	A9 uso de componentes con vulnerabilidades	CVE-2016-6145
OwaspZap	X-Frame-Options	Medio	A4 entidad externa de XML	CVE-2016-9168
OwaspZap	Application Error Disclosure	Medio	A9 uso de componentes con vulnerabilidades	CVE-2016-6145

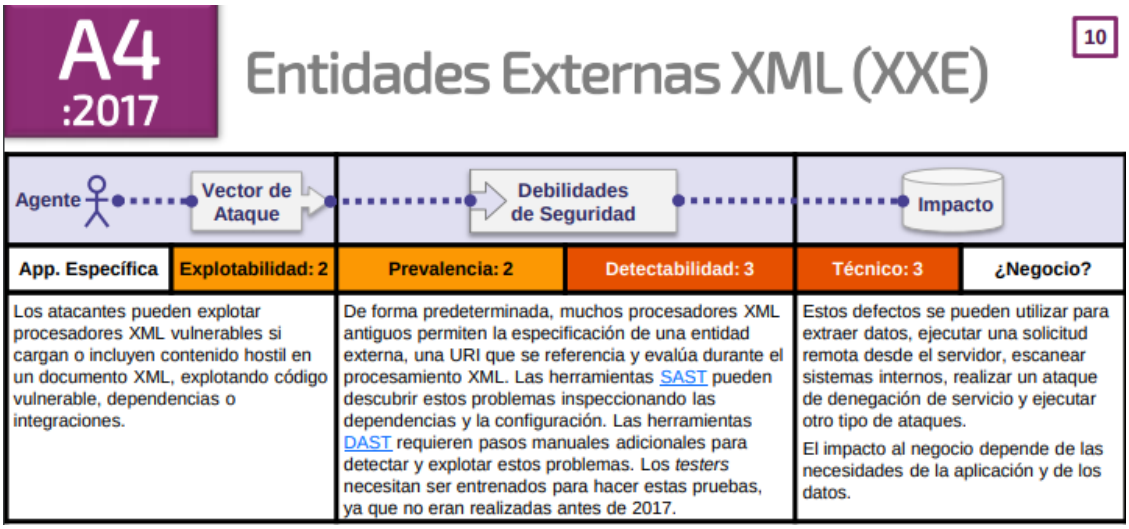
Fuente. Los autores

Posterior a esto se aplica el modelo propuesto y se dan los resultados de la evaluación y calificación de las vulnerabilidades en el sitio web de Mac Center puestas a prueba con el modelo planteado que contiene la calificación de Owasp con el modelo CVSS.

Para iniciar se analiza la vulnerabilidad X-Frame-Options, con el modelo donde la clasificación de OWASP para esta vulnerabilidad se analizó que pertenece a la clasificación A4 según los resultados de los escáneres, donde se obtiene las calificaciones

de 2 para explotabilidad, 2 para prevalencia y 3 para detectabilidad Según la figura 16.

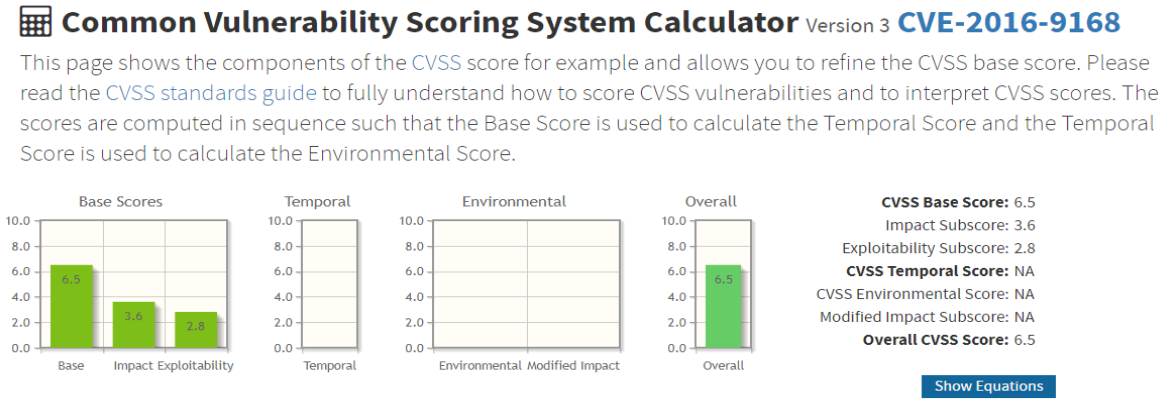
Figura 16. Clasificación A4 de Owasp 201.



Fuente. https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

Posterior mente se debe tomar la calificación de CVE en su componente base que para el impacto técnico de esta vulnerabilidad que es de (6.5) que tiene el código CVE-2016-9168 tal y como se ve en la figura 17 y que se puede consultar en "https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?name=CVE-2016-9168&vector=AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N".

Figura 17. CVE 2012-1961



Fuente https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator?name=CVE-2012-1961&vector=(AV:N/AC:M/Au:N/C:N/I:P/A:N)

Posteriormente se calificará el impacto de negocio según el gerente o los expertos, y el resultado de la calificación de la vulnerabilidad es de (6.19)

Figura 18. Análisis con el modelo propuesto de la vulnerabilidad 1.

CVSS(impacto tecnico)				
Vector de ataque	red	red adyacente	local	fisico
Complejidad de ata	bajo	alto		
pruvilegios	ninguno	bajo	alta	
interaccion con usu	ninguno	requerido		
Alcance	Sin cambio	Cambio		
Impacto				
confidencialidad	ninguno	bajo	alto	
integridad	ninguno	bajo	alto	
disponibilidad	ninguno	bajo	alto	

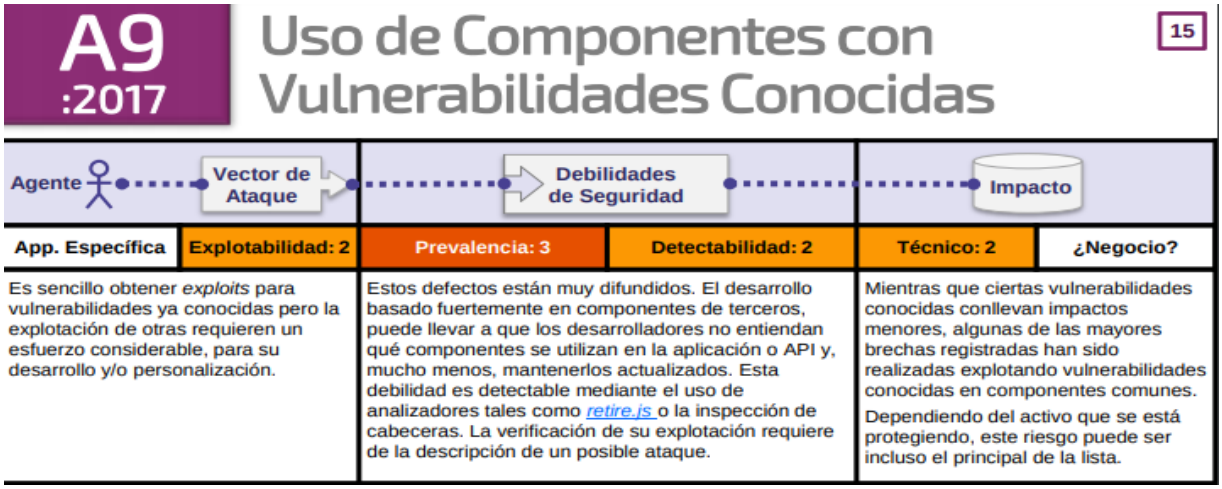
Modelo					
Owasp			**CVSS**	**Nist800-55(Mintic)**	
Explotabilidad (0-3)	**Prevalencia (0-3)**	**Detectabilidad (0-3)**	**Impacto tecnico (0-10)**	**Impacto de negocio (0-3)**	
2	2	3	6,5	Procesos	3
				Operación	2
				Procesos críticos	2
				Aplicaciones	3
				Bases de datos	2
				Comunicaciones	2
				Cuartos de maquinas	1
				equipos	2
				Recurso humano	2
2,33				Objetivos Misionales, estratégicos y de negocio	3
15,17				22	
TOTAL	**6,19**				

Fuente. Los autores.

Para proseguir se analiza la vulnerabilidad Application Error Disclosure con el modelo donde la clasificación de OWASP para esta vulnerabilidad se analizó que pertenece a la

clasificación A9 según los resultados de los escáneres, donde se obtiene las calificaciones de 2 para explotabilidad, 3 para prevalencia y 2 para detectabilidad Según la figura 19.

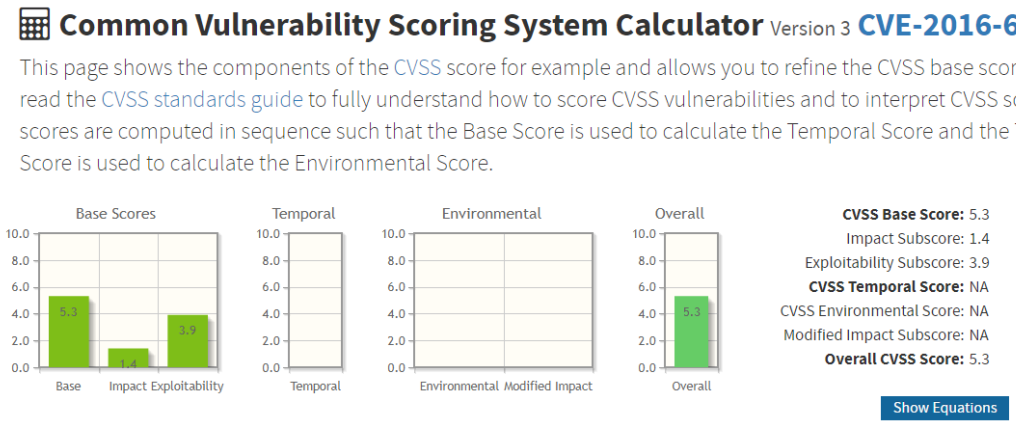
Figura 19. Calificación de OWASP para A9



Fuente. https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf.

Posterior mente se debe tomar la calificación de CVE en su componente base que para el impacto técnico de esta vulnerabilidad que es de (5.3) que tiene el código CVE-2016-6145 tal y como se ve en la figura 20 y que se puede consultar en "https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?name=CVE-2016-6145&vector=AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N".

Figura 20. Calificación de CVE-2016-6145



Fuente. https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?name=CVE-2016-6145&vector=AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N.

Posteriormente se calificará el impacto de negocio según el gerente o los expertos, y el resultado de la calificación de la vulnerabilidad es de (5.39)

Figura 21. Análisis con el modelo de la vulnerabilidad 2.

CVSS(impacto tecnico)				
Vector de ataque	red	red adyacente	local	fisico
Complejidad de ata	bajo	alto		
pruvilegios	ninguno	bajo	alta	
interaccion con usu	ninguno	requerido		
Alcance	Sin cambio	Cambio		
Impacto				
confidencialidad	ninguno	bajo	alto	
integridad	ninguno	bajo	alto	
disponibilidad	ninguno	bajo	alto	

Modelo					
Owasp			**CVSS**	**Nist800-55(Mintic)**	
Explotabilidad (0-3)	**Prevalencia (0-3)**	**Detectabilidad (0-3)**	**Impacto tecnico (0-10)**	**Impacto de negocio (0-3)**	
2	3	2	5,3	Procesos	3
				Operación	2
				Procesos críticos	3
				Aplicaciones	3
				Bases de datos	1
				Comunicaciones	1
				Cuartos de maquinas	1
				equipos	2
				Recurso humano	2
2,33				Objetivos Misionales, estratégicos y de negocio	2
12,37				20	
TOTAL	**5,39**				

Fuente. Los autores.

De esta forma se obtiene la clasificación de las dos vulnerabilidades con el modelo propuesto en este proyecto y finalmente se saca la calificación del sitio web promediando

las dos vulnerabilidades como se ve en la figura 22que da resultado de (5.79) de calificación media.

Figura 22. Resultado del sitio web.

	calificacion	Total
Vulnerabilidad 1	6,19	5,79
Vulnerabilidad 2	5,39	

Fuente. Los autores.

5. PRODUCTOS POR ENTREGAR

Dentro de este capítulo se describe, los productos a entregar alineados con los objetivos general y específicos delo proyecto a continuación se detallan cada paso de los entregables.

- Se comenzó con analizar las metodologías, marcos y normas para la gestionar el análisis y evaluación de vulnerabilidades, según el contexto de TI de gestión de riesgos y de controles,
- Análisis de resultados de los marcos de referencia, normas y metodologías para gestionar el análisis de vulnerabilidades en sitios web para así realizar seleccionar los principales ítems y acoplarlos para el modelo que se platea,
- Diseñó del modelo para análisis de vulnerabilidades
- Caso de prueba para validar su funcionalidad y correcta ejecución del modelo.

6. CONCLUSIONES

Se realizó análisis de los marcos de referencias los cuales podrían ayudar a potencializar nuestro modelo en cuanto a la evaluación de vulnerabilidades de la ciberseguridad, los cuales fueron ISO 27004, CVSS, OWASP y NIST 800-55.

Para el modelo propuesto se seleccionan dos marcos de referencias por su afinidad e integridad en la evaluación de vulnerabilidades (OWASP, NIST 800-55 y CVSS). Posterior a esto se realizó el desarrollo e implementación del modelo para la evaluación y calificación las vulnerabilidades en sitios web.

Se realizó prueba piloto de nuestro modelo en la empresa de Mac Center dando como resultados la respuesta a la pregunta de investigación de cómo debería ser y que características debería tener nuestro modelo para evaluar las vulnerabilidades en sitios web.

Se establece que el modelo para evaluar las vulnerabilidades cumple con las condiciones para ser usado en un ambiente empresarial, ya que permite hacer una calificación tanto del impacto técnico como del impacto de negocio en una calificación por cada vulnerabilidad y finalmente sacar una calificación de la vulnerabilidad del sitio web a evaluar.

7. RECOMENDACIONES

El proyecto se enfocó en el desarrollo de un modelo para medir el nivel de vulnerabilidad en sitios web basado en el top 10 de Owasp 2017, el cual se debe ir mejorando, actualizándose y ser una herramienta con la cual se pueda evaluar y calificar cualquier sitio web este permitirá optimizar la evaluación de vulnerabilidades con los cuales contribuyan a las organizaciones en la toma de decisiones y en la mejora continua de sus procesos y seguridad en sus activos de información.

8. TRABAJOS FUTUROS

Se debe tener presente que el modelo cuenta con los siguientes módulos explotabilidad, prevalencia, detectabilidad, impacto técnico e impacto del negocio, estos módulos se pueden actualizar a medida del tiempo o adicionar nuevos módulos que permitan tener una evaluación y calificación más exacta en el nivel de vulnerabilidades en sitios web, así mismo se puede automatizar una herramienta tomando el modelo propuesto para que sea una herramienta útil para cualquier tipo de negocio y aportar en la mejora continua de la seguridad de la información y en la toma de decisiones a nivel estratégico.

9. ESTRATEGIAS DE COMUNICACIÓN

Este proyecto posterior a su terminación se divulgará mediante diferentes tipos de comunicación para que los interesados ya sean a nivel educativo, profesional o especialistas en el campo de la seguridad de la información lo conozcan. Como estrategia se adoptará en primer lugar la sustentación del proyecto a nivel universitario, en segundo lugar, se continuará con el desarrollo del proyecto para que mediante la participación activa en comunidades y asociaciones para adquirir el reconocimiento para lo que se usaran los siguientes medios:

- Exposición en la universidad: Es necesario que cada integrante haga la exposición frente a los jurados y que sea aprobado el trabajo.

- Articulo: se adjunta un artículo con el resumen del trabajo de grado

- Publicación en Biblioteca: Se presentará el documento en la biblioteca de la universidad católica de Colombia para que pueda ser utilizado y expuesto como material de conocimiento.

10. BIBLIOGRAFÍA

Ballestas, P. (27 de 05 de 2016). *Análisis de Riesgos Magerit*. Obtenido de Análisis de Riesgos Magerit: https://prezi.com/ukh_2gzmboss/comparacion-iso-27002-analisis-de-riesgos-magerit-y-octave/

Control, G. (2015). *Evolución de la Seguridad Informática*. Obtenido de Seguridad Informática: https://www.grupocontrol.com/evolucion-de-la-seguridad-informatica

CVE. (06 de 08 de 2017). *CVE*. Obtenido de CVE: https://cve.mitre.org/

CVSS. (20 de 01 de 2017). *CVSS*. Obtenido de CVSS: https://www.first.org/cvss/

Definiciones.es. (12 de 04 de 2015). *Analisis cualitativos*. Obtenido de Analisis cualitativos: https://definicion.de/cualitativo/

Etico, H. (14 de 10 de 2014). *hacking-etico*. Obtenido de hacking-etico: https://hacking-etico.com/2014/10/14/analisis-del-cvss-de-shellshock/

ISACA. (13 de 06 de 2016). *ISACA*. Obtenido de ISACA: https://www.isaca.org/Pages/default.aspx?cid=1210069&Appeal=SEM&gclid=CjwKCAiAlb_fBRBHEiwAzMeEdr6i9mVJI1YoNI-6-7tGl9pIFs-dyO_GyY0nhxUoPYK240_t8JFZzBoCo5sQAvD_BwE&gclsrc=aw.ds

ISOTools. (02 de enero de 2014). *Medición de la Seguridad de la Información*. Obtenido de ISOTools: https://www.pmg-ssi.com/2014/01/isoiec-27004-medicion-de-la-seguridad-de-

la-informacion/

Mendoza, M. Á. (25 de 16 de 2015). *welivesecurity*. Obtenido de welivesecurity: https://www.welivesecurity.com/la-es/2015/06/25/cvss-version-3/

MinTic. (2014 de 03 de 2016). *Seguridad y privacidad de la informacion*. Obtenido de Seguridad y privacidad de la informacion: https://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf

Mintic. (02 de 05 de 2016). *sistemas de Gestion*. Obtenido de sistemas de Gestion: http://www.mintic.gov.co/gestionti/615/w3-article-5482.html

Mintic, G. (01 de 12 de 2015). *Guía para realizar el Análisis de*. Obtenido de Guía para realizar el Análisis de: https://www.mintic.gov.co/gestionti/615/articles-5482_G11_Analisis_Impacto.pdf

Moyano. (21 de 07 de 2017). *segu-info*. Obtenido de segu-info: http://blog.segu-info.com.ar/2013/04/auditoria_ti.html

NIST. (10 de 12 de 2008). *COMPUTER SECURITY RESOURCE CENTER*. Obtenido de COMPUTER SECURITY RESOURCE CENTER: https://csrc.nist.gov/publications/detail/sp/800-55/rev-1/final

owasp. (15 de 11 de 2017). *owasp*. Obtenido de owasp: https://www.owasp.org/index.php/Main_Page

School, O. (12 de 03 de 215). *Universidad de Barcelona*. Obtenido de Universidad de Barcelona: https://www.obs-edu.com/int/blog-investigacion/sistemas/seguridad-de-la-informacion-

un-conocimiento-imprescindible

Tools, I. (30 de 08 de 2016). *Iso y riesgos*. Obtenido de Iso y riesgos: http://www.isotools.com.co/etapas-del-proceso-gestion-del-riesgo-correspondencia-ntc-iso-31000-meci-saro/

tor, p. (04 de 09 de 2016). *torproject*. Obtenido de torproject: https://www.torproject.org/docs/tor-onion-service