# DESARROLLO DE UNA AUDITORÍA A LA APLICACIÓN WEB MUISCA BASADO EN HERRAMIENTAS DE SOFTWARE LIBRE DEL PROYECTO OWASP EN LA ENTIDAD DIAN

**MELGAREJO MARTINEZ EDWIN**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA**

**ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERA**

**ESPECIALIZACIÓN SEGURIDAD INFORMATICA**

**BOGOTA**

**2018**

# DESARROLLO DE UNA AUDITORÍA A LA APLICACIÓN WEB MUISCA BASADO EN HERRAMIENTAS DE SOFTWARE LIBRE DEL PROYECTO OWASP EN LA ENTIDAD DIAN.

**MELGAREJO MARTINEZ EDWIN**

**Optar el título de Especialista en Seguridad Informática**

**FRANCISCO JAVIER HILARIÓN NOVOA**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA**

**ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERA**

**ESPECIALIZACIÓN EN SEGURIDAD INFORMATICA**

**BOGOTA**

**2018**

Nota de Aceptación

Presidente de Jurado

Jurado

Jurado

Bogotá (diciembre, 2018)

## DEDICATORIA

Dedico este proyecto a Dios por darme la oportunidad de vivir, progresar y por estar conmigo en cada paso que doy, por fortalecer mi mente y por haber puesto en mi camino a aquellas personas fructíferas que han sido mi aliciente y compañía durante todo el proyecto de grado.

A mi madre por darme la luz, por sus valiosos consejos, por inculcarme sus valores bondadosos, por la constancia motivación para ser una persona de bien.

A mi esposa Xiomara el cual estuvo presente dándome el apoyo moral, por creer en mí y el motor de mi vida, todo esto te lo debo a ti.

A mi hermano Ferney, para que veas en mí un ejemplo a seguir en esta profesión.

## AGRADECIMIENTOS

Agradezco en general a todas las personas que de una manera o forma aportaron al desarrollo de este proyecto de grado, a Dios por iluminar este pasó en mi vida, a mi familia por el apoyo, y estar siempre a mi lado.

Gracias a los maestros y compañeros de esta especialización que hicieron parte activa en la consecución de este logro.

## TABLA DE CONTENIDO

pág.

## LISTA DE FIGURAS

pág.

## LISTA DE TABLAS

pág.

## LISTA DE GRAFICOS

pág.

## LISTA DE ANEXOS

pág.

## ABREVIATURAS

| | |
|---|---|
| OWASP | Open web application security project – Proyecto de seguridad de aplicaciones web abiertas.[1] |
| WWW | World Wide Web – Red informática mundial. |
| TCP | Transmission Control Protocol - Protocolo de control de transmisión.[2] |
| IP | Internet Protocol - Protocolo de internet. |
| URL | Uniform Resource Locator - Localizador Uniforme de Recursos. |
| HTML | HyperText Markup Language -Lenguaje de marcas de hipertexto.[3] |
| CSS | Cascading Style Sheets - Hoja de estilos en cascada |
| XML | Extensible Markup Language – Lenguaje de marcas Extensible.[4] |
| HTTP | Hypertext Transfer Protocol - Protocolo de transferencia de hipertexto.[5] |
| HTTPS | Hypertext Transfer Protocol Secure - Protocolo seguro de transferencia de hipertexto. |
| SSL | Secure Sockets Layer – Capa de conexión segura |

[1] Cervigón, A., & Ramos, M. (2011). Seguridad Informática. Madrid, España: paraninfo, SA.
[2] Varela, C., & Domínguez, L. (2002). Redes inalámbricas. Trabajo de carrera, España: Universidad de Valladolid, Escuela Técnica Superior de Ingeniería Informática.
[3] Martínez, C. A. B., & Jiménez, J. T. (1999). *XML como solución a los problemas de estructuración e intercambio de información por medios electrónicos* (Doctoral dissertation, CA Bonavides M.).
[4] World Wide Web Consortium. (2006). Extensible markup language (XML) 1.1.
[5] Avogadro, M. (2007). Glosario de nuevas tecnologías de la información y la comunicación. *Razón y palabra*, *55*.

## GLOSARIO

**Alcance.** Ámbito de la organización que queda sometido al SGSI es decir lo que abarca.[6]

**Amenaza.** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.[7]

**Autenticación.** Provisión de una garantía de que una característica afirmada por una entidad es correcta.[8]

**Autenticidad.** Propiedad de que una entidad es lo que afirma ser.[9]

**Checklist.** Lista de apoyo para el auditor con los puntos a auditar, que ayuda a mantener claros los objetivos de la auditoría, sirve de evidencia del plan de auditoría, asegura su continuidad y profundidad y reduce los prejuicios del auditor y su carga de trabajo.[10]

**Confidencialidad.** Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.[11]

**Control.** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado

[6] xLópez, A. El portal de ISO 27001 en Espanol. Recuperado de http://www.iso27000.es/glosario.html
[7] López, A. El portal de ISO 27001 en Espanol. Recuperado de http://www.iso27000.es/glosario.html
[8] López, A. El portal de ISO 27001 en Espanol. Recuperado de http://www.iso27000.es/glosario.html
[9] López, A. El portal de ISO 27001 en Espanol. Recuperado de http://www.iso27000.es/glosario.html
[10] López, A. El portal de ISO 27001 en Español. Recuperado de http://www.iso27000.es/glosario.html
[11] López, A. El portal de ISO 27001 en Espanol. Recuperado de http://www.iso27000.es/glosario.html

como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.[12]

**Directiva o directriz.** Una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.[13]

**Disponibilidad.** Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.[14]

**Gestión de claves.** Controles referidos a la gestión de claves criptográficas.[15]

**Gestión de incidentes de seguridad de la información.** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.[16]

**Integridad.** Propiedad de la información relativa a su exactitud y completitud.[17]

**ISO/IEC 27001.** Norma que establece los requisitos para un sistema de gestión de la seguridad de la información (SGSI). Primera publicación en 2005; segunda edición en 2013. Es la norma en base a la cual se certifican los SGSI a nivel mundial.[18]

[12] López, A. El portal de ISO 27001 en Espanol. Recuperado de http://www.iso27000.es/glosario.html
[13] López, A. El portal de ISO 27001 en Espanol. Recuperado de http://www.iso27000.es/glosario.html
[14] López, A. El portal de ISO 27001 en Espanol. Recuperado de http://www.iso27000.es/glosario.html
[15] López, A. El portal de ISO 27001 en Espanol. Recuperado de http://www.iso27000.es/glosario.html
[16] López, A. El portal de ISO 27001 en Espanol. Recuperado de http://www.iso27000.es/glosario.html
[17] López, A. El portal de ISO 27001 en Espanol. Recuperado de http://www.iso27000.es/glosario.html
[18] López, A. El portal de ISO 27001 en Espanol. Recuperado de http://www.iso27000.es/glosario.html

**No repudio.** Según [CCN-STIC-405:2006]: El no repudio o irrenunciabilidad es un servicio de seguridad que permite probar la participación de las partes en una comunicación.[19]

Según [OSI ISO-7498-2]: Servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido).

**Objetivo.** Declaración del resultado o fin que se desea lograr mediante la implementación de procedimientos de control en una actividad determinada.[20]

**Proceso.** Conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas.[21]

**Riesgo.** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.[22]

**Riesgo residual.** El riesgo que permanece tras el tratamiento del riesgo.[23]

**Seguridad de la información.** Preservación de la confidencialidad, integridad y disponibilidad de la información.[24]

**Trazabilidad.** Según [CESID: 1997]: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.[25]

**Vulnerabilidad.** Debilidad de un activo o control que puede ser explotada por una o más amenazas.

[19] López, A. El portal de ISO 27001 en Espanol. Recuperado de http://www.iso27000.es/glosario.html
[20] López, A. El portal de ISO 27001 en Espanol. Recuperado de http://www.iso27000.es/glosario.html
[21] López, A. El portal de ISO 27001 en Espanol. Recuperado de http://www.iso27000.es/glosario.html
[22] López, A. El portal de ISO 27001 en Espanol. Recuperado de http://www.iso27000.es/glosario.html
[23] López, A. El portal de ISO 27001 en Espanol. Recuperado de http://www.iso27000.es/glosario.html
[24] López, A. El portal de ISO 27001 en Espanol. Recuperado de http://www.iso27000.es/glosario.html
[25] López, A. El portal de ISO 27001 en Espanol. Recuperado de http://www.iso27000.es/glosario.html

## TITULO

***"Desarrollo de una auditoría a la aplicación web MUISCA basado en herramientas de Software libre del Proyecto OWASP en la Entidad DIAN"***

# INTRODUCCION

En ello se verá el desarrollo y la importancia de las herramientas de software libre como OWASP con el fin de realizarse una auditoria, para este caso con aplicaciones web; se sabe que en este estándar se cuenta con una amplia gama de módulos para el cual nos conlleva a tener resultados que nos permite analizar y tomar decisiones para un óptimo desarrollo de seguridad en las páginas y estar a la vanguardia del día a día en temas de la tecnología.

La importancia de realizar este proyecto nos conlleva a ver como las guía OWASP vienen de manera recursiva y fácil de entender la terminología para la correcta aplicación de las pruebas a obtener, es importante para el especialista la investigación y estudio de algoritmos de diferentes lenguajes de programación para el fácil entendimiento de las acciones y funciones en las aplicaciones web; es por ello que esta metodología es amigable e interactiva para llevarse a cabo una auditoria.

El profesional se ve comprometido con la necesidad de afrontar retos importantes en la vida profesional y de acuerdo a la compañía donde se preste este tipo de servicios se tomarán decisiones y la búsqueda de implementar códigos rigurosos con el fin de mitigar los impactos ante el robo de información o alteración de las aplicaciones web.

Las mejoras en este tipo de sistemas de información son necesarias en el día a día por la exposición y los cambios el cual nos enfrentamos en la tecnología informática, y por ende hay personas que están en el mundo del internet en disposición de sabotear, alterar y modificar sistemas para beneficios propios, a raíz de ellos todas las compañías deben estar al tanto de la seguridad para no afectar el activo más preciado como es la información.

# 1. FORMULACION DEL PROBLEMA

Sobre este proyecto se ha visto la necesidad de enfocarnos en aplicar el desarrollo de las aplicaciones web seguras en la entidad DIAN; entidad del estado colombiano encargado de la recaudación de los impuestos para los recursos de la nación, y está enfocada en brindar a todos los declarantes y contribuyentes una herramienta web donde se pueden realizar de manera práctica y amigable los diferentes tramites como lo son en relación a la inscripción del RUT, generación de la declaración de renta, prevalidadores básicos para el diligenciamiento de los diferentes formularios para tal fin, consulta de aranceles entre otros.

En este punto las personas naturales y compañías declaradoras ingresan a la página web (muisca.dian.gov.co), por este medio a un acceso para ver sus trazabilidades y movimientos de los ejercicios de declaraciones realizadas en todos los años, esto está categorizado con el nombre de Muisca.

El problema de seguridad en aplicaciones web últimamente se ha visto vulnerables en todas en las Entidades Privadas y Públicas, es por ello que se están expuestas a las siguientes acciones como lo son la ejecución maliciosa de código, referencias directas inseguras a objetos, almacenamiento criptográfico inseguro, comunicaciones inseguras de redes entre otros.

Se evidencio que se debe dar solución al entorno de auditar los aplicativos webs en esta importante entidad, tal que nos vemos la necesidad de implementar una auditoria en este ámbito y basándonos en la guía OWASP, herramienta eficaz de software libre por el cual da una revisión del código que se maneja a fondo, incluyendo una serie de puntos de verificación de la seguridad en los módulos y en la aplicación en general.

Contamos con el aval de la entidad para la realización de este proyecto, con el fin de interactuar y hacer dichos auditajes, para mayor facilidad del mismo; con ello se analizará y se estudiará la metodología OWASP Insecure Web App y OWASP Pantera Web Assessment Studio, con el fin de realizar auditoría a aplicaciones web sobre Muisca.

Para realizar este proyecto se requiere de manera especial la investigación a fondo de la metodología OWASP y con base en esto aplicar una auditoría de calidad a la aplicación web nombrada de una Entidad real.

## 1.1 PREGUNTA PROBLEMA

¿Una auditoria de aplicaciones web será de vital importancia realizarse en la entidad DIAN para fortalecer la seguridad en la información, la gestión y el tratamiento del aplicativo MUISCA?

# 2. JUSTIFICACION

En la actualidad vemos como las diferentes formas de probar fallos de seguridad han estado en auge por el activo de la información a respaldar, y en este documento se plasmaría de parte de expertos, fundamentados en la guía OWASP para realizarse esta comprobación de manera rápida, exacta y eficientemente una auditoria web segura.

Se revisa el tema y la importancia de ver coma la guía OWASP son desarrollados por personas colaborativas en el entorno de la seguridad web y por lo tal esta de modo totalmente abierto y gratuito. La seguridad es un tema que nos permitiría ver como cualquier persona de la ingeniería está abierta para aprender y ver cómo se puede corregir detalles de los desarrolladores y blindarlo con el fin de no tener fácil intrusión en donde comprometan el robo de información en un sistema de información. En estas guías nos facilita ver un detallado especifico metodologías por el cual se busca mitigar y corregir algoritmos sensibles, para con ello se busquen mecanismos o maneras de solucionarse, esto con el fin de fortalecerlo y no comprometer el activo de la información para la entidad. La necesidad de este trabajo de auditoria sirve de punto de partida para futuros proyectos informáticos y a manos de la entidad DIAN.

Es de vital importancia como el personal tecnológico, debe estar preparados sobre temas de seguridad de la información y a su vez enfocarse en mecanismos e implementaciones para un correcto funcionamiento de las aplicaciones web seguras; los desarrolladores de los sistemas de información deben estar al tanto y preparados para estos ser aplicados en los códigos y algoritmos y minimizar los ataques con fines maliciosos o robo de información al instruir y vulnerar las aplicaciones web, por eso la recomendación de realizar monitoreo y pruebas continuas para estar al tanto de estas infiltraciones. Nuestro alcance será auditar la aplicación web segura en la DIAN, utilizando las metodologías del proyecto OWASP basada en software libre.

Se adoptará el enfoque wiki con la comunidad OWASP para este tema de las auditorias en donde se puede evolucionar y expandir la información que bajo esta guía nos fortalece y se saca provecho ante las amenazas que se presentan en las aplicaciones web.

# 3. OBJETIVOS

## *3.1. Objetivo General:*

Desarrollar una propuesta de auditoria de la aplicación web MUISCA en la DIAN, utilizando las metodologías OWASP Insecure Web App y OWASP Pantera Web Assessment Studio basada en software libre.

## *3.2. Objetivos Específicos:*

- Detallar los procedimientos y herramientas utilizadas por las metodologías **OWASP Insecure Web App** y **OWASP Pantera Web Assessment Studio** para auditar una aplicación Web.

- Evidenciar las pruebas y resultados de la auditoría al sistema de información seleccionado, aplicado a las metodologías **OWASP.**

- Generar los informes sobre las vulnerabilidades encontradas en la auditoría del Proyecto **OWASP.**

# 4. MARCO REFERENCIAL

## 4.1. ANTECEDENTES

Hasta el momento no se ha manejado un seguimiento de auditoria en las aplicaciones web de la entidad DIAN, se han ido actualizando en servicios tecnológicos a la vanguardia del día a día y a su vez fortaleciéndose en el tema de las declaraciones de renta de los ciudadanos y otros trámites que se manejan dentro de ella.

Según información suministrada por ellos, se pudo corroborar que las aplicaciones vienen siendo estándares para todos los servicios que ofrecen en la entidad.

Por este motivo se observó la necesidad de desarrollar una auditoria a la aplicación web segura MUISCA, aplicación manejada a nivel nacional.

## 4.2. MARCO CONTEXTUAL

La entidad Dian se constituye en una organización sólida en el sector público; gracias a su fundación exactamente 25 años está en la vanguardia en el tema de la recaudación de impuestos para la nación.

Son responsables de administrar con calidad el cumplimiento de las obligaciones tributarias, aduaneras y cambiarias, mediante el servicio, la fiscalización y el control; facilitar las operaciones de comercio exterior y proveer información

confiable y oportuna, con el fin de garantizar la sostenibilidad fiscal del Estado colombiano.[26]

Para el año 2020, la entidad generara un alto nivel de cumplimiento voluntario de las obligaciones tributarias, aduaneras y cambiarias, apoyando la sostenibilidad financiera del país y fomentando la competitividad de la economía nacional, gestionando la calidad y aplicando las mejores prácticas internacionales.[27]

Dentro del mapa de procesos la planeación institucional juega un papel importante y por el cual consiste en la modelación y presentación expresa que hace la entidad de su proyección a mediano y largo plazo, estas siendo representadas en el plan estratégico, el direccionamiento estratégico y los proyectos de inversión.[28]

También, la evaluación institucional dentro del marco referente presenta los informes de evaluación con los niveles de avance en la ejecución de la planeación estratégica, la planeación operativa y los proyectos de inversión.

Se puede consultar el organigrama, mapa de procesos y la estructura donde pertenece el área de tecnología de la entidad en el Anexo C, D, E.

## 4.3. MARCO CONCEPTUAL

La realización de una auditoria hoy en día es de crucial importancia por el cual nos permite realizar un seguimiento y mitigar fallas que comprometan los datos de información contenida dentro de ella; con esto se vio en la necesidad de aplicarlo con herramientas de software libre y el cual son de mayor impacto a la

[26] Portafolio de trámites y servicios de dirección de impuestos y aduanas nacionales. Recuperado de http://hacialaintegridad.unodc.org.co/project/dian/
[27] Portafolio de trámites y servicios de dirección de impuestos y aduanas nacionales. Recuperado de http://hacialaintegridad.unodc.org.co/project/dian/
[28] Misión, visión y políticas – DIAN. Extraído de https://www.dian.gov.co/.../DocumentoPlanEstrategicoDIAN20142018_17042016.pdf

hora de realizarse con el fin de ver los resultados para la toma de decisiones en una aplicación web, en general existen varias metodologías por los cuales se pueden trabajar pero el enfoque va ser por medio de la guía OWASP.

La consideración el cual prima estas auditorías tiene que ver con la política de seguridad informática donde es valuarte las características esenciales, como sus aspectos principales vienen siendo la disponibilidad, la confidencialidad, la autenticidad y la integridad, donde también se puede tener en cuenta estos otros aspectos como lo son la trazabilidad y accesibilidad; bajo el concepto de cumplimiento y de acuerdo a un plan de riesgo evaluado y planteado a la hora de realizarlo.

Por tal motivo es necesario la necesidad de desarrollar una auditoria a la aplicación web segura de la DIAN, aplicación manejada a nivel de usuarios internos (funcionarios) y externos (declarantes) a nivel nacional; es importante saber del tema para la presente investigación y así tener un desarrollo beneficioso de este proyecto.

Las auditorias en su entorno son importantes evaluaciones y mediciones de los procesos para saber el estado en que se encuentran sus actividades, y estos cumplan con lineamientos claros para los objetivos y la productividad de las empresas.

La auditoría en sus casos más puntuales lo que se busca fundamentalmente es revisar la forma en las cuales la información afectan a la entidad no sean medidas y valederas. Por lo general es tarea de la auditoría determinar la fiabilidad y el buen funcionamiento de las aplicaciones web para los procedimientos reales en todas las operaciones de la empresa.

La Guía de OWASP con finalidad de construcción de aplicaciones web seguras se ha convertido para los profesionales especializados en seguridad informática,

consultores y desarrolladores un buen producto para el reforzamiento de los códigos en estas aplicaciones web, por eso el auge de ser referida en varios entornos como la parte de gobiernos, corporativos, financieros entre otros, esto se ve plasmado en una manual que sirve con fines de diseñar, auditar y desarrollar aplicaciones web seguras·

## 4.4. MARCO TEORICO

La importancia de hoy en día es estar preparados y con herramientas de software libre nos brinda la posibilidad de explorar y a su vez de implementar auditorias más seguras y de muchos beneficios para garantizar como es en este caso las mejoras continuas a las aplicaciones de la entidad DIAN.

Se puede deducir que actualmente se han venido presentando problemas de seguridad por el cual hacen comprometer a una aplicación web, razón de ello se generan focos de seguridad en los códigos al momento de la implementación de la misma, por lo tanto, para los atacantes se les hace más fácil la intrusión y el cambio de parámetros donde por motivos de extracción de información o sabotaje del mismo perjudican al correcto funcionamiento de una aplicación web.

Podemos ver como ahora estas aplicaciones web se han visto inseguras, por el impacto de la información que se maneje y es un activo a cuidar. El tema de la seguridad es por ende en la actualidad un factor clave para aplicarse en estas tecnologías.

En las herramientas de la guía OWASP nos hacen ver y plasmar de una manera fácil y practica un aprendizaje optimo y a la vez de manera soluble el material para aplicarse en las auditorías de aplicaciones web seguras de la actualidad, las normas establecidas dentro de él nos hace para el especialista el reforzamiento y la investigación a fondo de estos temas y la construcción de una aplicación segura es de vital interés siempre realizar pruebas de seguridad en ella antes de darse a producción o subida en internet.

Hoy en día muchos contratistas de empresas de fábrica de software no tienen en las buenas prácticas, mecanismos de seguridad (código) como parte de su proceso estándar de desarrollo.

En la comprobación y pruebas de seguridad, es necesario una medida particularmente confiable y segura, en ello se existe un número infinito de modos en que un atacante podría ser capaz de colgarse a una aplicación, y es simplemente imposible comprobarlas todos. Sin embargo, la comprobación de seguridad tiene la perspectiva de convencer a las empresas y de verse la necesidad de implementar dichas auditorias para garantizar la información como factor importante en una entidad.

El monitoreo constante de los mecanismos de seguridad implementados ha demostrado ser un elemento clave para cualquier organización para dar confianza en el software que se produce o se usa para fines procesales en la entidad.

Han pasado muchos años y estas aplicaciones web han sido foco de vulnerabilidad, permitiendo que personas no autorizadas tengan el privilegio de acceder a datos confidenciales y así mismo causar pérdida de información.

Hoy día se ha vuelto en un tema de mucha importancia la seguridad informática en todos los proyectos tecnológicos, ya que a través de cifras y números son de vital enfoque a las empresas para mitigar y prevenir los ataques informáticos en donde se están expuestas al robo de información y alteraciones de códigos con fines maliciosos.

Cuando se ve el desarrollo de esta auditoría, es importante ver como la entidad DIAN va ser de gran beneficio, la evaluación y el seguimiento de esta práctica, para visualizar las vulnerabilidades críticas y los focos al cual sus atacantes pueden sacar provecho de información valiosa sobre las firmas digitales e información que se maneja para las declaraciones de rentas.

## 4.5. MARCO LEGAL

### 4.5.1. Constitución Política de 1991

En los artículos 209 y 269 se fundamenta el sistema de control interno en el Estado Colombiano, el primero establece: “La administración pública, en todos sus órdenes, tendrá un control interno que se ejercerá en los términos que señale la ley” y en el 269, se soporta el diseño del sistema: “En las entidades públicas, las autoridades correspondientes están obligadas a diseñar y aplicar, según la naturaleza de sus funciones, métodos y procedimientos de control interno, de conformidad con lo que disponga la ley, la cual podrá establecer excepciones y autorizar la contratación de dichos servicios con empresas privadas colombianas”. [29]

### 4.5.2. Leyes informáticas colombianas

**Ley estatutaria 1266 del 31 de diciembre de 2008**

Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. [30]

### 4.5.3. Ley 1273 del 5 de enero de 2009. Delitos informáticos [31]

Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras.

En el congreso de Colombia de ese año se publicó la Ley 1273 el cual es relacionado contra la protección de la información y de los datos para así

[29] Artículo 209 de la Constitución Política de Colombia. Recuperado de http://www.constitucioncolombia.com/titulo-7/capitulo-5/articulo-209
[30] Ley 1266 de 2008 Nivel Nacional - Secretaría Jurídica Distrital. (31-12-2008). Recuperado de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488
[31] Ley 1273 de 2009 Nivel Nacional - Secretaría Jurídica Distrital. (05-01-2009). Recuperado de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

preservar los sistemas en donde se utilicen las tecnologías de la información y las comunicaciones.

Es importante recalcar en esta ley como se clasifico los delitos por conductas relacionadas con el manejo de datos personales, donde gracias a esto garantizan para las empresas se sientan respaldadas jurídicamente y así mitigar en estos patrones penales.

La importancia dentro de ella hace que temas como la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos sean factores a blindar.

Se enumeran los artículos influyentes de esta ley a continuación tomado del código penal colombiano:

– Artículo 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

– Artículo 269B: OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

– Artículo 269C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas

provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

– Artículo 269D: DAÑO INFORMÁTICO. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

– Artículo 269E: USO DE SOFTWARE MALICIOSO. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

– Artículo 269F: VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

– Artículo 269G: SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

– Artículo 269I: HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239[3] manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 del Código Penal[4], es decir, penas de prisión de tres (3) a ocho (8) años.

– Artículo 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes.

Por último, se es importante informar ante las empresas la inculcación de este tema por donde se mire es una herramienta importante para basarse y denunciar los actos delictivos en los que hoy en día se puedan someterse.

### 4.5.4. Ley 1341 del 30 de julio de 2009 [32]

Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.

### 4.5.5. Ley estatutaria 1581 de 2012 [33]

Entró en vigencia la Ley 1581 del 17 de octubre 2012 de PROTECCIÓN DE DATOS PERSONALES, sancionada siguiendo los lineamientos establecidos por el Congreso de la República y la Sentencia C-748 de 2011 de la Corte

[32] Ley 1507 de 2012 Nivel Nacional - Secretaría Jurídica Distrital. (10-01-2012). Recuperado de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=45327
[33] Ley 1581 de 2012 Nivel Nacional - Secretaría Jurídica Distrital. (17-10-2012). Recuperado de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

Constitucional como resultado de la sanción de la anunciada ley toda entidad pública o privada, cuenta con un plazo de seis meses para crear sus propias políticas internas de manejo de datos personales, establecer procedimientos adecuados para la atención de peticiones, quejas y reclamos, así como ajustar todos los procesos, contratos y autorizaciones a las disposiciones de la nueva norma.

### 4.5.6. Aspectos claves de la normatividad[34]

A. Cualquier ciudadano tendrá la posibilidad de acceder a su información personal y solicitar la supresión o corrección de la misma frente a toda base de datos en que se encuentre registrado.

B. Establece los principios que deben ser obligatoriamente observados por quienes hagan uso, de alguna manera realicen el tratamiento o mantengan una base de datos con información personal, cualquiera que sea su finalidad.

C. Aclara la diferencia entre clases de datos personales construyendo las bases para la instauración de los diversos grados de protección que deben presentar si son públicos o privados, así como las finalidades permitidas para su utilización.

D. Crea una especial protección a los datos de menores de edad.

E. Establece los lineamientos para la cesión de datos entre entidades y los procesos de importación y exportación de información personal que se realicen en adelante.

F. Define las obligaciones y responsabilidades que empresas de servicios tercer izados tales como Call y Contact Center, entidades de cobranza y, en general, todos aquellos que manejen datos personales por cuenta de un tercero, deben cumplir en adelante.

[34]Marco legal de Seguridad de la Información en Colombia. (23-02-2010). Recuperado de http://seguridadinformacioncolombia.blogspot.com/2010/02/marco-legal-de-seguridad-de-la.html

G. Asigna la vigilancia y control de las bases de datos personales a la ya creada Superintendencia Delegada para la Protección de Datos Personales, de la Superintendencia de Industria y Comercio.

H. Crea el Registro Nacional de Bases de Datos.

I. Establece una serie de sanciones de carácter personal e institucional dirigidas a entidades y funcionarios responsables del cumplimiento de sus lineamientos.

### 4.5.7. Ley 603 de 2000[35]

Esta ley se refiere a la protección de los derechos de autor en Colombia. Recuerde: el software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales.

### 4.5.8. El derecho de autor [36]

Constitución Política de 1991. En su artículo 61, que expresa: "El Estado protegerá la propiedad intelectual por el tiempo y mediante las formalidades que establezca la ley".

Decisión 351 de 1993, o Régimen Común Andino sobre Derecho de Autor y Derechos Conexos, es de aplicación directa y preferente a las leyes internas de cada país miembro del Grupo Andino.

Ley 23 de 1982, contiene las disposiciones generales y especiales que regulan la protección del derecho de autor en Colombia.

[35] Marco legal de Seguridad de la Información en Colombia. (23-02-2010). Recuperado de http://seguridadinformacioncolombia.blogspot.com/2010/02/marco-legal-de-seguridad-de-la.html
[36] Régimen Legal de Bogotá D.C. Recuperado de http://www.alcaldiabogota.gov.co/sisjur/index.jsp

DECRETO 1360 DE 1989 (junio 23). "Por el cual se reglamenta la inscripción de soporte lógico (software) en el Registro Nacional del Derecho de Autor".

Decreto 460 de 1995, por la cual se reglamenta el Registro Nacional de Derecho de Autor.

### 4.5.9. Ley 734 de 2002, Numeral 21 y 22 del Art. 34 [37]

Son deberes de los servidores Públicos “vigilar y salvaguardar los bienes y valores que le han sido encomendados y cuidar que sean utilizados debida y racionalmente”, y “responder por la conservación de los útiles, equipos, muebles y bienes confiados a su guarda o administración y rendir cuenta oportuna de su utilización”.

### 4.5.10. Decreto 1377 de 2013[38]

Protección de Datos, decreto por el cual se reglamenta parcialmente la Ley 1581 de 2012.

[37] Régimen Legal de Bogotá D.C. Recuperado de http://www.alcaldiabogota.gov.co/sisjur/index.jsp
[38] Régimen Legal de Bogotá D.C. Recuperado de http://www.alcaldiabogota.gov.co/sisjur/index.jsp

# 5. DISEÑO METODOLOGICO PRELIMINAR

Este proyecto cuenta con la siguiente estructura metodológica, el cual permite tener un paso lógico de los procesos el cual se deben llevar a cabo para dar cumplimiento a los objetivos propuestos.

1. Realizar un levantamiento de información más críticos de la compañía en cuanto al nivel de seguridad de la aplicación web a auditar, según los resultados obtenidos de las encuestas, se establece una entrevista al personal encargado de cada proceso o ciclo del software, que permite establecer y valorizar al nivel de crisis que se presente.

2. Realizar la tabulación respectiva de las encuestas, por el cual nos permite ver la esencia para esta auditoria web, y a partir de ella evaluar los puntos críticos a obtener para así poder minimizar el riesgo.

3. Se plantea en la entidad llevar este tipo de auditorías de aquí en adelante para estar a la vanguardia tecnológica y el avance de la misma.

4. Se creará un plan de recomendaciones para el grupo de tecnología de la entidad, el alcance para este plan nos posibilita a ver un análisis a fondo de posibles riesgos por los cuales pueden estar expuestos las aplicaciones web y sistemas de información.

5. Se procede a aplicar medidas de seguridad para proteger la información como activo más preciado de la entidad.

## 5.1 TIPO DE INVESTIGACION

El estudio de caso presente es de tipo cuantitativo porque nos permite realizar análisis sobre las vulneraciones a la que está expuesta la información en el aplicativo web MUISCA de la entidad DIAN.

La información cualitativa obtenida a través de las encuestas y demás métodos de recolección de datos será tabulada para poder presentar información cuantitativa que permita tomar decisiones y evaluar de manera eficiente y efectiva la hipótesis del problema.

## 5.2. HIPOTESIS

La realización de esta auditoría de aplicaciones web con herramientas de software libre aportara a la entidad DIAN controles efectivos para mantenerse y mejorar las medidas de seguridad y protección de los activos más relevantes, mejorando los siguientes aspectos:

1. Mitigar los riesgos de perdida y corrupción de la información.
2. Mantener un conjunto estructurado, documentado que permita definir el tratamiento que se les dará a los riesgos encontrados.
3. Reducir los niveles de riesgo detectados a un estándar más aceptable.
4. Mejorar la seguridad de la red y facilitar la presentación de informes

### 5.2.1. Variables e indicadores

Variables independientes

- Auditoría sistema de seguridad en la información

Variables dependientes

- Herramientas de software libre
- Planes de contingencia

## 5.3. UNIVERSO

Este proyecto está dirigido de forma primordial a una entidad de tipo publica que se dedica a la recaudación de impuestos ubicada en la ciudad de Bogotá, Colombia, es importante aclarar que la auditoria de aplicaciones web seguras puede ser aplicable a cualquier tipo de entidades y empresas.

## 5.4. POBLACION

Esta auditoria va enfocado en la entidad pública DIAN, con respecto a la aplicación web llamada MUISCA (aplicación recaudadora de impuestos tramites y gestión).

## 5.5. MUESTRA

En esta parte del proyecto, se toman las partes más relevantes de un instructivo por el cual está de soporte para ver la raíz y el origen de esa implementación con fines de trámites de impuestos y aduaneros para apoyar la importancia de una auditoria web segura.

## 5.6. TECNICA DE ANALISIS y PROCESAMIENTO DE DATOS

Para lograr obtener la información relevante de los usuarios externos e internos es importante recalcar sobre el manejo que le están dando a la información en cuanto a la seguridad de esta aplicación web, es necesario aplicar encuestas que contengan información estratégica sobre el manejo de esta herramienta tecnológica.

Luego de tabular la información obtenida se procede a transmitir esta información al comité de control interno de la entidad para establecer un plan de mejora sobre los niveles de vulnerabilidad que se presentan, esta información debe ser socializada y realizar jornadas de sensibilización que permitan a los usuarios externos y internos para que se familiaricen con el plan de mejora; después de ello posterior a la implementación se realizará una nueva encuesta que permita comparar resultados y de esta manera medir la confiabilidad y disponibilidad de esta aplicación web llamada MUISCA.

Tabla N°1. Encuesta Propuesta

| **ENCUESTA** | | |
|---|---|---|
| **Objetivo**: recopilar información para evaluar riesgos de la información e infraestructura de la entidad. | | |
| **Nombre del Encuestado** | **Cargo del Encuestado** | **Teléfono del Encuestado** |
| | | |
| **ENCUESTA USUARIO EXTERNO** | | **CUMPLIMIENTO** |

| | | |
|---|---|---|
| **PREGUNTAS** | **SI** | **NO** |
| ¿Conoce la misión y la visión de la entidad? | | |
| ¿Se cuenta con un objetivo principal para la realización de los trámites relacionados? | | |
| ¿Están claramente delimitadas sus tareas y tramites respectivos? | | |
| ¿Conoce usted o está enterado de la política de seguridad de la información de la entidad? | | |
| ¿Conoce el tratamiento que se le debe dar a los correos con origen sospechoso? | | |
| ¿Conoce alguien diferente de usted sus usuarios y contraseñas de acceso? | | |
| ¿Para el manejo dentro de la plataforma MUISCA, es confiable el tratamiento de los datos que se manejan allí? | | |
| TOTALES | | |
| _____<br>FIRMA ENCUESTADO | _____<br>Vo. Bo. Tecnología | |

Fuente: El autor

Se realizarán todos los elementos importantes y comprendidos en una auditoria de este tipo. El resultado de este nos servirá para redactar y sacar conclusiones, que conlleven a la entidad a tomar las mejoras continuas en sus desarrollos tecnológicos en los momentos que se quiera a dar a nueva implementaciones o aplicaciones a la vanguardia de la tecnología (servicios).

Esta investigación va encaminado a ver la realidad del funcionamiento y de la conservación de la información por el cual se maneja en el muisca, el factor de seguridad al poder el cliente final ver sus operaciones con datos verídicos y seguros.

Para este caso de investigación se hará énfasis en detallar los pasos a pasos de la auditoria con la guía de proyecto OWASP para las aplicaciones web seguras en la entidad DIAN.

## 5.7. TABULACION Y ANALISIS DE LAS ENCUESTAS

En este aparte se mostrarán las diferentes tablas y gráficos el cual corresponde a la información recolectada en las encuestas para la auditoria web en la entidad DIAN, cada tabla se realizó con su respectivo grafico para examinar la tendencia de las respuestas obtenidas y con ello un análisis a los resultados para sacar una conclusión acertada del mismo.

- Pregunta N° 1

¿Conoce la misión y la visión de la entidad?

Tabla N° 2 Resultado 1° Pregunta

| RESPUESTA | TOTAL | |
|---|---|---|
| | CANTIDAD | % |
| SI | 10 | 100% |
| NO | 0 | 0 |
| TOTAL | 10 | 100% |

Fuente: El autor

Grafico 1. Consolidado pregunta N°1


Fuente: El autor

Interpretación:

De 10 usuarios encuestados el 100% de ellos conocen muy claramente la misión y la visión de la entidad.

Análisis:

Se puede observar que, aunque la mayoría son funcionarios tiene muy claro que este tema es clave para la pertenencia del mismo.

- Pregunta N° 2

¿Se cuenta con un objetivo principal para la realización de los trámites relacionados?

Tabla N° 3 Resultado 2° Pregunta

| RESPUESTAS | TOTAL | |
|---|---|---|
| | CANTIDAD | % |
| SI | 8 | 80% |
| NO | 2 | 20% |
| TOTAL | 10 | 100% |

Fuente: El autor

Grafico 2. Consolidado pregunta N°2


Fuente: El autor

Interpretación:

De 10 usuarios encuestados el 80% de ellos conoce los objetivos para la utilización del aplicativo web mientras el 20% no tiene claro las funcionalidades que se manejan allí.

Análisis:

En esta pregunta las cifras fueron favorables y se nota que la mayoría conoce el motivo claro de utilizar esta importante aplicación con fines de recaudos y declaraciones de renta, sin embargo no se potencializa al máximo el tema a los encuestados.

- Pregunta N° 3

¿Están claramente delimitadas sus tareas y tramites respectivos?

Tabla N° 4 Resultado 3° Pregunta

| RESPUESTAS | TOTAL | |
|---|---|---|
| | CANTIDAD | % |
| SI | 8 | 80% |
| NO | 2 | 20% |
| TOTAL | 10 | 100 |

Fuente: El autor

Grafico 3. Consolidado pregunta N°3


Fuente: El autor

Interpretación:

Con un total de 10 encuestados el 80% de ellos cuentan con los roles para los diferentes procesos dentro de ella, sin embargo el restante 20% no tiene las tareas al máximo de acuerdo al tipo de cliente o tramite a realizar.

Análisis:

Los usuarios en su mayoría están contando con roles el cual pueden manejar todos los tramites incluidos, esto haciéndolo amigable y evitar las congestiones de filas en los puntos de contactos, para las personas limitantes en estas tareas se vería bueno reforzarlas en el tema.

- Pregunta N° 4

¿Conoce usted o está enterado de la política de seguridad de la información de la entidad?

Tabla N° 5 Resultado 4° Pregunta

| RESPUESTAS | TOTAL | |
|---|---|---|
| | CANTIDAD | % |
| SI | 8 | 80% |
| NO | 2 | 20% |
| TOTAL | 10 | 100% |

Fuente: El autor

Grafico 4. Consolidado pregunta N°4


Fuente: El autor

Interpretación:

Con un total de 10 usuarios encuestados el 80% de ellos conoce la importancia de la política de seguridad en la entidad mientras el 20% no tiene claro el punto de partida para garantizar el manejo de la información y confidencialidad del mismo en la aplicación web.

Análisis:

Siendo esta pregunta como la más clave para la realización de la auditoria, es importante profundizar en el tema a todos los usuarios mediante charlas o volantes informativos para la concientización de los datos que se manejan en la entidad y así garantizar la confianza de los declarantes.

- Pregunta N° 5

¿Conoce el tratamiento que se le debe dar a los correos con origen sospechoso?

Tabla N° 6 Resultado 5° Pregunta

| RESPUESTAS | TOTAL | |
|---|---|---|
| | CANTIDAD | % |
| SI | 9 | 90% |
| NO | 1 | 10% |
| TOTAL | 10 | 100% |

Fuente: El autor

Grafico 5. Consolidado pregunta N°5


Fuente: El autor

Interpretación:

Siendo un total de 10 usuarios encuestados el 90% de ellos conoce la importancia de visualizar y detectar los correos sospechosos siendo el 10% que no tiene claro el detectar el origen de un correo sospechoso.

Análisis:

Debido a esta cifra vemos como los usuarios día a día han ganado conocimiento para este tema de la identificación de los correos enviados por la entidad y no caer en trampas con fines delictivos.

- Pregunta N° 6

¿Conoce alguien diferente de usted sus usuarios y contraseñas de acceso?

Tabla N° 7 Resultado 6° Pregunta

| RESPUESTAS | TOTAL | |
|---|---|---|
| | CANTIDAD | % |
| SI | 0 | 0 |
| NO | 10 | 100 |
| TOTAL | 10 | 100 |

Fuente: El autor

Grafico 6. Consolidado pregunta N°6


Fuente: El autor

Interpretación:

Con un total de 10 usuarios encuestados el 100% de ellos tiene la claridad de que los credenciales de acceso a la aplicación web son confidencial y única.

Análisis:

La mayoría de los usuarios saben de la importancia de manejar estas claves de manera personalizada, por la información que se maneja dentro de ella y los datos sensibles.

- Pregunta N° 7

¿Para el manejo dentro de la plataforma MUISCA, es confiable el tratamiento de los datos que se manejan allí?

Tabla N° 8 Resultado 7° Pregunta

| RESPUESTAS | TOTAL | |
|---|---|---|
| | CANTIDAD | % |
| **SI** | 8 | 80 |
| **NO** | 2 | 20 |
| **TOTAL** | 10 | 100 |

Fuente: El autor

Grafico 7. Consolidado pregunta N°7


Fuente: El autor

Interpretación:

De un total de 10 usuarios encuestados el 80% de ellos podemos ver dicen estar seguros de realizar los trámites dentro de la aplicación web mientras el 20% duda y requiere que se maneje otro mecanismo de seguridad en ella.

Análisis:

Podemos visualizar que la confianza del usuario al realizar sus trámites de declaración o consulta asumen estar confiables, esto al trato de la información y el respaldo el cual son factores determinantes para que esté disponible y actualizado dentro de la aplicación web.

Lo anteriormente mostrado fue basado en la aplicación de la encuesta física de acuerdo al modelo presentado y este se ve plasmado al final del documento **(Ver Anexos).**

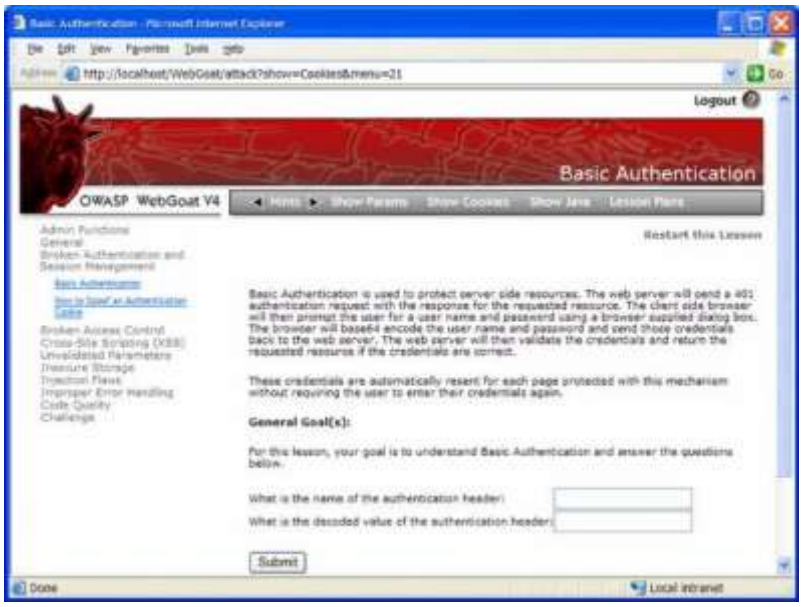
# 6. CARACTERISTICAS DE LAS HERRAMIENTAS

La herramienta para los laboratorios del proyecto OWASP se manejará por WEBGOAT.

Esta herramienta mostrará los procesos claves sobre la seguridad en las aplicaciones web:

- Autenticación
- Autorización
- Gestión de sesiones
- Validación de datos
- Gestión de errores, log y auditoría
- Configuración

Figura 1. Página inicio del Webgoat

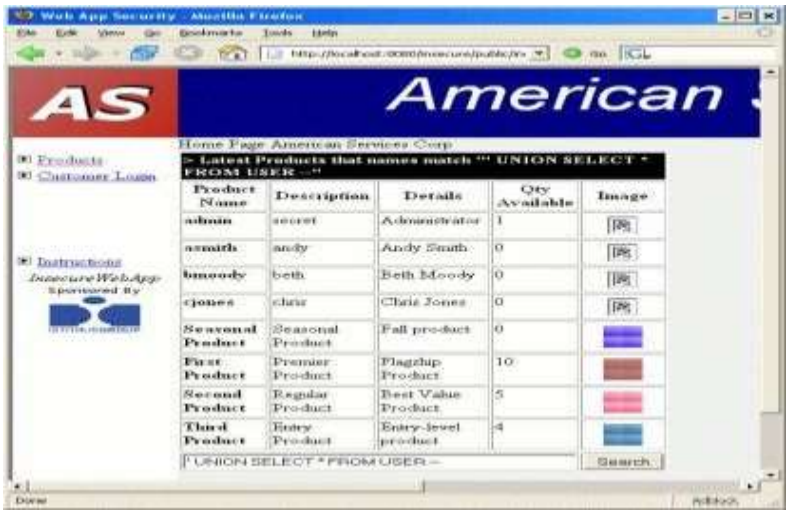



Fuente: http://www.notageek.it/owasp-webgoat-project.html

Según a lo informado en el planteamiento del problema, y revisado con la GUIA de Proyectos OWASP, nos centraremos en estas metodologías y sus funcionalidades:

## 6.1. OWASP Insecure Web App:

Figura 2. Página de inicio de Insecure




Fuente: https://sourceforge.net/projects/insecurewebapp/

InsecureWebApp es una herramienta por el cual su factor principal nos incluye vulnerabilidades comunes en aplicaciones Web. Por ende, su objetivo de pruebas es a través de pestesting automatizadas, estos apoyados en manuales, su amplio análisis de código fuente, monitoreo y evaluación de vulnerabilidades así generando modelado de amenazas para ser practico una toma de decisiones y ejecución.

Esto ante todo nos sirve como ayuda para investigar y mejorar las habilidades e implementaciones de diseño y codificación segura. Es fundamental que personal como arquitectos y desarrolladores se deban aprender a identificar las vulnerabilidades en una aplicación Web real.

Los objetivos fundamentales se resumen en tres tipos:

a) Demostración de eventos en logs donde pueden ser las vulnerabilidades de las aplicaciones web.

b) Analizar y verificar la relación que existe entre la teoría de seguridad en aplicaciones web seguras y el código implementado en su momento por un especialista de desarrollo.

c) Se sirve aprender de estas vulnerabilidades para ser arregladas de manera eficiente y menos atracción para los atacantes.

Parte de ello para el estudio y aplicación de esta herramienta se asume al auditor tener conocimientos previos o teoría acerca de vulnerabilidades en aplicaciones Web, el cual pone en particular la manipulación de parámetros, el buscar romper autenticación, aplicar inyección SQL e inyección HTML entre otros.

## 6.2. OWASP Pantera Web Assessment Studio:

Figura 3. Página de inicio de Pantera


Fuente: https://www.owasp.org/index.php/File:Pantera1.jpg

En esta herramienta se usa una versión de SpikeProxy el cual nos proporciona una poderosa máquina de monitoreo para análisis de aplicaciones Web. Uno de los objetivos se trata de combinar las instrucciones automáticas y donde se aplican para ver mejores resultados en las pruebas de intrusión.
Esta se puede realizar personalizaciones como el efecto visual, colores, fuentes, vistas entre otros para la manera más fácil al especialista de acceder a la información, tomar decisiones, análisis de datos, etc.

El lenguaje para esta herramienta es trabajado sobre Python donde su arquitectura es multiplataforma, de fácil instalación y uso haciendo de esto el lenguaje perfecto para usarlo. Cuando hablamos de multiplataforma nos

centramos en sistemas tradicionales (Windows, Linux) y por el lado de multinavegador están como él (IE, Firefox, Chrome, Opera).

Un beneficio de la poderosa herramienta está en el análisis de código, esto significa hace que cada página Pantera analiza y demuestra resultados como comentarios, scripts, vulnerabilidades, etiquetas ocultas y más detalles.

En este tipo de prueba es importante recalcar el análisis de forma transparente para el usuario mientras se prueba el aplicativo Web y parte del resultado de esta información es almacenada en la base de datos para la toma de decisiones.

La configuración en los archivos de datos XML hace para el auditor una manera práctica de realizar las pruebas y ataques para ver las vulnerabilidades a encontrarse en el objetivo, haciendo de este en el resultado almacenado en archivos XML para la validación y la manera de corregir detalles.

El gestor de la base de datos donde se almacena lo encontrado se basa en MySQL, siendo un factor interesante para guardar la auditoria; al momento de realizar una auditoria con Pantera este genera una sesión, en donde este permite editar, borrar y modificar el contenido de la auditoria. La ventaja se radica donde al día siguiente en el mismo lugar donde se detuvo continuaría con el proceso y la garantía de soporte en este gestor para la manipulación del resultado.

Las diferencias en estas auditorías se ven reflejada por sesiones, en resumida ofrece administración de proyectos para crear nuevos, abrir o borrar haciendo de este una manera práctica y ágil de manejar los datos obtenidos.

La importancia de la generación de reportes garantiza en las auditorias con toda la información resumidas y las vulnerabilidades encontradas; soportando formatos conocidos como los son en HTML, XML, PDF, ente otros y a su vez los reportes también pueden ser personalizados para la presentación en un comité.

En síntesis, final las evidencias tomadas sobre esta auditoria con las metodologías mencionadas anteriormente, nos servirán de análisis y toma de decisiones para generar los respectivos informes técnicos y ejecutivos para demostrar a la entidad DIAN sobre las vulnerabilidades encontradas y con ello plasmaremos la propuesta final con el fin de tomar medidas de seguridad y controles, por lo cual les servirá de referente para las demás aplicaciones web de esta entidad.

# 7. DESARROLLO Y PROCEDIMIENTO

En esta sección veremos el paso a paso de las herramientas a trabajarse, para tal fin sobre la ejecución de la auditoria a aplicaciones web seguras de la entidad DIAN.

## 7.1. INSTALACION OWASP INSECURE WEB APP

Esta herramienta se encuentra alojada y disponible en la siguiente url: https://sourceforge.net/projects/insecurewebapp/files/

La configuración mínima recomendada es:

- Apache Tomcat 4.1.31 con Java de Sun 1.4.2_06. Fuente: https://archive.apache.org/dist/tomcat/tomcat-4/v4.1.31/bin/

- Java SDK SE Versión 8. Fuente: http://www.oracle.com/technetwork/java/javase/downloads/jdk8-downloads-2133151.html

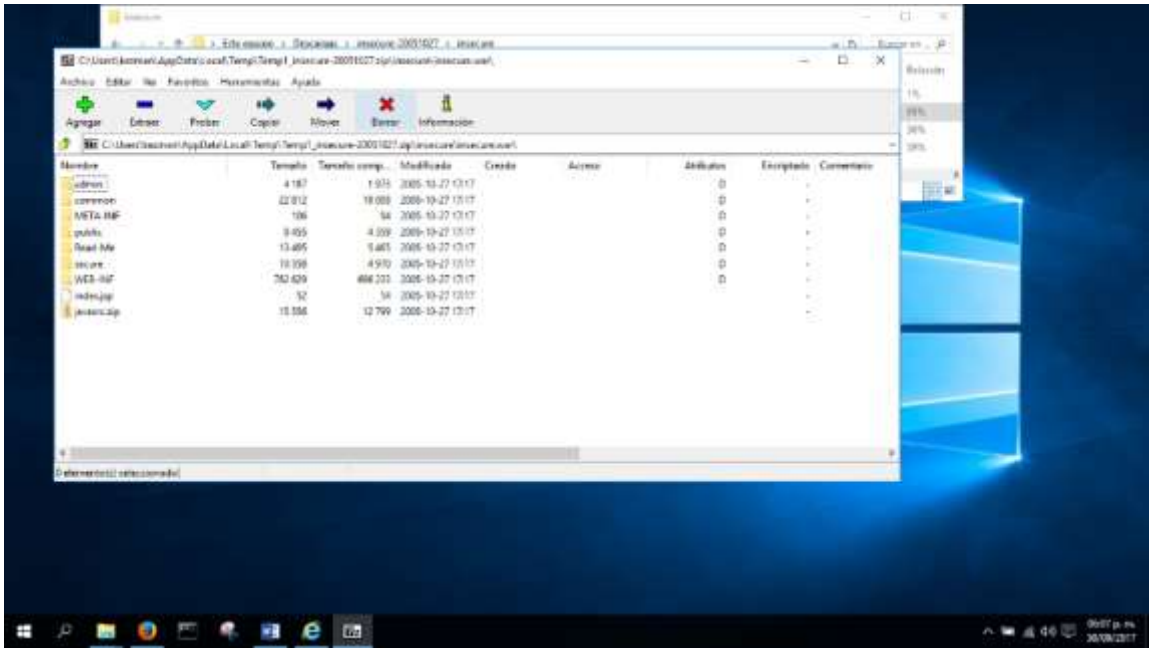
- InsecureWebApp utiliza una base de datos en memoria (HSQL) pero otros orígenes de datos son posibles.

- InsecureWebApp está disponible como un archivo .war desplegable, incrustado en Tomcat.

Se verá a continuación y paso a paso del proceso de instalación:

La figura 4 se muestra la descarga y el contenido de esta herramienta.

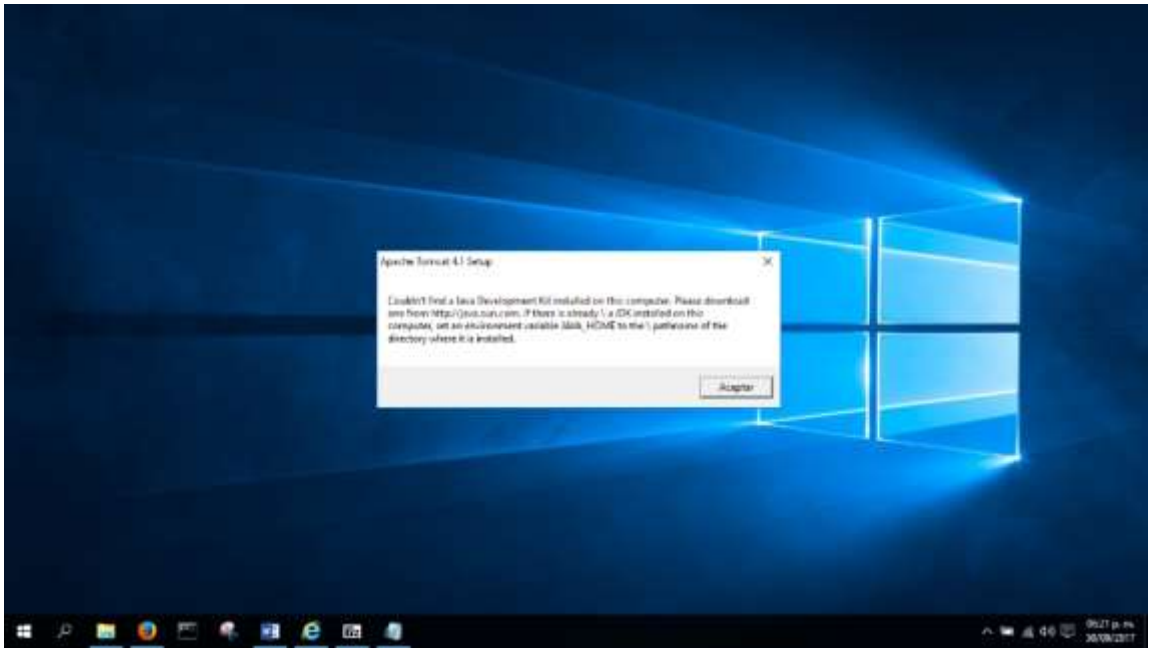
Figura 4. Comprimido de InsecureWeb



Fuente: El autor

La figura 5. Se observa un mensaje de alerta, es la instalación de un complemento JDK (Java) para continuar e instalar un servidor local (Tomcat 4.1).

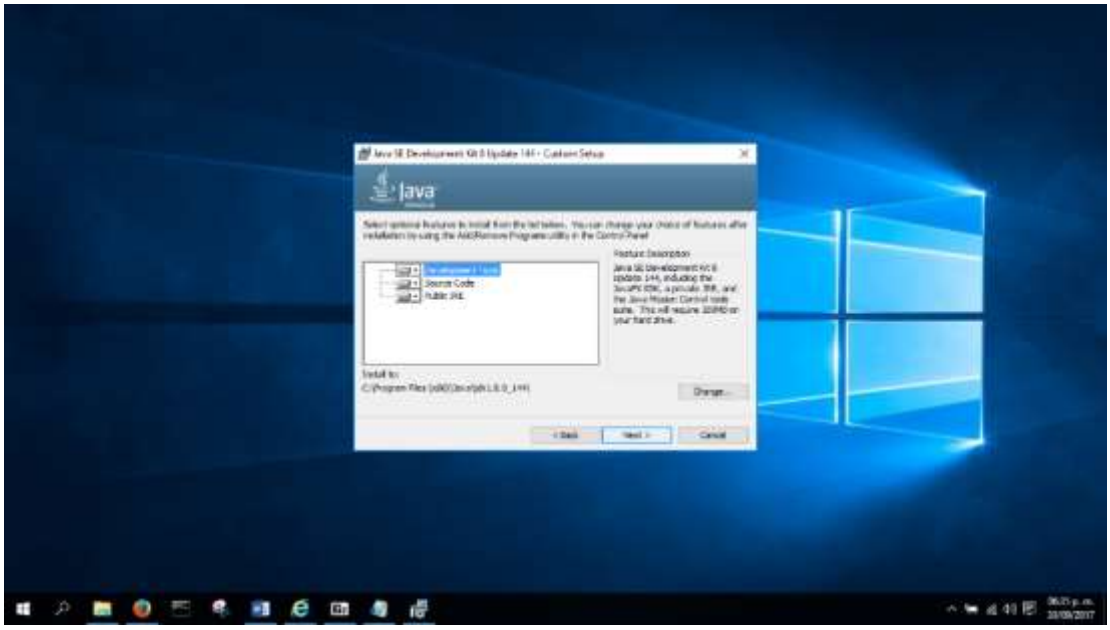
Figura 5. Requerimiento servidor web local



Fuente: El autor

La figura 6. Se detalla en ítems lo que viene comprendido en el JDK del Java.

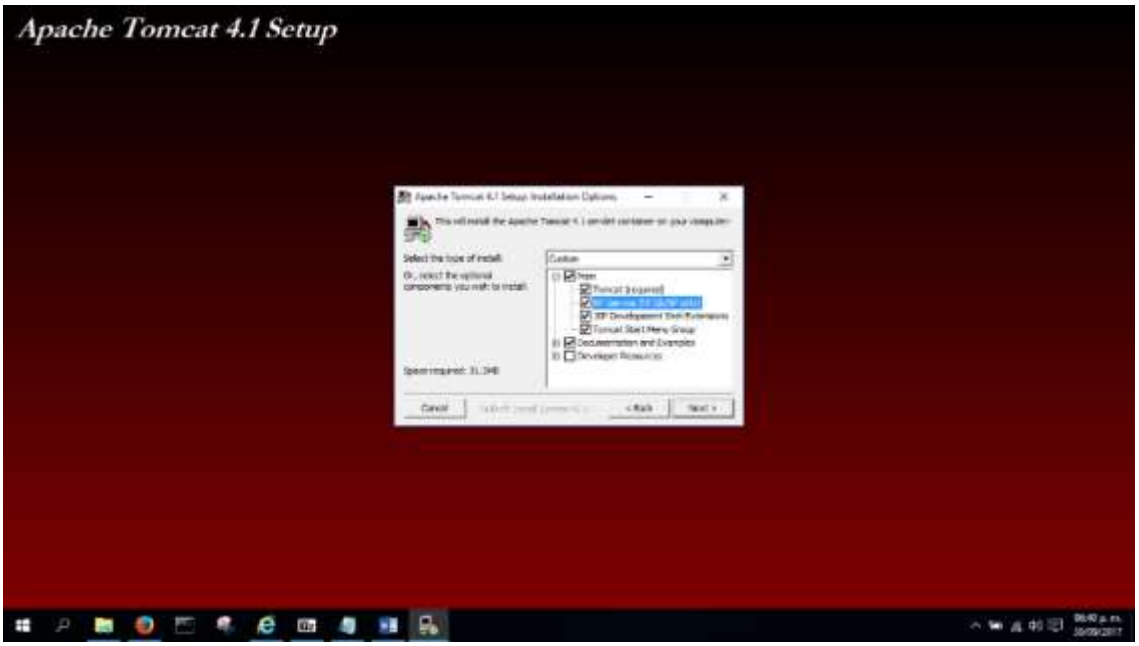
Figura 6. Complementos SDK




Fuente: El autor

La figura 7. Se muestra los servicios el cual va a manejar el Servidor local Tomcat.

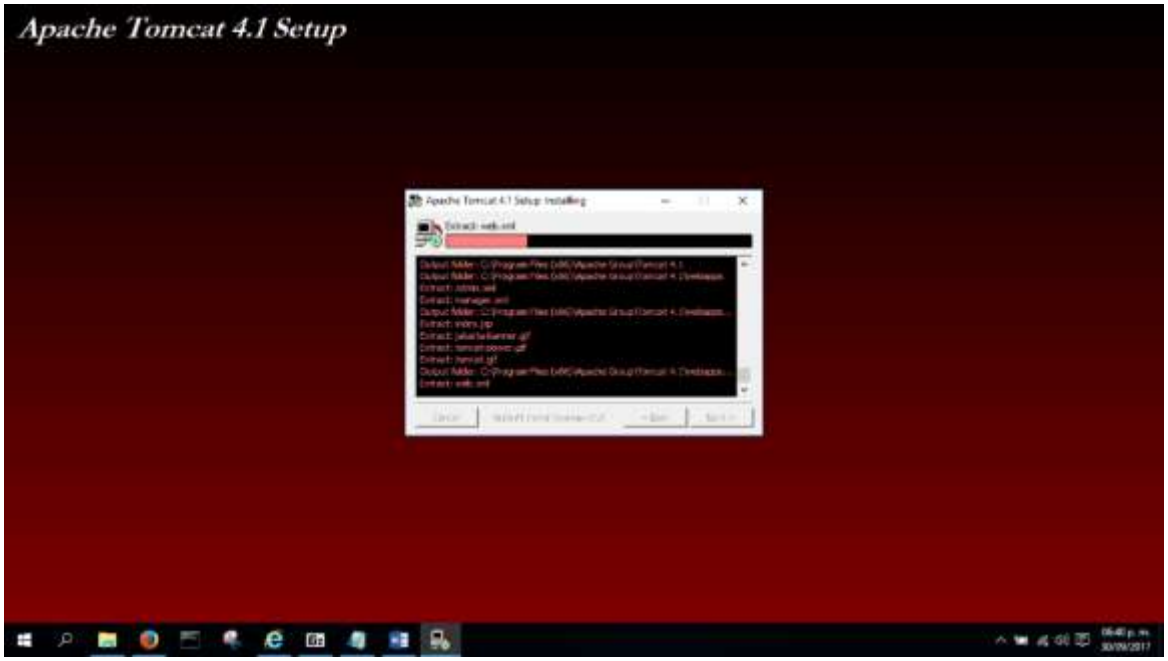
Figura 7. Complementos Tomcat




Fuente: El autor

La figura 8. Se visualiza el avance del Tomcat en la maquina a trabajar.

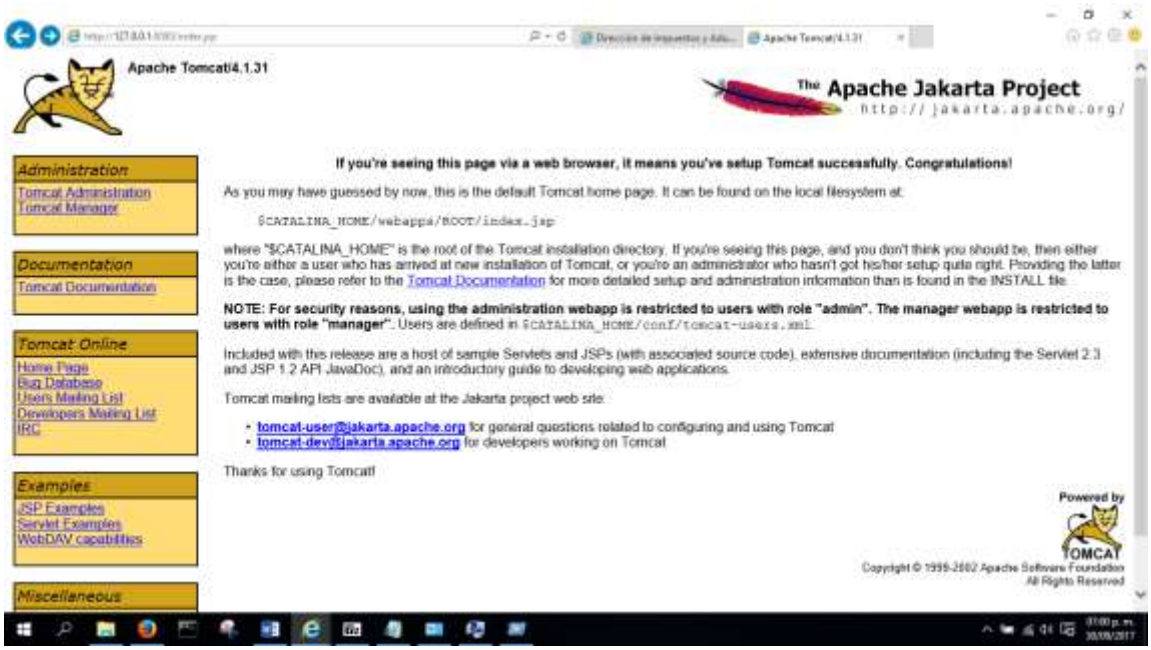
Figura 8. Proceso instalación Tomcat




Fuente: El autor

La figura 9. Se aprecia el resultado favorable de la instalación del servidor local Tomcat en la máquina.

Figura 9. Servidor local activado




Fuente: El autor

La figura 10. Se visualiza la página de inicio de la herramienta seleccionada para la auditoria.

Figura 10. Página inicio InsecureWeb


Fuente: El autor

## 7.2. INSTALACION OWASP PANTERA WEB ASSESSMENT STUDIO

La herramienta se encuentra disponible en la siguiente url: https://sourceforge.net/project/showfiles.php?group_id=64424&package_id=208668&release_id=483035

La configuración mínima recomendada es:

- Python 2.4.4 Lenguaje de programa. Fuente: https://www.python.org/download/releases/2.4.4/

- MySQL versión 5. Fuente: https://dev.mysql.com/downloads/mysql/

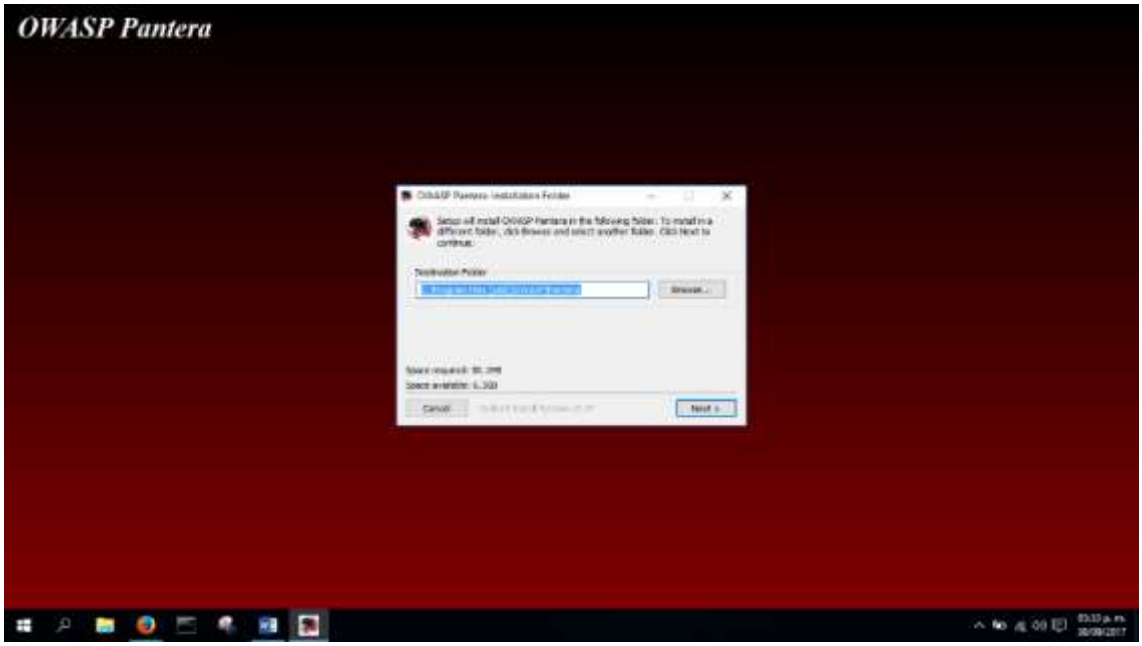
- PyOpenSSL. Fuente: https://pypi.python.org/pypi/pyOpenSSL

- FormBuild 4.0.0 . Fuente: https://pypi.python.org/pypi/FormBuild

Se verá a continuación y paso a paso del proceso de instalación:

La figura 11. Se refleja el inicio de la instalación de la herramienta y su posible ubicación en la máquina.

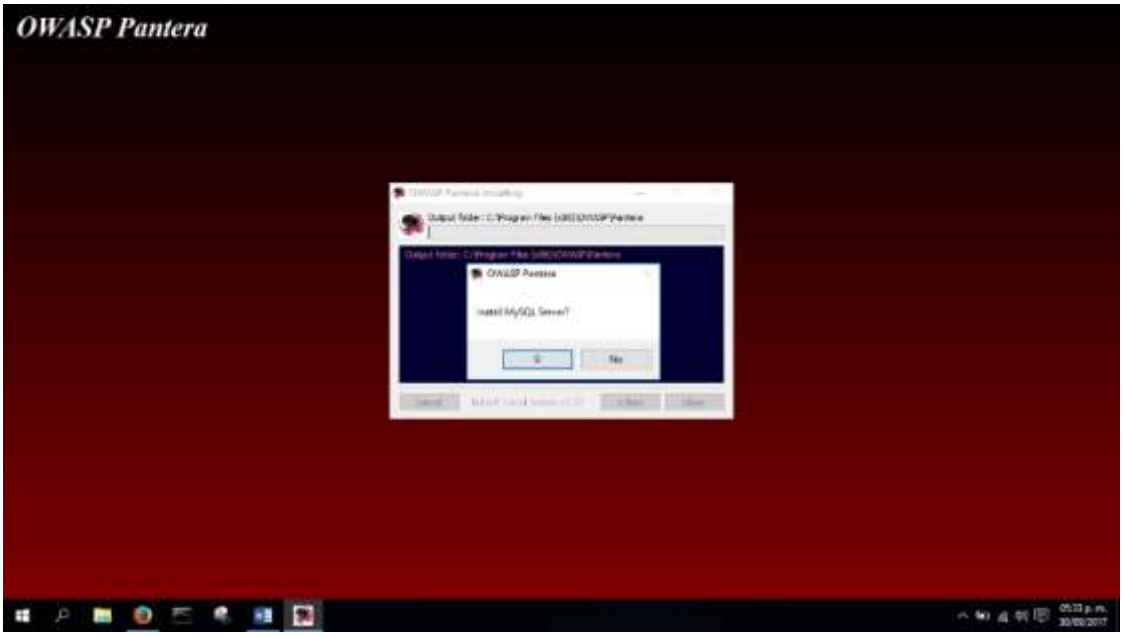
Figura 11. Instalación primaria Pantera




Fuente: El autor

La figura 12. Se observa una alerta de los complementos mínimos para la instalación efectiva de esta, en este caso un gestor de base de datos.

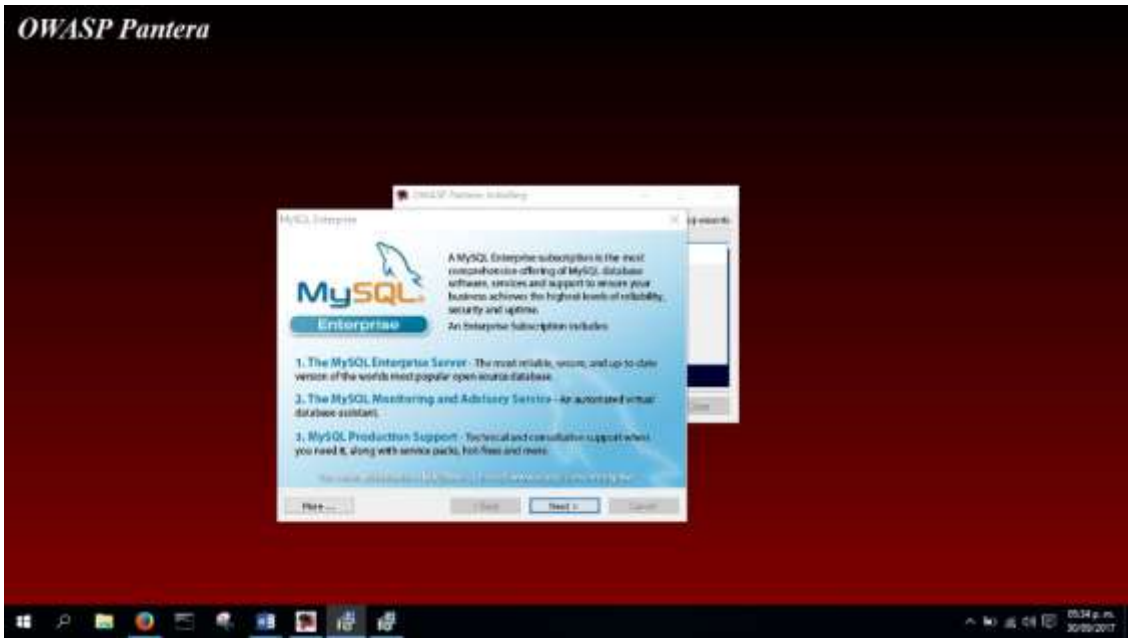
Figura 12. Requisitos mínimos herramienta




Fuente: El autor

La figura 13. Se visualiza el from de instalación del MySQL.

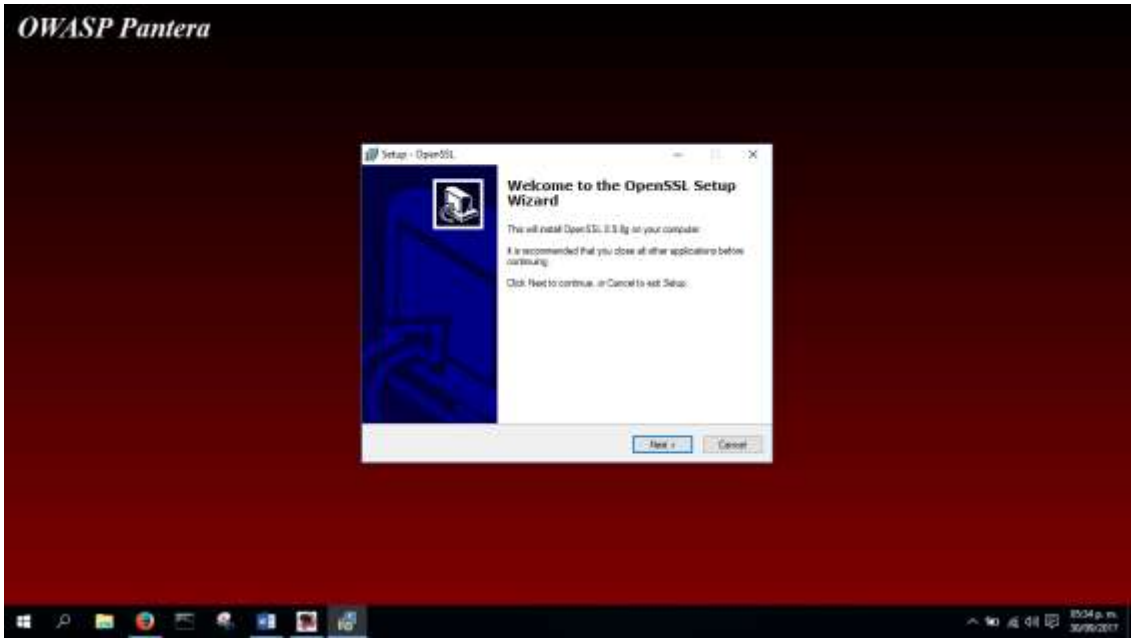
Figura 13. Gestor MySQL




Fuente: El autor

La figura 14. Se continúa con la instalación del complemento Open SSL esto haciendo a referencia del tema de certificado de seguridad.

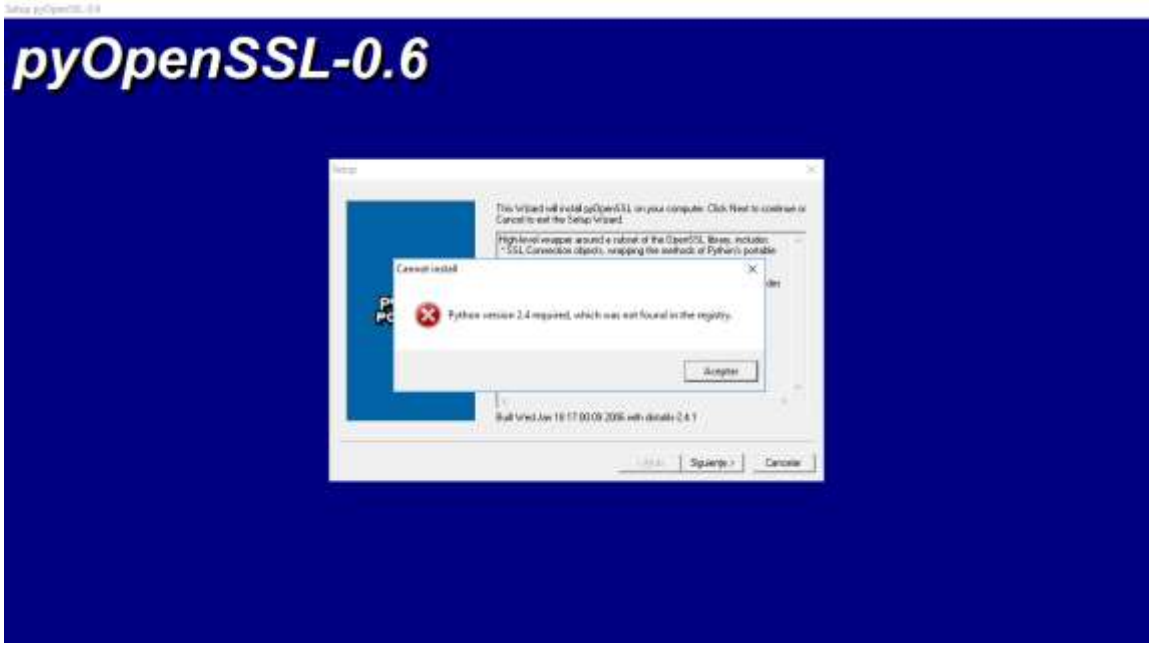
Figura 14. Complemento Open SSL




Fuente: El autor

La figura 15. Se aprecia una alerta indicando la instalación del lenguaje requerido como es este caso el Python.

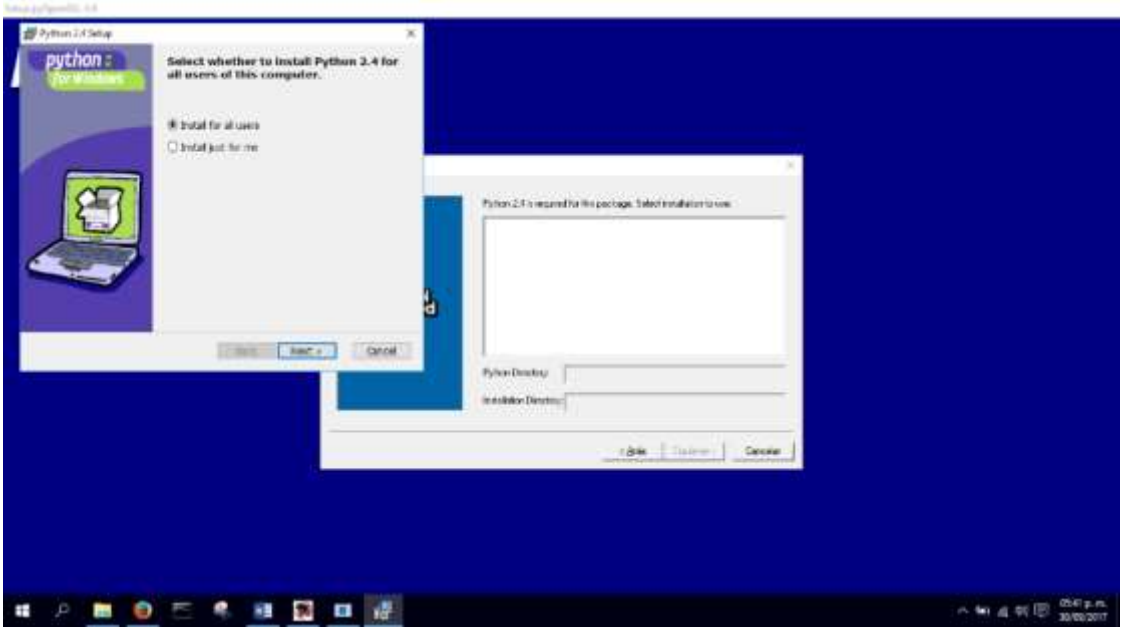
Figura 15.  Solicitud de herramienta Python




Fuente: El autor

La figura 16. Se detalla las maneras de trabajar en la máquina, en este caso se utilizará para el usuario activo o sesión trabajada.

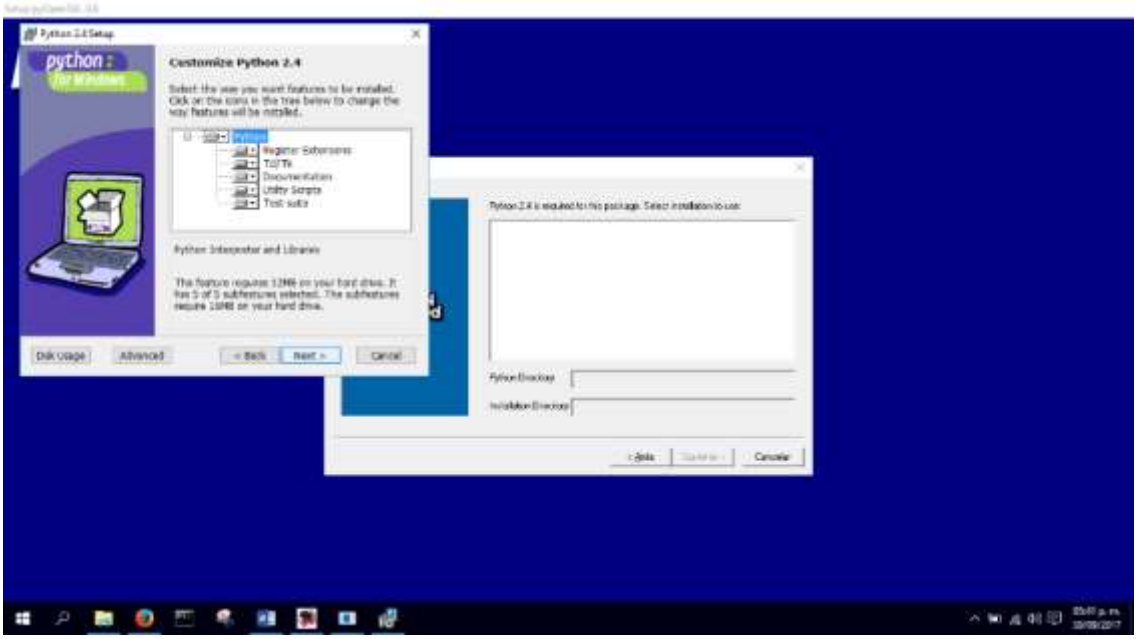
Figura 16.  Instalación primaria Python




Fuente: El autor

La figura 17. Se observa las características contenidas en este lenguaje a tenerse en cuenta, seleccionaremos todas para el correcto funcionamiento.

Figura 17. Complementos Python




Fuente: El autor

La figura 18. Se observa la inclusión de un paquete del Python el cual nos sirve de relación con MySQL (conexión).

Figura 18.  Paquete PIL

Fuente: El autor

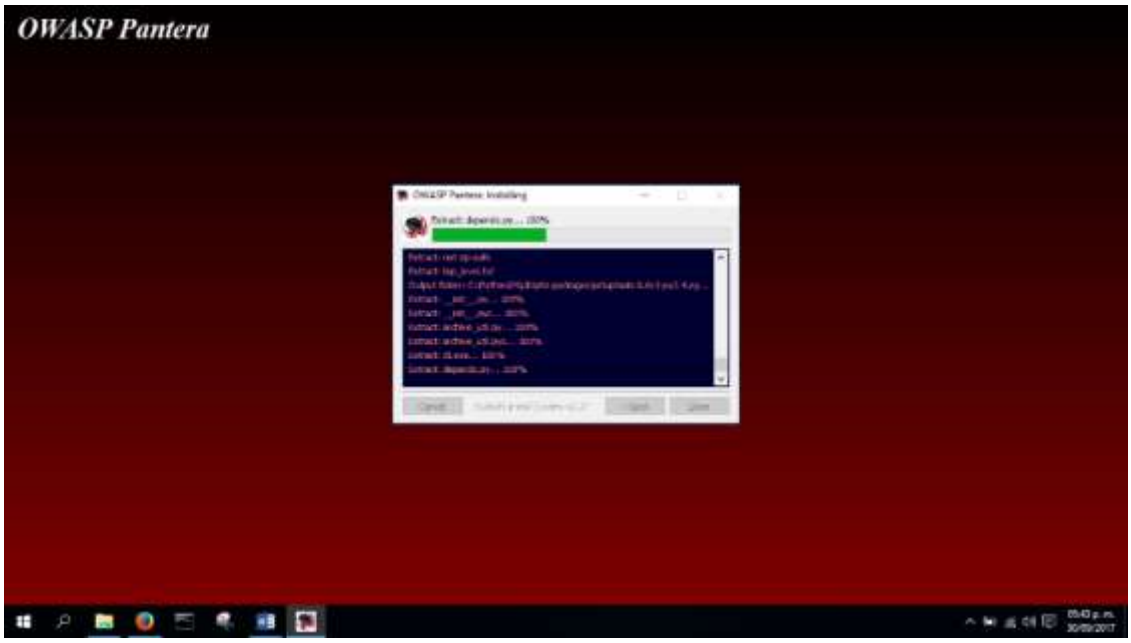
La figura 19. Se aprecia las características y la forma que está diseñado para trabajarse entre sí.

Figura 19. Relación MySQL-Python


Fuente: El autor

La figura 20. Se demuestra el avance de instalación de la herramienta de auditoria escogida.

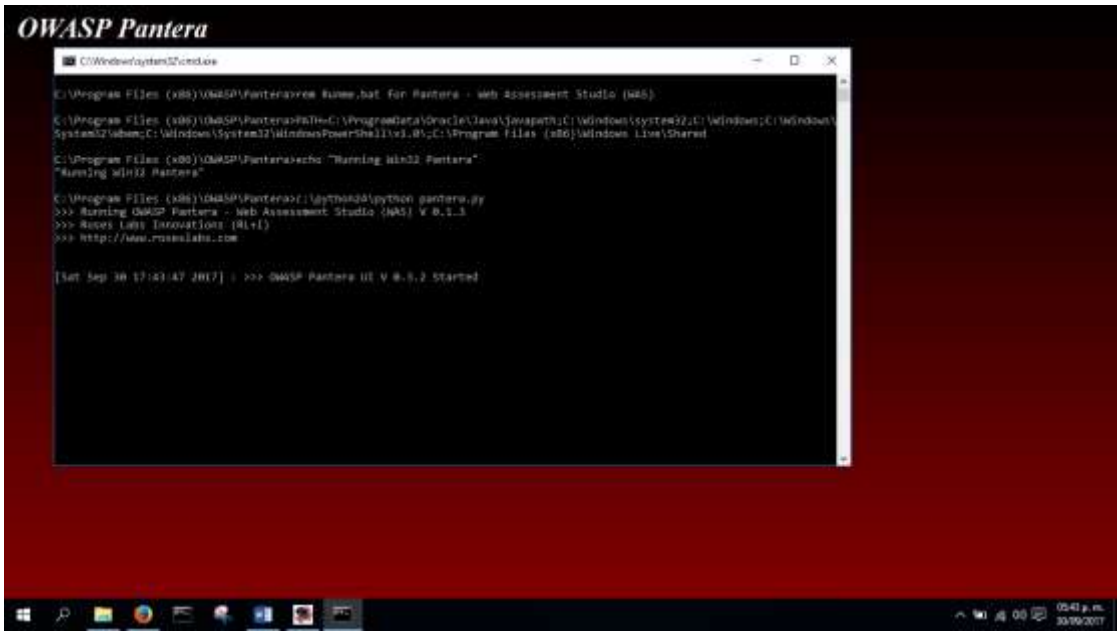
Figura 20. Desarrollo final Pantera




Fuente: El autor

La figura 21. Se observa el resultado del funcionamiento de la herramienta en tiempo real (escaneo).

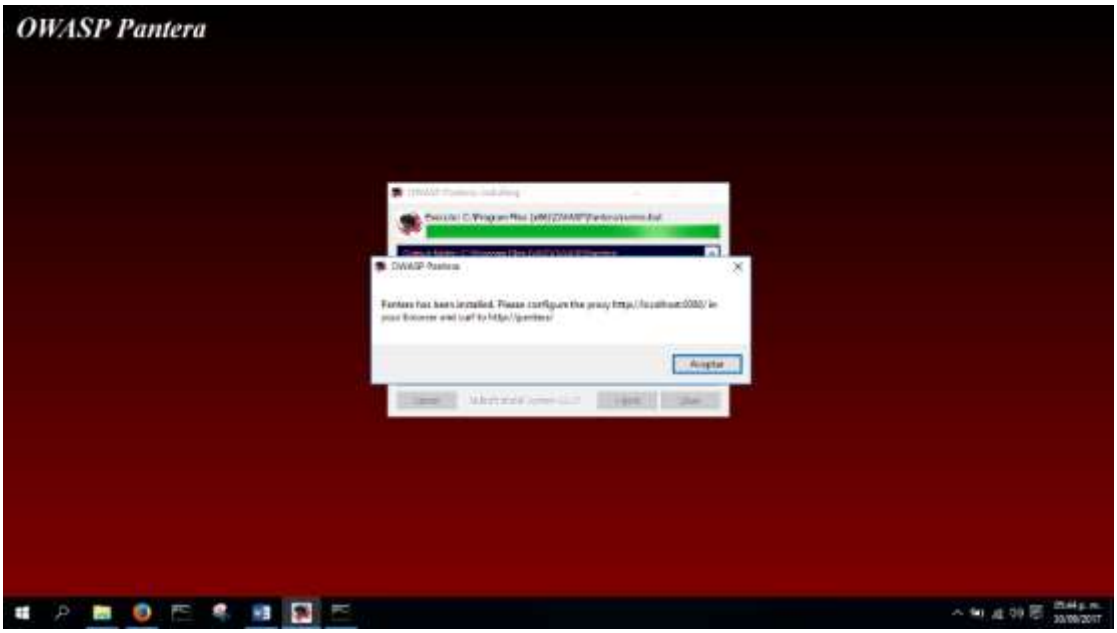
Figura 21. Prueba de la instalación




Fuente: El autor

La figura 22. Se aprecia el mensaje de configuración para realizar las pruebas de auditaje en la máquina (localhost).

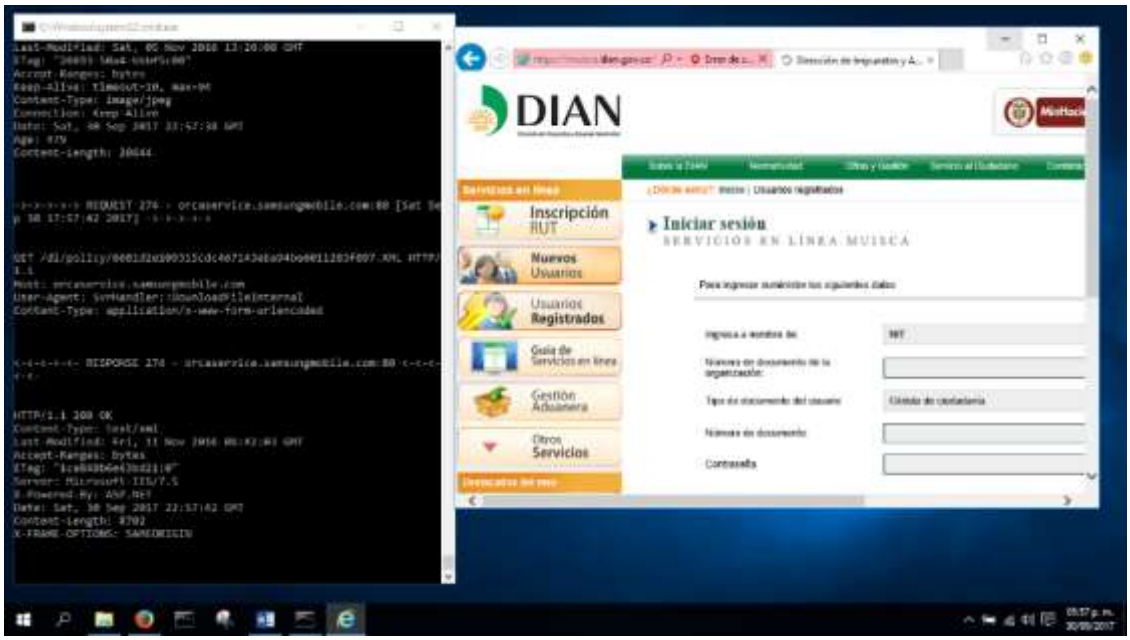
Figura 22.  Mensaje de configuración final




Fuente: El autor

La figura 23. Se demuestra el resultado final de la herramienta a trabajarse.

Figura 23.  Funcionamiento final




Fuente: El autor

# 8. DESARROLLO DE LA AUDITORIA

En una auditoría de este tipo a una entidad como la DIAN es necesario cumplir con una serie de requisitos para ver el alcance y las situaciones del trabajo a realizarse.

Para ello en este trabajo lo que buscamos es demostrarle al cliente sobre el desarrollo propuesto en esta auditoría web.

Es de vital importancia esclarecer puntos el cual nos va a llevar a tener claro los puntos a trabajarse:

- El alcance de la propuesta indicada.
- La revisión del entorno al cual auditar.
- Las metodologías para utilizar de acuerdo con lo informado por el personal TI.
- La distribución del tiempo a llevarse en la auditoría.
- Los respaldos y seguimientos ante la detección de vulnerabilidades en la aplicación web escogida.
- El escoger y describir los controles a auditar.
- Los requisitos básicos para realizar las pruebas dentro de la entidad.

Al no tratarse de una auditoría real en el sitio, la aplicación web a auditar se implementará en un entorno de laboratorio. Con ello se trabajará en las herramientas escogidas para este proyecto para realizar las pruebas e implementarlas.

Para la ejecución de la auditoria se efectuarán las pruebas indicadas en el desarrollo de las mismas contra la aplicación web MUISCA a auditar. De tal modo la intervención de las pruebas se realizaría bajo el siguiente ciclo:

- Técnica de Escaneo:

En esta se obtiene importante información sobre los activos de especial enfoque a la comunicación entre la red, este se referencia al escaneo de puertos, llamado de servicios, hallazgo de host entre otros.

- Técnica de Reconocimiento:

Va encaminado a obtener información en relación a bases de datos, servidores como el DNS, WSUS, WEB entre otros.

- Detección de vulnerabilidades:

En este paso se recopila la información obtenida de las técnicas anunciadas anteriormente, luego se procede a identificarse las vulnerabilidades por el cual en su momento se presenta en la aplicación web escogida.

- Comprobación de vulnerabilidades:

Para esta parte se pide verificar las vulnerabilidades y realizar las pruebas directamente, con el fin de ver el comportamiento y resultado concreto para evaluar.

- Estudio de resultados:

En este se efectuará un examen detallado de toda la información recopilada y obtenida.

En síntesis final en la auditoria web, es importante referirnos al informe final donde se originará el cuerpo del proyecto final; se llamará el seguimiento o transcurso de la auditoria aplicada para un entorno web de la entidad, a su vez los detalles específicos de la ejecución de las herramientas, las encuestas generadas, las evidencias encontradas y por ultimo las recomendaciones finales para la mejora continua de la aplicación web, con base a ello entregadas a la entidad.

Para la realización de esta auditoria web, es importante recalcar lo siguiente; en las entrevistas sostenidas con el personal de tecnología de la DIAN se dejó definido el alcance de este proyecto, como a su vez el bosquejo y las pruebas en el tiempo estimado y por último la descripción final de lo encontrado en esta auditoría.

Con la recopilación y todo a su vez lo anterior este corroborado con el personal se tiene en cuenta el cronograma pactado para la ejecución de las pruebas contra aplicación web objetivo MUISCA.

En la confirmación de los riesgos se explorará en la mayoría de controles de seguridad, estos bajo el informe OWASP Testing; para esto se ha intentado incorporar en lo posible, para las evidencias a las pruebas a realizarse.

Hoy en día las herramientas sistemáticas para estas pruebas de intrusión ofrecen gran cantidad de información en sus resultados. Los informes de estas herramientas se incluyen en los anexos de este documento.

Las pruebas de auditoria se ejecutaran en un laboratorio o área de Testing de la entidad; este a su vez en una maquina física nos enfocamos en el contenido de una máquina virtual (VMWare) con las herramientas OWASP escogidas, sabiéndose que el alcance definido en esta auditoria web es sólo para la aplicación de recaudos MUISCA, situado en el dominio https://muisca.dian.gov.co .

En la auditoría a ejecutar es de enfoque caja gris, donde se realizarán pruebas con similitudes de métodos a la caja negra, en pocas palabras disimulando ataques reales. En tanto se contará información previa de la aplicación web a auditar, y en donde la información más relevante serán los ficheros de configuración, diagramas de red y arquitectura, entre otros.

# 9. PLAN DE AUDITORIA

En este plan de auditoría web se observará detalles significativos; sabiéndose que para una auditoría real a una entidad como esta sería importante tramitar una serie de permisos para ser de manera realista el alcance, esto bajo las circunstancias del trabajo a realirse, en este documento se busca ante ellos la idoneidad de la entidad sobre el informe en el plan de auditoría.

Es válido informar los siguientes puntos:

1. Instalación del alcance.
2. Definición del entorno escogido para auditar.
3. Aplicación de metodologías que se usarán.
4. Implementación de los plazos acordados en la auditoría.
5. La comunicación con los responsables durante el proceso.
6. El ejercicio y pruebas ante la detección de vulnerabilidades críticas en el sistema a auditar.
7. Condiciones y criterio para realizar las pruebas de intrusión.

Al no tratarse de una auditoría real, el aplicativo web a auditar se implementará en un entorno de laboratorio, en ello se seleccionará el objetivo específico para lanzar las pruebas e implementarla.

Nuestro objetivo de la auditoría a realizar para la entidad DIAN será identificar problemas de seguridad, para ser más exacto se lanzarán una serie de controles en una aplicación web y con ello se podrán realizar las siguientes pruebas:

Escaneos código, detección de vulnerabilidades y explotación de vulnerabilidades.

Las pruebas de auditaje se realizarán desde la dirección IP_EMPRESA. Desde esta dirección IP se lanzarán una serie de técnicas utilizadas para comprobar la presencia de brechas u focos de seguridad en la aplicación web, se entiende en el plan de auditoría se ejecutará entre las fechas del 15/08/2017 – 15/12/2017.

Los tiempos temporales indicados para las fases de la auditoría son los siguientes:

Tabla Nº 9. Fases

| Nombre de Fase | Fecha inicio | Fecha final |
|---|---|---|
| Planeación de Auditoría | 15/08/2017 | 08/10/2017 |
| Ejecución de pruebas de auditoría | 01/10/2017 | 31/10/2017 |
| Informe de auditoría | 15/11/2017 | 30/11/2017 |
| Presentación de la auditoría | 01/12/2017 | 13/12/2017 |

Fuente. El Autor

# 10. EVIDENCIAS ENCONTRADAS

A continuación, se verá reflejado con las herramientas la auditoria respectiva y así dar en detalle lo encontrado, se escogió lo más puntual con el fin de revisarse y tomar decisiones para mejoramiento y continuidad del negocio.

Se tomará la herramienta Insecure Web en el cual nos permitirá revisar si la aplicación web a auditar en este caso MUISCA, cuenta con focos de seguridad en el código utilizado por este software, se observará mediante una prueba de intrusión.

*El primer paso es ingresar al url objetivo y hacer clic en el botón Attack.

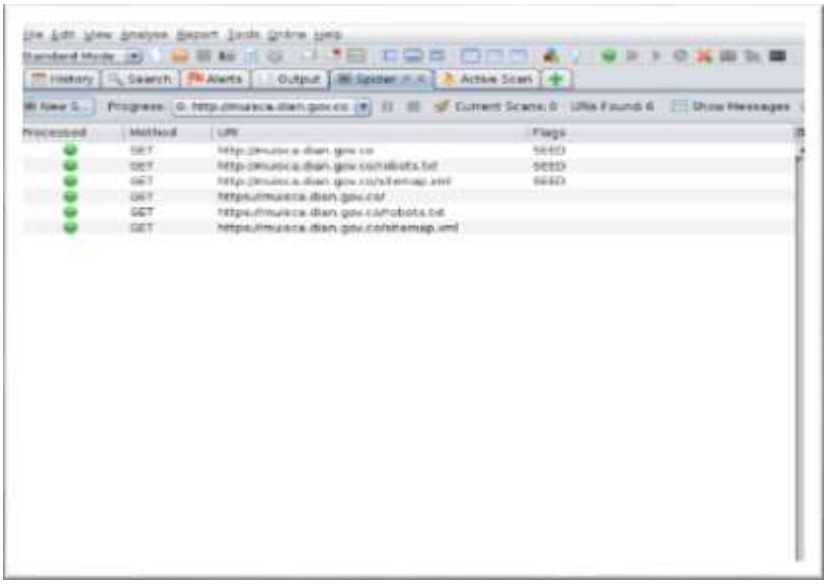
*Después de ello inicia la labor de escáner el sitio web para buscar las vulnerabilidades, situación que consume un tiempo considerable.

Para obtener una aplicación web segura, OWASP Insecure Web y Pantera, se sirven con estas características:[39]

- Una gestión organizacional que abogue por la seguridad.
- Políticas de seguridad documentadas y apropiadamente basadas en estándares nacionales.
- Una metodología de desarrollo con adecuados puntos de control y actividades de seguridad

[39] Políticas de seguridad informática – Redalyc. Extraido de http://www.redalyc.org/html/2654/265420388008/

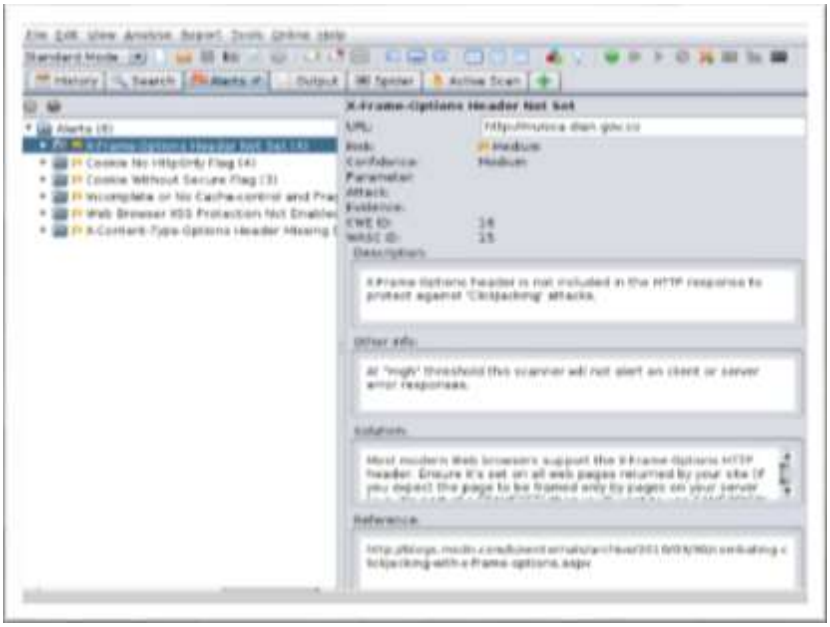
Figura 24. Herramienta Owasp Insecure evidencia 1



Fuente: El autor

Se observa en la imagen anterior que este aplicativo en referencia cuenta con un nivel aceptable de la utilización e ingreso de esta plataforma; en donde se realizan tramites de RUT, declaraciones entre otros.

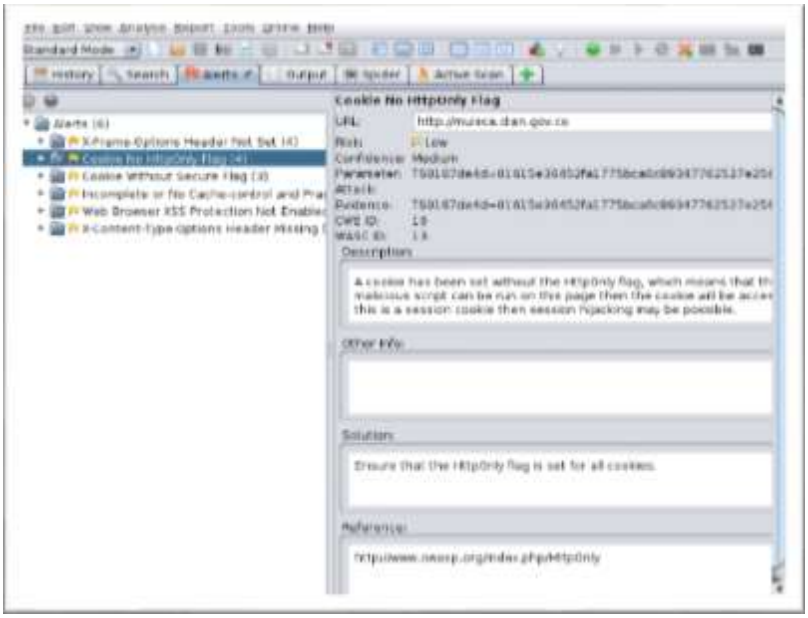
Figura 25.  Herramienta Owasp Insecure evidencia 2



Fuente: El autor

La figura muestra un método de filtro XSS del navegador web cuando está activado, en este indicando en la cabecera las respuestas HTTP X-XSS, con ello X-Frame se debe ajustar con parámetros rigurosos para dar respuestas efectivas al servidor.

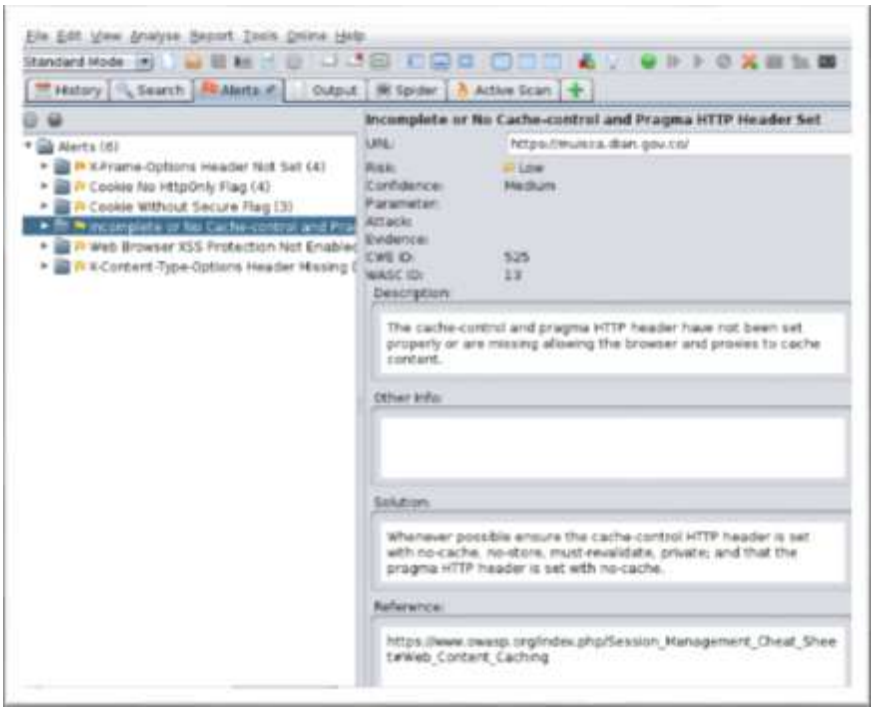
Figura 26. Herramienta Owasp Insecure evidencia 3




Fuente: El autor

Estos archivos de código JavaScript y cookies se cargan a partir de fuentes de confianza solamente, y las fuentes no pueden ser controladas por los usuarios finales de la aplicación.

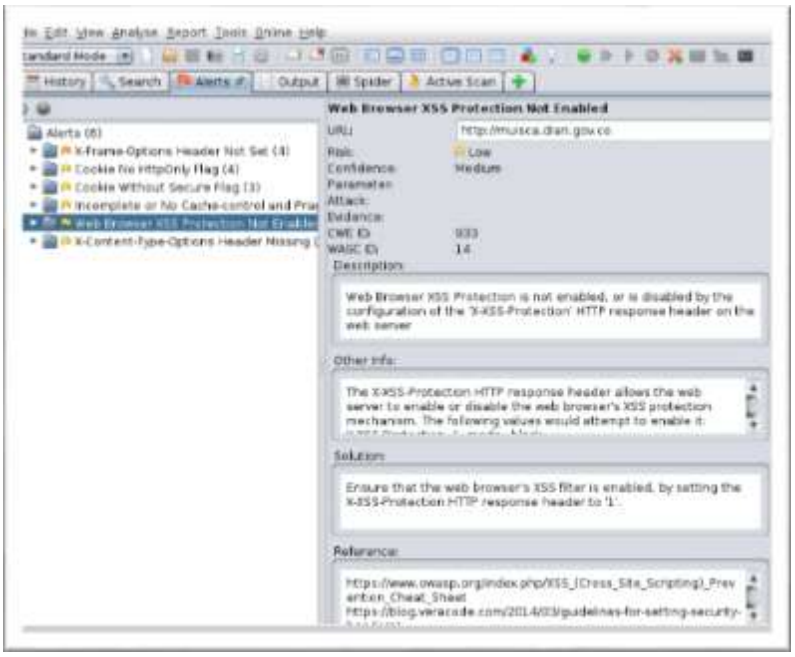
Figura 27. Herramienta Owasp Insecure evidencia 4




Fuente: El autor

Se detalla esta figura se detalla que no se cuenta con un nivel avanzado en la dirección HTTP, se solicita eliminar la dirección IP privada en el cuerpo de la respuesta HTTP; para estos comentarios se debe usar JSP / ASP y los comentarios por el lugar en HTML / JavaScript donde puede ser visto por los exploradores del cliente.

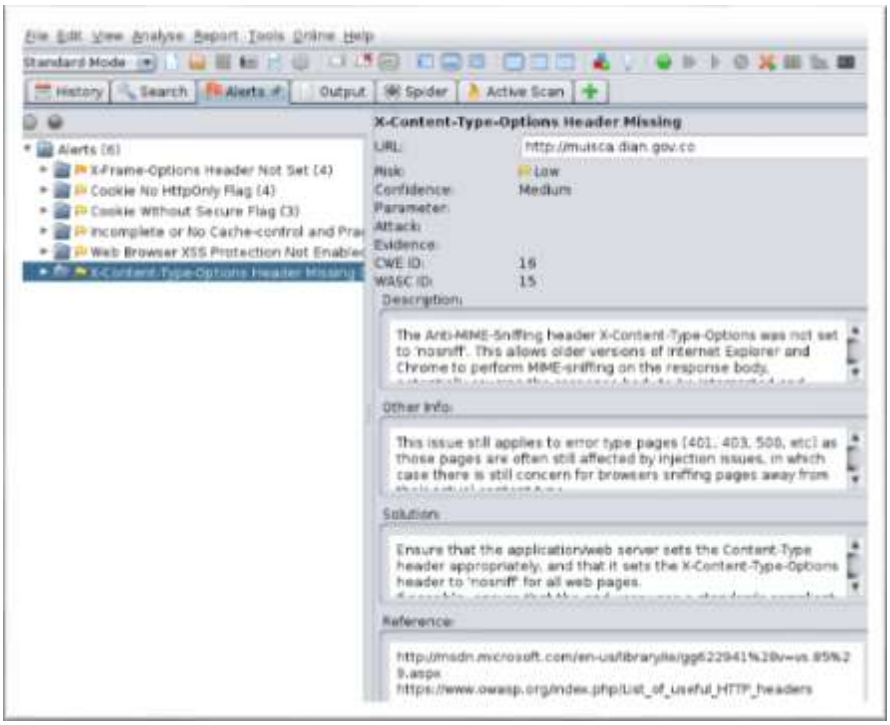
Figura 28. Herramienta Owasp  Insecure evidencia




Fuente: El autor

Al observar dentro del servidor de aplicaciones web en la entidad, se ve establecido la cabecera Content-Type inapropiadamente, por consiguiente, se refleja que la cabecera X-Content-Type-Opciones de 'NOSNIFF', es sensible y está siempre presente en todas las páginas web. Es por esto que se recomienda asegurar al usuario final utilizar un navegador web compatible y seguro con los mecanismos de seguridad de la información, para no conllevar a que se realice por parte del atacante un MIME-sniffing que comprometa con la información que se maneje allí; para este caso es recomendable el navegador Mozilla versión 48 en adelante.

Figura 29. Herramienta Owasp Insecure evidencia 6




Fuente: El autor

Se observa en este resultado, el problema del error de tipo (401, 403, 500, etc.) como esas páginas a menudo todavía se ven afectados por problemas de inyección SQL, por ello se ve como todavía hay posibles fallas en los navegadores, ya que las aplicaciones web pueden sufrir ruptura y extracción de datos en sitios no seguros o confiables. Se puede determinar este escáner no alerta sobre las respuestas de los clientes o del error del servidor.

Se realizan pruebas con Owasp Pantera con el fin de explorar y examinar la configuración de la arquitectura que hay en esta aplicación, en parte de estos sistemas se originan por defecto, configuraciones el cual hacen ver funciones principales de documentación, páginas de pruebas en donde no se deberían estar alojadas antes de versen en un entorno de producción.

El análisis de este se podría ver en importantes apartes directorios, ficheros de pruebas, los comentarios en las compilaciones del código y por ultimo también configuraciones del sistema que comprometen la seguridad en esta aplicación.

Al ejecutarse el escaneo de este se genera un documento en formato .txt y se reflejado a continuación:

En esta prueba se ve un ataque XSS reflejado, hace reflejar cuando el atacante o la persona curiosa introduce un código corrupto en un navegador a través de una respuesta HTTP. Al observar este código no es almacenado en la aplicación web, a su vez solo se genera cuando los usuarios externos abren el enlace con destino malicioso.

La referencia de este código el cual se indica es de lenguaje JavaScript, es manifestado en el navegador del usuario directamente. Por ende, se sirve eludir estas medidas y es necesario usar la codificación del mismo.

Para consultar el resultado de las pruebas realizadas es mostrado en el Anexo F.

Para la evaluación de los ficheros .txt mostrados era importante listar los puntos de entrada para ver cómo se hacen participes con la interacción al usuario.

Es de vital importancia estar atento al código con las peticiones HTTP, métodos GET y POST, parámetros y formularios que este genera en la aplicación web.

En estos métodos de uso GET y uso POST en el código, hace que se usen peticiones GET no sólidos, y al momento de transmitirse información importante van encaminados a que se usen los métodos POST.

Al mirar la captura de los datos obtenidos en las peticiones POST se comprobará con un proxy de la DIAN, el cual enlazará y probará las conexiones y con ello se dará acceso al código y ver las peticiones dentro de la misma.

Con el resultado de la verificación de los puntos de entrada de la aplicación web se usarán para verificar si en ella es vulnerable a SQLi, XSS entre otras vulnerabilidades.

En esta parte se refleja el otro informe de esta herramienta en donde se mencionan las vulnerabilidades encontradas, el nivel del riesgo y las recomendaciones a tener en cuenta:

- Resumen de alertas

Tabla N° 10 Resultado Consolidado Alertas Pantera

| Nivel de riesgo | Número de alertas |
|---|---|
| Alto | 0 |
| Medio | 1 |
| Bajo | 4 |
| informativo | 0 |

Fuente: El autor

- Detalles de alerta

Tabla N° 11 Resultado Reporte Pantera

| Medium (Medio) | X-Frame-Opciones de cabecera no Set |
|---|---|
| Descripción | cabecera-Opciones X-Frame no está incluido en la respuesta HTTP para protegerse de ataques 'clickjacking'. |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/index.shtml |

| | |
|---|---|
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/robots.txt |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/sitemap.xml |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/ |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/index3_archivos/filelist.xml |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/index3_archivos/editdata.mso |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/index3_archivos/themedata.thmx |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/index3_archivos/colorschememapping.xml |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/index3_archivos/image003.gif |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/index3_archivos/index3_archivos/filelist.xml |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/index3_archivos/index3_archivos/editdata.mso |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/index3_archivos/index3_archivos/themedata.thmx |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/index3_archivos/index3_archivos/colorschememapping.xml |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/index3_archivos/index3_archivos/image003.gif |
| Instancias | 2030 |
| Solución | La mayoría de navegadores modernos soportan la cabecera HTTP X-Frame-Options. Asegúrese de que está establecido en todas las páginas web que devuelve su sitio (si se espera que la página se enmarca únicamente por páginas de su servidor (por ejemplo, que es parte de un conjunto de marcos), entonces usted querrá usar SAMEORIGIN, de lo contrario si no esperas la página para ser enmarcado, se debe utilizar negar. PERMITIR dE-permite a los sitios web específicos para enmarcar la página web en los navegadores web compatibles). |
| Otra información | En el umbral de "alta" este escáner no alertar sobre las respuestas de los clientes o de error del servidor. |

| | |
|---|---|
| Referencia | http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx |
| CWE Id | Dieciséis |

| | |
|---|---|
| Id WASC | 15 |
| **Medio bajo)** | **Navegador Web XSS protección no habilitado** |
| Descripción | Navegador Web XSS La protección no está habilitada, o está deshabilitado de la configuración del encabezado de respuesta HTTP "X-XSS-Protección 'en el servidor web |

| | |
|---|---|
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/index.shtml |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/robots.txt |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/sitemap.xml |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/ |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/index3_archivos/filelist.xml |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/index3_archivos/editdata.mso |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/index3_archivos/themedata.thmx |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/index3_archivos/colorschememapping.xml |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/index3_archivos/image003.gif |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/index3_archivos/index3_archivos/filelist.xml |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/index3_archivos/index3_archivos/editdata.mso |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/index3_archivos/index3_archivos/themedata.thmx |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/index3_archivos/index3_archivos/colorschememapping.xml |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/index3_archivos/index3_archivos/image003.gif |
| Instancias | 2030 |
| Solución | Asegúrese de que el filtro XSS del navegador web está activado, indicando en la cabecera de respuesta HTTP X-XSS-Protección a '1'. |
| Otra información | El encabezado de respuesta HTTP X-XSS-Protection permite al servidor Web para activar o desactivar el mecanismo de protección XSS del navegador web. Los siguientes valores intentarían que les permitan:<br><br>X-XSS-Protección: 1; mode = bloque |

| | |
|---|---|
| | X-XSS-Protección: 1; Informe = http: //www.example.com/xss<br><br>Los siguientes valores se desactivarlo:<br><br>X-XSS-Protección: 0<br><br>El encabezado de respuesta HTTP X-XSS-Protection es compatible actualmente con Internet Explorer, Chrome y Safari (WebKit).<br><br>Tenga en cuenta que esta alerta se eleva solamente si el cuerpo de la respuesta podría potencialmente contener una carga útil XSS (con un tipo de contenido basado en texto, con una longitud distinta de cero). |

| | |
|---|---|
| Referencia | https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet<br><br>https://blog.veracode.com/2014/03/guidelines-for-setting-security-headers/ |
| CWE Id | 933 |
| Id WASC | 14 |
| **Medio bajo)** | **X-Content-Type-Opciones Cabecera Missing** |
| Descripción | El Anti-MIME-Oler cabecera X-Content-Type-Las opciones no se establece en 'NOSNIFF'. Esto permite que las versiones anteriores de Internet Explorer y Chrome para realizar MIME-olfateando en el cuerpo de la respuesta, que puede causar el cuerpo de la respuesta que se interpreta y se muestra como un tipo de contenido que no sea el tipo de contenido declarado. Corriente (principios de 2014) y heredados versiones de Firefox se utilice el tipo de contenido declarado (si se ha establecido), en lugar de realizar MIME-sniffing. |

| | |
|---|---|
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/index.shtml |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/robots.txt |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/sitemap.xml |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/ |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/index3_archivos/filelist.xml |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/index3_archivos/editdata.mso |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/index3_archivos/themedata.thmx |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/index3_archivos/colorschememapping.xml |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/index3_archivos/image003.gif |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/index3_archivos/index3_archivos/filelist.xml |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/index3_archivos/index3_archivos/editdata.mso |

| | |
|---|---|
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/index3_archivos/index3_archivos/themedata.thmx |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/index3_archivos/index3_archivos/colorschememapping.xml |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/index3_archivos/index3_archivos/image003.gif |
| Instancias | 2030 |
| Solución | Asegúrese de que el servidor de aplicaciones / web establece la cabecera Content-Type apropiadamente, y que establece la cabecera X-Content-Type-Opciones de 'NOSNIFF' para todas las páginas web.<br><br>Si es posible, asegúrese de que el usuario final utiliza un navegador web compatible con los estándares y moderno que no realiza MIME oler en absoluto, o que puede ser dirigida por el servidor de aplicaciones web / web para que no realice MIME-sniffing. |
| Otra información | Este problema todavía se aplica a páginas de error de tipo (401, 403, 500, etc.) como esas páginas a menudo todavía se ven afectados por problemas de inyección, en cuyo caso, todavía hay preocupación por los navegadores oler las páginas fuera de su tipo de contenido real.<br><br>En el umbral de "alta" este escáner no alertar sobre las respuestas de los clientes o de error del servidor. |

| | |
|---|---|
| Referencia | http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx<br><br>https://www.owasp.org/index.php/List_of_useful_HTTP_headers |
| CWE Id | dieciséis |
| Id WASC | 15 |
| **Medio bajo)** | **Divulgación IP privada** |
| Descripción | Una organización privada IP, como 10.xxx, 172.xxx, 192.168.xx se ha encontrado en el cuerpo de la respuesta HTTP. Esta información podría ser útil para otros ataques contra los sistemas internos. |

| | |
|---|---|
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/uso/usage_201812.html |
| Ataque | 190.157.8.33 |
| Evidencia | 190.157.8.33 |

| | |
|---|---|
| Instancias | 1 |
| Solución | Eliminar la dirección IP privada del cuerpo de la respuesta HTTP. Para comentarios, usar JSP / ASP comentario en lugar de comentario HTML / JavaScript que puede ser visto por los exploradores del cliente. |
| Otra información | 190.157.8.33 |

| | |
|---|---|
| Referencia | https://tools.ietf.org/html/rfc1918 |
| CWE Id | 200 |
| Id WASC | 13 |
| **Medio bajo)** | **Galleta de la bandera n HttpOnly** |
| Descripción | Una cookie se ha fijado sin el indicador HttpOnly, lo que significa que la cookie se puede acceder por JavaScript. Si un script malicioso se puede ejecutar en esta página, entonces la cookie será accesible y puede ser transmitida a otro sitio. Si se trata de una cookie de sesión a continuación, secuestro de sesión puede ser posible. |

| | |
|---|---|
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/apc-aa/filldisc.php3 |
| Parámetro | AA_d_author = OWASP PANTERA; expira = Mar 21-Feb-2017 00:14:14 GMT; path = /; domain = muisca.dian.gov.co |
| Evidencia | AA_d_author = OWASP PANTERA; expira = Mar 21-Feb-2017 00:14:14 GMT; path = /; domain = muisca.dian.gov.co |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/apc-aa/filldisc.php3 |
| Parámetro | AA_d_e_mail = OWASP PANTERA; expira = Mar 21-Feb-2017 00:14:14 GMT; path = /; domain = muisca.dian.gov.co |
| Evidencia | AA_d_e_mail = OWASP PANTERA; expira = Mar 21-Feb-2017 00:14:14 GMT; path = /; domain = muisca.dian.gov.co |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/apc-aa/filldisc.php3 |
| Parámetro | AA_d_url_address = OWASP PANTERA; expira = Mar 21-Feb-2017 00:14:14 GMT; path = /; domain = muisca.dian.gov.co |
| Evidencia | AA_d_url_address = OWASP PANTERA; expira = Mar 21-Feb-2017 00:14:14 GMT; path = /; domain = muisca.dian.gov.co |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/apc-aa/filldisc.php3 |

| | |
|---|---|
| Parámetro | AA_d_url_description = borrado; expira = Mar 24-Nov-2018 00:14:13 GMT; path = /; domain = muisca.dian.gov.co |
| Evidencia | AA_d_url_description = borrado; expira = Mar 24-Nov-2018 00:14:13 GMT; path = /; domain = muisca.dian.gov.co |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/apc-aa/filldisc.php3 |
| Parámetro | AA_d_author = OWASP PANTERA; expira = Mar 21-Feb-2017 00:14:17 GMT; path = /; domain = muisca.dian.gov.co |
| Evidencia | AA_d_author = OWASP PANTERA; expira = Mar 21-Feb-2017 00:14:17 GMT; path = /; domain = muisca.dian.gov.co |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/apc-aa/filldisc.php3 |
| Parámetro | AA_d_e_mail = OWASP PANTERA; expira = Mar 21-Feb-2017 00:14:17 GMT; path = /; domain = muisca.dian.gov.co |
| Evidencia | AA_d_e_mail = OWASP PANTERA; expira = Mar 21-Feb-2017 00:14:17 GMT; path = /; domain = muisca.dian.gov.co |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/apc-aa/filldisc.php3 |
| Parámetro | AA_d_url_address = OWASP PANTERA; expira = Mar 21-Feb-2017 00:14:17 GMT; path = /; domain = muisca.dian.gov.co |
| Evidencia | AA_d_url_address = OWASP PANTERA; expira = Mar 21-Feb-2017 00:14:17 GMT; path = /; domain = muisca.dian.gov.co |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/apc-aa/filldisc.php3 |
| Parámetro | AA_d_url_description = borrado; expira = Mar 24-Nov-2018 00:14:16 GMT; path = /; domain = muisca.dian.gov.co |
| Evidencia | AA_d_url_description = borrado; expira = Mar 24-Nov-2018 00:14:16 GMT; path = /; domain = muisca.dian.gov.co |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/apc-aa/filldisc.php3 |
| Parámetro | AA_d_author = OWASP PANTERA; expira = Mar 21-Feb-2017 00:14:18 GMT; path = /; domain = muisca.dian.gov.co |
| Evidencia | AA_d_author = OWASP PANTERA; expira = Mar 21-Feb-2017 00:14:18 GMT; path = /; domain = muisca.dian.gov.co |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/apc-aa/filldisc.php3 |
| Parámetro | AA_d_e_mail = OWASP PANTERA; expira = Mar 21-Feb-2017 00:14:18 GMT; path = /; domain = muisca.dian.gov.co |
| Evidencia | AA_d_e_mail = OWASP PANTERA; expira = Mar 21-Feb-2017 00:14:18 GMT; path = /; domain = muisca.dian.gov.co |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/apc-aa/filldisc.php3 |

| | |
|---|---|
| Parámetro | AA_d_url_address = OWASP PANTERA; expira = Mar 21-Feb-2017 00:14:18 GMT; path = /; domain = muisca.dian.gov.co |
| Evidencia | AA_d_url_address = OWASP PANTERA; expira = Mar 21-Feb-2017 00:14:18 GMT; path = /; domain = muisca.dian.gov.co |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/apc-aa/filldisc.php3 |
| Parámetro | AA_d_url_description = borrado; expira = Mar 24-Nov-2018 00:14:17 GMT; path = /; domain = muisca.dian.gov.co |
| Evidencia | AA_d_url_description = borrado; expira = Mar 24-Nov-2018 00:14:17 GMT; path = /; domain = muisca.dian.gov.co |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/apc-aa/filldisc.php3 |
| Parámetro | AA_d_author = OWASP PANTERA; expira = Mar 21-Feb-2017 00:14:19 GMT; path = /; domain = muisca.dian.gov.co |
| Evidencia | AA_d_author = OWASP PANTERA; expira = Mar 21-Feb-2017 00:14:19 GMT; path = /; domain = muisca.dian.gov.co |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/apc-aa/filldisc.php3 |
| Parámetro | AA_d_e_mail = OWASP PANTERA; expira = Mar 21-Feb-2017 00:14:19 GMT; path = /; domain = muisca.dian.gov.co |
| Evidencia | AA_d_e_mail = OWASP PANTERA; expira = Mar 21-Feb-2017 00:14:19 GMT; path = /; domain = muisca.dian.gov.co |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/apc-aa/filldisc.php3 |
| Parámetro | AA_d_url_address = OWASP PANTERA; expira = Mar 21-Feb-2017 00:14:19 GMT; path = /; domain = muisca.dian.gov.co |
| Evidencia | AA_d_url_address = OWASP PANTERA; expira = Mar 21-Feb-2017 00:14:19 GMT; path = /; domain = muisca.dian.gov.co |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/apc-aa/filldisc.php3 |
| Parámetro | AA_d_url_description = borrado; expira = Mar 24-Nov-2018 00:14:18 GMT; path = /; domain = muisca.dian.gov.co |
| Evidencia | AA_d_url_description = borrado; expira = Mar 24-Nov-2018 00:14:18 GMT; path = /; domain = muisca.dian.gov.co |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/apc-aa/filldisc.php3 |
| Parámetro | AA_d_author = OWASP PANTERA; expira = Mar 21-Feb-2017 00:14:20 GMT; path = /; domain = muisca.dian.gov.co |
| Evidencia | AA_d_author = OWASP PANTERA; expira = Mar 21-Feb-2017 00:14:20 GMT; path = /; domain = muisca.dian.gov.co |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/apc-aa/filldisc.php3 |

| | |
|---|---|
| Parámetro | AA_d_e_mail = OWASP PANTERA; expira = Mar 21-Feb-2017 00:14:20 GMT; path = /; domain = muisca.dian.gov.co |
| Evidencia | AA_d_e_mail = OWASP PANTERA; expira = Mar 21-Feb-2017 00:14:20 GMT; path = /; domain = muisca.dian.gov.co |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/apc-aa/filldisc.php3 |
| Parámetro | AA_d_url_address = OWASP PANTERA; expira = Mar 21-Feb-2017 00:14:20 GMT; path = /; domain = muisca.dian.gov.co |
| Evidencia | AA_d_url_address = OWASP PANTERA; expira = Mar 21-Feb-2017 00:14:20 GMT; path = /; domain = muisca.dian.gov.co |
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/apc-aa/filldisc.php3 |
| Parámetro | AA_d_url_description = borrado; expira = Mar 24-Nov-2018 00:14:19 GMT; path = /; domain = muisca.dian.gov.co |
| Evidencia | AA_d_url_description = borrado; expira = Mar 24-Nov-2018 00:14:19 GMT; path = /; domain = muisca.dian.gov.co |
| Instancias | 52 |
| Solución | Asegúrese de que el indicador HttpOnly se establece para todas las cookies. |
| Referencia | http://www.owasp.org/index.php/HttpOnly |
| CWE Id | dieciséis |
| Id WASC | 13 |

Fuente: El autor

Tabla N° 12 Resultado Consolidado Alertas Total Pantera

| **Nivel de riesgo** | **Número de alertas** |
|---|---|
| Alto | 0 |
| medio | 1 |
| Bajo | 4 |
| informativo | 0 |

Fuente: El autor

- Resumen de alertas

Tabla N° 13 Resultado Reporte total Pantera

| **Medium (Medio)** | **X-Frame-Opciones de cabecera no Set** |
|---|---|
| Descripción | cabecera-Opciones X-Frame no está incluido en la respuesta HTTP para protegerse de ataques 'clickjacking'. |
| Instancias | 2030 |
| Solución | La mayoría de navegadores modernos soportan la cabecera HTTP X-Frame-Options. Asegúrese de que está establecido en todas las páginas web que devuelve su sitio (si se espera que la página se enmarca únicamente por páginas de su servidor (por ejemplo, que es parte de un conjunto de marcos), entonces usted querrá usar SAMEORIGIN, de lo contrario si no esperas la página para ser enmarcado, se debe utilizar negar. PERMITIR dE-permite a los sitios web específicos para enmarcar la página web en los navegadores web compatibles). |
| Otra información | En el umbral de "alta" este escáner no alertar sobre las respuestas de los clientes o de error del servidor. |
| Referencia | http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx |
| CWE Id | dieciséis |
| Id WASC | 15 |
| **Medio bajo)** | **Navegador Web XSS protección no habilitado** |
| Descripción | Navegador Web XSS La protección no está habilitada, o está deshabilitado de la configuración del encabezado de respuesta HTTP "X-XSS-Protección 'en el servidor web |
| Instancias | 2030 |
| Solución | Asegúrese de que el filtro XSS del navegador web está activado, indicando en la cabecera de respuesta HTTP X-XSS-Protección a '1'. |
| Otra información | El encabezado de respuesta HTTP X-XSS-Protection permite al servidor Web para activar o desactivar el mecanismo de protección |

| | |
|---|---|
| | XSS del navegador web. Los siguientes valores intentarían que les permitan:<br><br>X-XSS-Protección: 1; mode = bloque<br><br>X-XSS-Protección: 1; Informe = http: //www.example.com/xss<br><br>Los siguientes valores se desactivarlo:<br><br>X-XSS-Protección: 0<br><br>El encabezado de respuesta HTTP X-XSS-Protection es compatible actualmente con Internet Explorer, Chrome y Safari (WebKit).<br><br>Tenga en cuenta que esta alerta se eleva solamente si el cuerpo de la respuesta podría potencialmente contener una carga útil XSS (con un tipo de contenido basado en texto, con una longitud distinta de cero). |

| | |
|---|---|
| Referencia | https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet<br><br>https://blog.veracode.com/2014/03/guidelines-for-setting-security-headers/ |
| CWE Id | 933 |
| Id WASC | 14 |
| **Medio bajo)** | **X-Content-Type-Opciones Cabecera Missing** |
| Descripción | El Anti-MIME-Oler cabecera X-Content-Type-Las opciones no se establece en 'NOSNIFF'. Esto permite que las versiones anteriores de Internet Explorer y Chrome para realizar MIME-olfateando en el cuerpo de la respuesta, que puede causar el cuerpo de la respuesta que se interpreta y se muestra como un tipo de contenido que no sea el tipo de contenido declarado. Corriente (principios de 2014) y heredados versiones de Firefox se utilice el tipo de contenido declarado (si se ha establecido), en lugar de realizar MIME-sniffing. |

| | |
|---|---|
| Instancias | 2030 |
| Solución | Asegúrese de que el servidor de aplicaciones / web establece la cabecera Content-Type apropiadamente, y que establece la cabecera X-Content-Type-Opciones de 'NOSNIFF' para todas las páginas web. |

| | |
|---|---|
| | Si es posible, asegúrese de que el usuario final utiliza un navegador web compatible con los estándares y moderno que no realiza MIME oler en absoluto, o que puede ser dirigida por el servidor de aplicaciones web / web para que no realice MIME-sniffing. |
| Otra información | Este problema todavía se aplica a páginas de error de tipo (401, 403, 500, etc.) como esas páginas a menudo todavía se ven afectados por problemas de inyección, en cuyo caso, todavía hay preocupación por los navegadores oler las páginas fuera de su tipo de contenido real.<br><br>En el umbral de "alta" este escáner no alertar sobre las respuestas de los clientes o de error del servidor. |

| | |
|---|---|
| Referencia | http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx<br><br>https://www.owasp.org/index.php/List_of_useful_HTTP_headers |
| CWE Id | dieciséis |
| Id WASC | 15 |
| **Medio bajo)** | **Divulgación IP privada** |
| Descripción | Una organización privada IP, como 10.xxx, 172.xxx, 192.168.xx se ha encontrado en el cuerpo de la respuesta HTTP. Esta información podría ser útil para otros ataques contra los sistemas internos. |

| | |
|---|---|
| Instancias | 1 |
| Solución | Eliminar la dirección IP privada del cuerpo de la respuesta HTTP. Para comentarios, usar JSP / ASP comentario en lugar de comentario HTML / JavaScript que puede ser visto por los exploradores del cliente. |
| Otra información | 10.2.0.58 |

| | |
|---|---|
| Referencia | https://tools.ietf.org/html/rfc1918 |
| CWE Id | 200 |
| Id WASC | 13 |
| **Medio bajo)** | **Galleta de la bandera n HttpOnly** |
| Descripción | Una cookie se ha fijado sin el indicador HttpOnly, lo que significa que la cookie se puede acceder por JavaScript. Si un script malicioso se puede ejecutar en esta página, entonces la |

| | |
|---|---|
| | cookie será accesible y puede ser transmitida a otro sitio. Si se trata de una cookie de sesión a continuación, secuestro de sesión puede ser posible. |

| | |
|---|---|
| URL | https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/apc-aa/filldisc.php3 |
| Instancias | 52 |
| Solución | Asegúrese de que el indicador HttpOnly se establece para todas las cookies. |
| Referencia | http://www.owasp.org/index.php/HttpOnly |
| CWE Id | Dieciséis |
| Id WASC | 13 |

Fuente: El autor

# 11. VULNERABILIDADES ENCONTRADAS EN EL MUISCA

A continuación, se enumerarán las vulnerabilidades y como se pudo ver en las evidencias están clasificadas en nivel medio y bajo, motivo por el cual no comprometen el riesgo mayor de fuga de información, pero es de vital importancia aplicar los controles y configuraciones de código con el fin de mitigar los ataques a la aplicación web:

- Se observa la situación de vulnerabilidad de RFI y LFI el cual conlleva cargar ficheros remotos o llamados cookies con fin de tener copia de ficheros locales en el sistema.

- Se pueden llegar a ejecutar comandos del sistema y así mostrar detalles específicos en la aplicación web.

- No se ve una implementación de una política de contraseñas segura y estricta; al observarse esta muestra un mensaje diferente al incluir usuario no permitido, el cual no garantiza el nivel de seguridad dentro de ella, en esto se puede prestar para enumerar usuarios y almacenarse en los cookies del navegador, de ello se observa como los identificadores de usuarios registrados en su momento continúan con el mismo patrón.

- Se pueden someter en un futuro en la aplicación web, ataques frecuentes que comprometan la seguridad del mismo y permitan la extracción de información confidencial con fines delictivos y beneficios propios, por tal motivo se debe estar en constante seguimiento para mitigar estos ataques.

- Se ven posibles ficheros con información vulnerables publicados en la web, los cuales pueden ser utilizados para modificación y demora en procesos de consulta dentro del mismo.

- Se puede observar varias vulnerabilidades XSS por el cual pueden ser utilizadas para comprometer a los usuarios externos y internos de la entidad.

- Al versen mensajes de error estos nos muestran información por el cual se puede utilizar con fines de ataques hacia la aplicación web.

- Se observan vulnerabilidad en los servicios el cual hacen uso de túneles cifrados; en donde el identificador de sesión, este es manejado y enviado por un canal no cifrado, por eso el acceso a esta información colaboraría a un atacante tomar posesión dentro del aplicativo web.

# 12. INFORME FINAL DE AUDITORIA

Ésta auditoría se comenzó en el mes de agosto del presente año, con la presentación de una petición formal a un especialista de la DIAN en el tema de los desarrollos de la entidad DIAN el Ingeniero Divier Riascos que a su vez delegó al Ingeniero Edwin Melgarejo Ingeniero TIC, para la coordinación y ejecución de la auditoría. De esto fue necesario la realización de un proyecto de auditaje interno donde se plasmará la auditoria con herramientas de software libre a ejecutarse dentro de la DIAN Nivel Central; en donde se especificó un cronograma de actividades previstas en un tiempo de cuatro meses aproximadamente para tal fin. Las visitas al área de fábrica de software se realizaron dos veces por semana específicamente (miércoles y jueves), y durante las dos (2) primeras semanas se recopiló información de los aplicativos asociados en el muisca, su seguimiento, estructura organizacional de la empresa, entre otros.

Durante todo éste tiempo encontramos inconvenientes con la información a solicitar por parte de ellos debido a la demora o permisos que se debían gestionar para llevarse a cabo lo propuesto; para la recopilación de ésta no fue suficiente, ni oportuna por parte del cliente. En las siguientes semanas se realizaron pruebas de aplicación con el software OWASP y muestra de resultados (pre informe).

En este punto de la auditoría, tuvimos inconvenientes por el mismo factor (tiempo), debido a todas las restricciones por el tema de seguridad que se tiene lineado en la entidad. También se estuvo en contacto con ellos para la realización de las pruebas en las fechas que estaban previsto en la planeación. En cuanto a la entrega del pre-informe, se vio la elaboración de éste no llenaba los requerimientos y expectativas de la entidad, pues el enfoque que teníamos no era el deseado por ellos.

Por lo tanto en coordinación con el ingeniero se hizo el nuevo direccionamiento de éste conllevando a cumplirse la labor; durante la semana del nuevo direccionamiento del informe nos enfatizamos mejor en el campo de la infraestructura y de la parte del desarrollo, con la verificación de la información de las auditorias o procesos de control interno en el entidad que a través de ello se realizó una evaluación más exhaustiva de la seguridad actual de la aplicación web Muisca tanto en una red pública y privada.

En la semana diecinueve (19) se confirmó la entrega del informe donde el resultado del proceso ejercido fue satisfactorio dentro de los tiempos establecidos con la DIAN.

Se tomó las fases en donde se pudo observar que hay ciertas vulnerabilidades por el cual no comprometen a mayor riesgo el sistema de información al usuario interno y externo, para esto las pruebas nos conlleva a revisar el tema de reforzamiento del código de la aplicación web y específicamente en el lenguaje JavaScript; se contextualiza el impacto que se genera por la información que se maneja dentro de ella, debido a los datos sensibles como el registro de información vital como nombres completos, números de celular, correo electrónico y la mayor cantidad de los posibles implicados.

El paso de identificar las vulnerabilidades en el aplicativo web involucrado, se reconocieron las características físicas y lógicas que permitirán más adelante recrear las evidencias encontradas más exactamente, proporcionando los detalles determinantes para el transcurso de la auditoria informática.

Las herramientas de la metodología Owasp se ha llevado a cabo por medio de investigaciones y es de total confiabilidad para obtener resultados y análisis de vulnerabilidades en este campo de la seguridad informática, en estas permiten verificar las vulnerabilidades, amenazas y a su observar toda la información concerniente a la misma que permite determinar el tipo de ataque y el modo de realizarlo.

Fue necesario disponer de cerca de varias semanas de investigación y aplicación (analizando los focos de seguridad y reconstruyendo la manera de estos ítems

en la aplicación web) para lograr establecer con claridad la secuencia de la vulnerabilidad en donde es posible que el atacante se instruya y los cuidados o controles futuros a tener en cuenta para evitar este tipo de inconvenientes.

En síntesis final el objetivo primordial era ver la situación real de la aplicación web MUISCA en cuanto al tema de seguridad dentro de la misma; sobre este se redacta en la segunda semana de diciembre cumpliendo a cabalidad con el cronograma propuesto ante la entidad, se hace certificar en este proyecto se realizó con herramientas libres de la familia OWASP.

# 13. ANÁLISIS DETALLADO

- La prueba debe arrojar la no presencia de código malicioso y en el caso de ser positiva establecer los mecanismos y los controles necesarios para evitarlo.

- Para el experto en esta rama de la seguridad informática, el principal objetivo es asegurar la aplicación web y la información que estos contienen, en donde hace parte de los mecanismos mediante los cuales se logra el aseguramiento.

- El proyecto refleja una visión más clara de la implementación de la metodología Owasp la cual brinda información valiosa para analizar y corregir detalles en las aplicaciones web.

## 14. RECURSOS DISPONIBLES

Para llevarse a cabo la elaboración de este proyecto se requiere lo siguiente:

a) Humanos

- Personal laboral de la DIAN

b) Materiales

- Papelería
- Laboratorio
- Conexión a internet

c) Técnicos

- 3 portátiles personales
- 1 disco duro Externo
- Tecnología y software

d) Financieros

# 15. PRESUPUESTO

Tabla N°14. Planeación-Gastos

| CONCEPTO | Presupuesto |
|---|---|
| Gastos de personal de proyecto | 1200000 |
| Gastos de personal temporal | 500000 |
| Gastos papelería | 120000 |
| Gastos transportes | 250000 |
| Otros gastos | 100000 |
| TOTAL, SOLICITADO | 2150000 |

Fuente: El autor

## 16. CRONOGRAMA

Tabla N°15. Diseño Cronograma

| MESES | AGOSTO | | | | SEPTIEMBRE | | | | OCTUBRE | | | | NOVIEMBRE | | | | DICIEMBRE | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **SEMANAS** | **1** | **2** | **3** | **4** | **1** | **2** | **3** | **4** | **1** | **2** | **3** | **4** | **1** | **2** | **3** | **4** | **1** | **2** | **3** | **4** |
| **Actividades** | | | | | | | | | | | | | | | | | | | | |
| Diagnóstico de la entidad | | X | X | | | | | | | | | | | | | | | | | |
| Estudio de caso y evaluación | | X | X | X | X | | | | | | | | | | | | | | | |
| Diseño de procedimientos | | | | | X | X | X | X | X | | | | | | | | | | | |
| Práctica y evidencias | | | | | | | | | X | X | X | X | | | | | | | | |
| Entregable procedimiento | | | | | | | | | | | | X | X | X | | | | | | |
| Ajuste de la propuesta | | | | | | | | | | | | | | X | X | | | | | |
| Elaboración de informe final | | | | | | | | | | | | | | | X | X | | | | |
| Presentación Final | | | | | | | | | | | | | | | | | X | X | | |

Fuente: El autor

# 17. CONCLUSIONES

- El apoyo fundamental de las partes (Dian-Auditor web) fue posible esta auditoría y ver la funcionalidad de la misma para buscar mecanismos seguros y mitigar los impactos de riesgos en la entidad.

- El análisis de vulnerabilidades es una de las fases más importantes de este proyecto, con ello se encuentran los fallos, su clasificación y ejecución de mecanismo de seguridad (refuerzo código) en la aplicación web.

- Siempre se debe tomar un plan de acción respecto a las vulnerabilidades de severidad media y alta, con el fin de mitigar de forma casi que inmediata y tener la operatividad de la aplicación web disponible.

# 18. RECOMENDACIONES

Particularizando al caso en estudio las recomendaciones generales de seguridad, es conveniente hacer énfasis en lo siguiente:

- Para aplicar la metodología Owasp se debe previamente realizar un plan de pruebas en un ambiente de trabajo local o en sitio, donde se pueda conocer el tipo de vulnerabilidad y aplicar configuraciones por el cual no afecten la funcionalidad del sistema de información web.
- Es recomendable conocer y utilizar a fondo las herramientas de software libre para los diferentes tipos de procesos de investigación.
- Los resultados de este proyecto podrán servir como base para realizar futuras auditorias en la entidad con otras aplicaciones o proyectos en curso.
- Aplicación de privilegios para permitir o restringir acceso a determinada información.
- Aplicación de políticas de grupo para garantizar el software en los equipos de la organización solo se pueda llevar a cabo por personal autorizado.
- Se buscaría implementar una auditoria interna más consecuente con el fin de garantizar que los procesos se estén cumpliendo a cabalidad.
- Aplicar políticas de seguridad estrictas con el fin de no tener ninguna extracción de parte de los atacantes para mitigar fugas de información.
- Se debe programar análisis periódico, una vez a la semana revisión de los sistemas y actualización de firmas ante nuevas amenazas y vulnerabilidades.
- Programar y planear tareas de actualización en el sistema operativo y el software de los equipos, ya que los ataques que se presentan son programas que se ingresan al equipo y este se propaga tomando las vulnerabilidades presentes.

- Se debería restringir el acceso a páginas a los usuarios de la institución.
- Informar a los usuarios internos y externos sobre las tendencias de ataques que se están presentando en la actualidad.
- Demostrar directrices de seguridad, en donde se recomiende a los administradores de aplicaciones web utilizar la herramienta Owasp, para resolver las vulnerabilidades y obtener soluciones óptimas.
- La herramienta Owasp Project es fuente principal para analizar mediante códigos de inserción y en esta ayuda hace verificar la seguridad que contiene el sistema de información web (aplicación).

# 19. DIVULGACION

Con un informe de ethical hacking desarrollado con la metodología OWASP la divulgación se hace de manera confidencial para la entidad ya que es un portal web de la entidad pública como la DIAN.

El proyecto se deja publicado en los repositorios de la UNAD para disponerla como material de consulta de cualquier estudiante.

## BIBLIOGRAFIAS


DIAZ, Raúl (junio de 2013). Proyectos de seguridad informática. Disponible en http://es.slideshare.net/raulosj/proyectos-de-seguridad-informatica

Salgado Yánez, Á. L. (2014). Análisis de las aplicaciones web de la Superintendencia de Bancos y Seguros, utilizando las recomendaciones Top Ten de OWASP para determinar los riesgos más críticos de seguridad e implementar buenas prácticas de seguridad para el desarrollo de sus aplicativos. Disponible en http://repositorio.espe.edu.ec/xmlui/bitstream/handle/21000/8245/T-ESPE-047920-R.pdf?sequence=3&isAllowed=y

Díaz, V. A. (2013). OWASP Top 10 2013: actualización de los riesgos más extendidos asociados a las aplicaciones web. Revista SIC: ciberseguridad, seguridad de la información y privacidad, (106), 92. Recuperado de https://www.isecauditors.com/sites/default/files//files/SIC106_OWASP-ISECA.pdf.

Zulueta, D. P., Ríos, M. Q., Aguilar, V. H., Gil, L., & Loro, M. F. L. Á. (2009). Procedimiento para pruebas de intrusión en aplicaciones Web – Redalyc. Disponible en http://www.redalyc.org/articulo.oa?id=92217153010

DIAZ, Raúl (junio de 2013). Proyectos de seguridad informática. Disponible en http://es.slideshare.net/raulosj/proyectos-de-seguridad-informtica

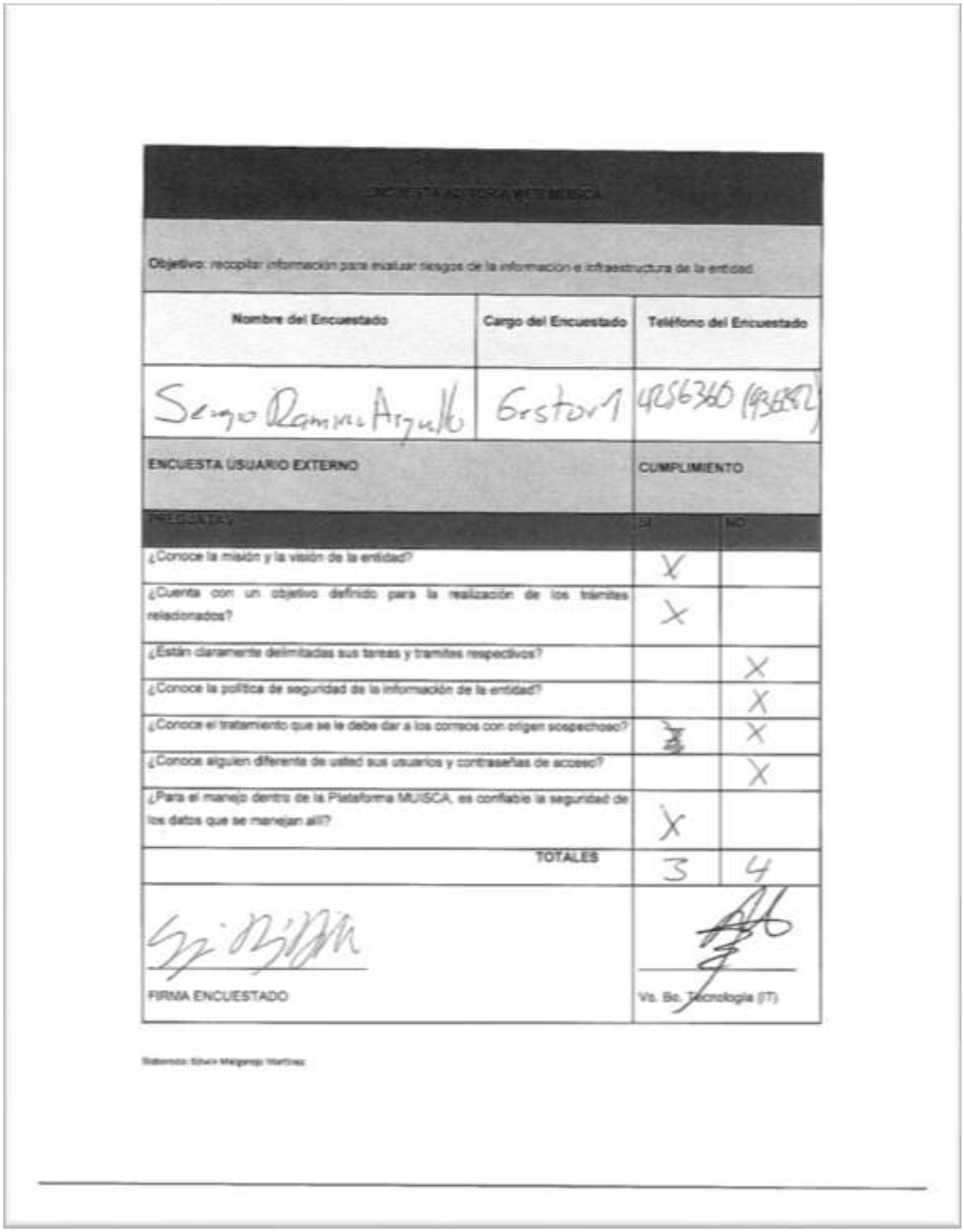
OWASP. 2008. OWASP FOUNDATION. 01 de 01 de 2008. [Citado el: 21 de 09 de 2013.] https://www.owasp.org

Consortium, Web Application Security. 2004. Web Application Security Consortium. 01 de 01 de 2004. [Citado el: 21 de 09 de 2013.] www.webappsec.org

OWASP. (2005). Una Guía para Construir Aplicaciones y Servicios Web Seguros. Recuperado el noviembre de 2016, de https://www.owasp.org/index.php/Top_10_2013-Top_10

## ANEXOS

Anexo N°1. Encuesta 1

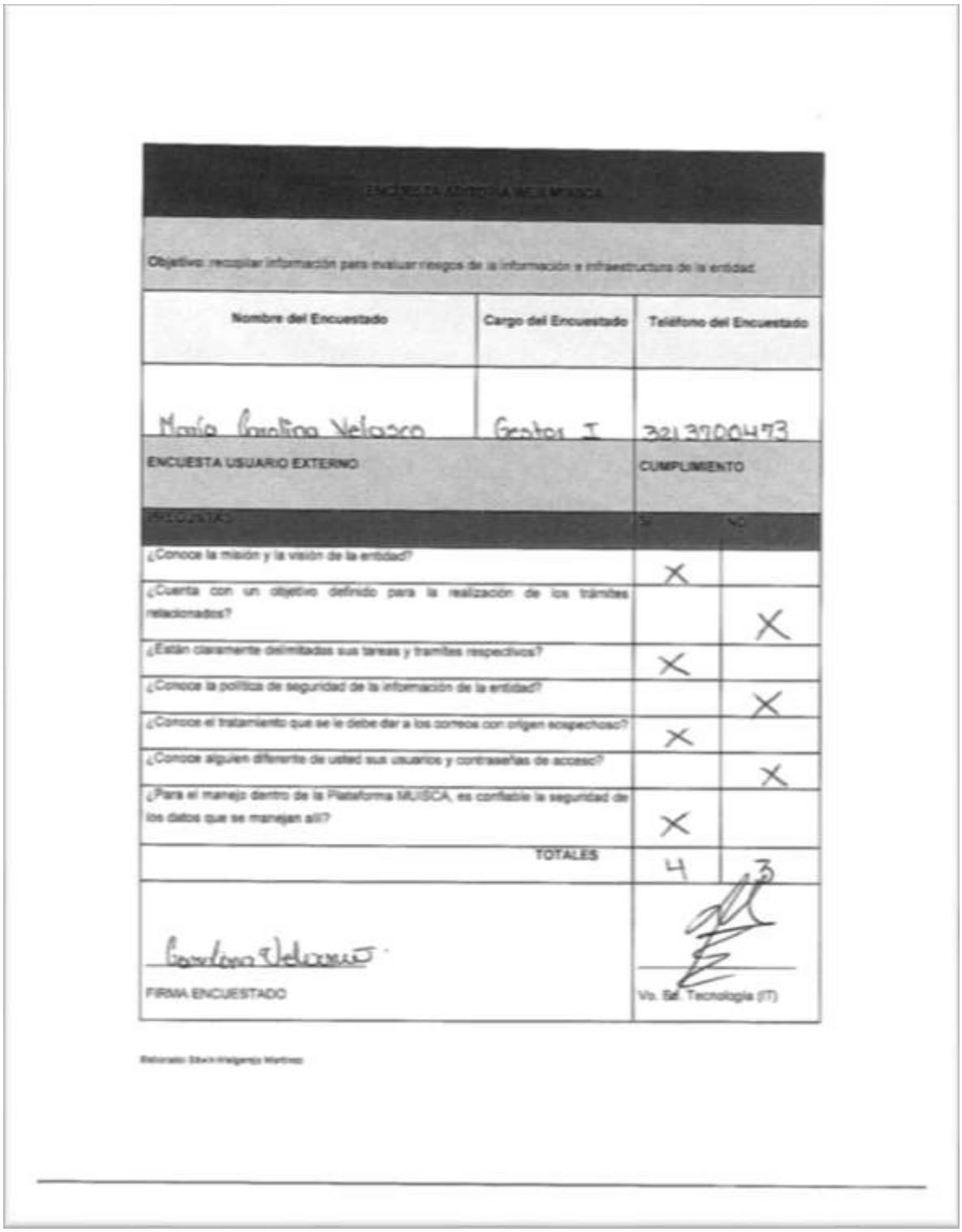


| ENCUESTA ACCESO A LA MUISCA | | |
|---|---|---|
| **Objetivo:** recopilar información para evaluar riesgos de la información e infraestructura de la entidad | | |
| **Nombre del Encuestado** | **Cargo del Encuestado** | **Teléfono del Encuestado** |
| Sergio Ramirez Arguello | Gestor 1 | 4256360 (19[illegible] |
| **ENCUESTA USUARIO EXTERNO** | | **CUMPLIMIENTO** |
| **PREGUNTAS** | **SI** | **NO** |
| ¿Conoce la misión y la visión de la entidad? | X | |
| ¿Cuenta con un objetivo definido para la realización de los trámites relacionados? | X | |
| ¿Están claramente delimitadas sus tareas y trámites respectivos? | | X |
| ¿Conoce la política de seguridad de la información de la entidad? | | X |
| ¿Conoce el tratamiento que se le debe dar a los correos con origen sospechoso? | | X |
| ¿Conoce alguien diferente de usted sus usuarios y contraseñas de acceso? | | X |
| ¿Para el manejo dentro de la Plataforma MUISCA, es confiable la seguridad de los datos que se manejan allí? | X | |
| **TOTALES** | 3 | 4 |
| FIRMA ENCUESTADO | Vo. Bo. Tecnologia (IT) | |

Elaborado: Edwin Melgarejo Martínez

Fuente. El Autor

Anexo N°2. Encuesta 2



ENCUESTA AUDITORIA MUISCA

**Objetivo:** recopilar información para evaluar riesgos de la información e infraestructura de la entidad.

| Nombre del Encuestado | Cargo del Encuestado | Teléfono del Encuestado |
|---|---|---|
| María Carolina Velasco | Gestor I | 3213700473 |

| ENCUESTA USUARIO EXTERNO | CUMPLIMIENTO | |
|---|---|---|
| ENCUESTA | SI | NO |
| ¿Conoce la misión y la visión de la entidad? | X | |
| ¿Cuenta con un objetivo definido para la realización de los trámites relacionados? | | X |
| ¿Están claramente delimitadas sus tareas y trámites respectivos? | X | |
| ¿Conoce la política de seguridad de la información de la entidad? | | X |
| ¿Conoce el tratamiento que se le debe dar a los correos con origen sospechoso? | X | |
| ¿Conoce alguien diferente de usted sus usuarios y contraseñas de acceso? | | X |
| ¿Para el manejo dentro de la Plataforma MUISCA, es confiable la seguridad de los datos que se manejan allí? | X | |
| TOTALES | 4 | 3 |

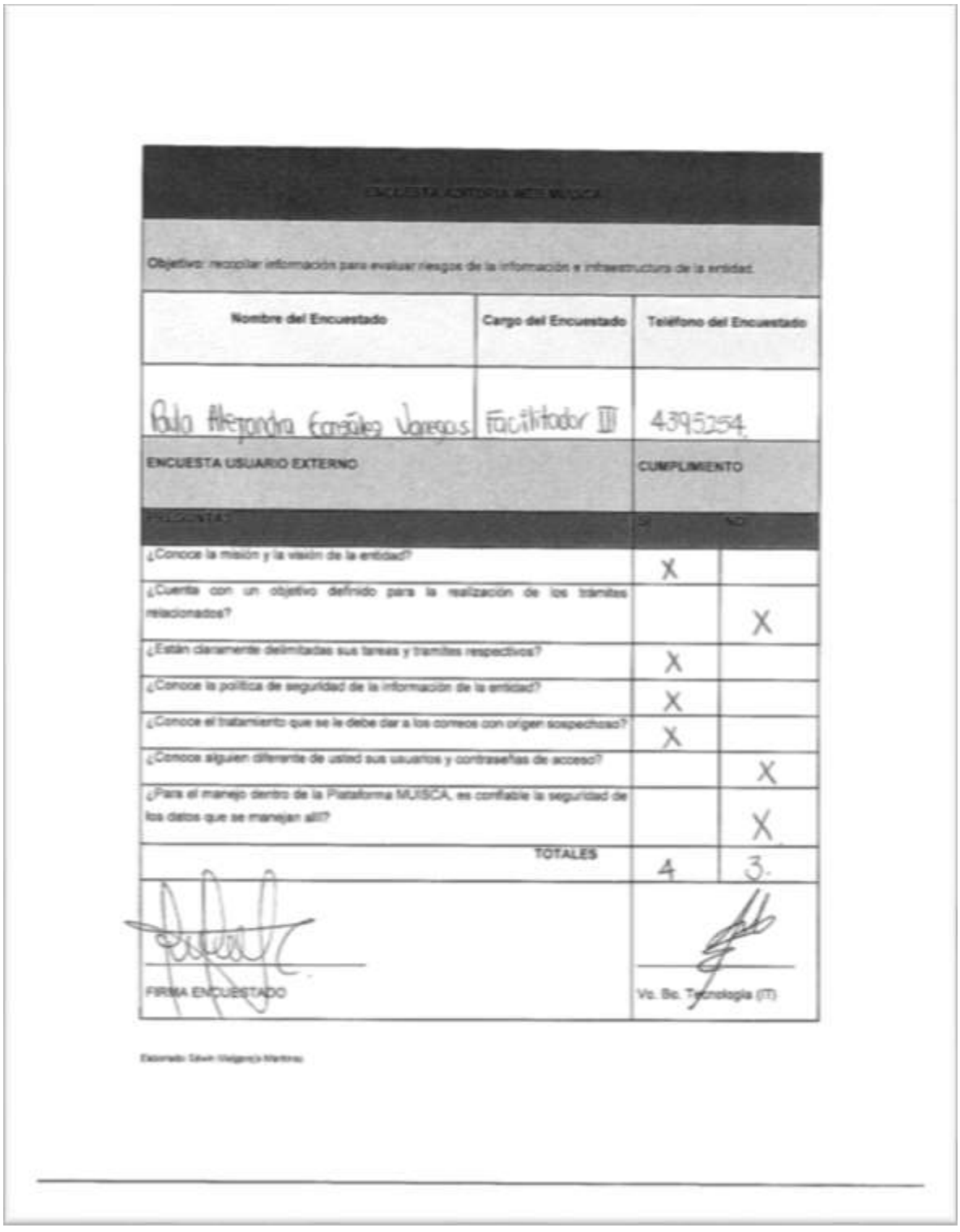
FIRMA ENCUESTADO

Vo. Bo. Tecnología (IT)

Elaborado: Edwin Holguín Martínez

Fuente. El Autor

Anexo N°3. Encuesta 3



[redacted]

Objetivo: recopilar información para evaluar riesgos de la información e infraestructura de la entidad.

| Nombre del Encuestado | Cargo del Encuestado | Teléfono del Encuestado |
|---|---|---|
| Paula Alejandra González Vanegas | Facilitador III | 4395254 |

| ENCUESTA USUARIO EXTERNO | CUMPLIMIENTO | |
|---|---|---|
| PREGUNTAS | SI | NO |
| ¿Conoce la misión y la visión de la entidad? | X | |
| ¿Cuenta con un objetivo definido para la realización de los trámites relacionados? | | X |
| ¿Están claramente delimitadas sus tareas y trámites respectivos? | X | |
| ¿Conoce la política de seguridad de la información de la entidad? | X | |
| ¿Conoce el tratamiento que se le debe dar a los correos con origen sospechoso? | X | |
| ¿Conoce alguien diferente de usted sus usuarios y contraseñas de acceso? | | X |
| ¿Para el manejo dentro de la Plataforma MUISCA, es confiable la seguridad de los datos que se manejan allí? | | X |
| TOTALES | 4 | 3 |

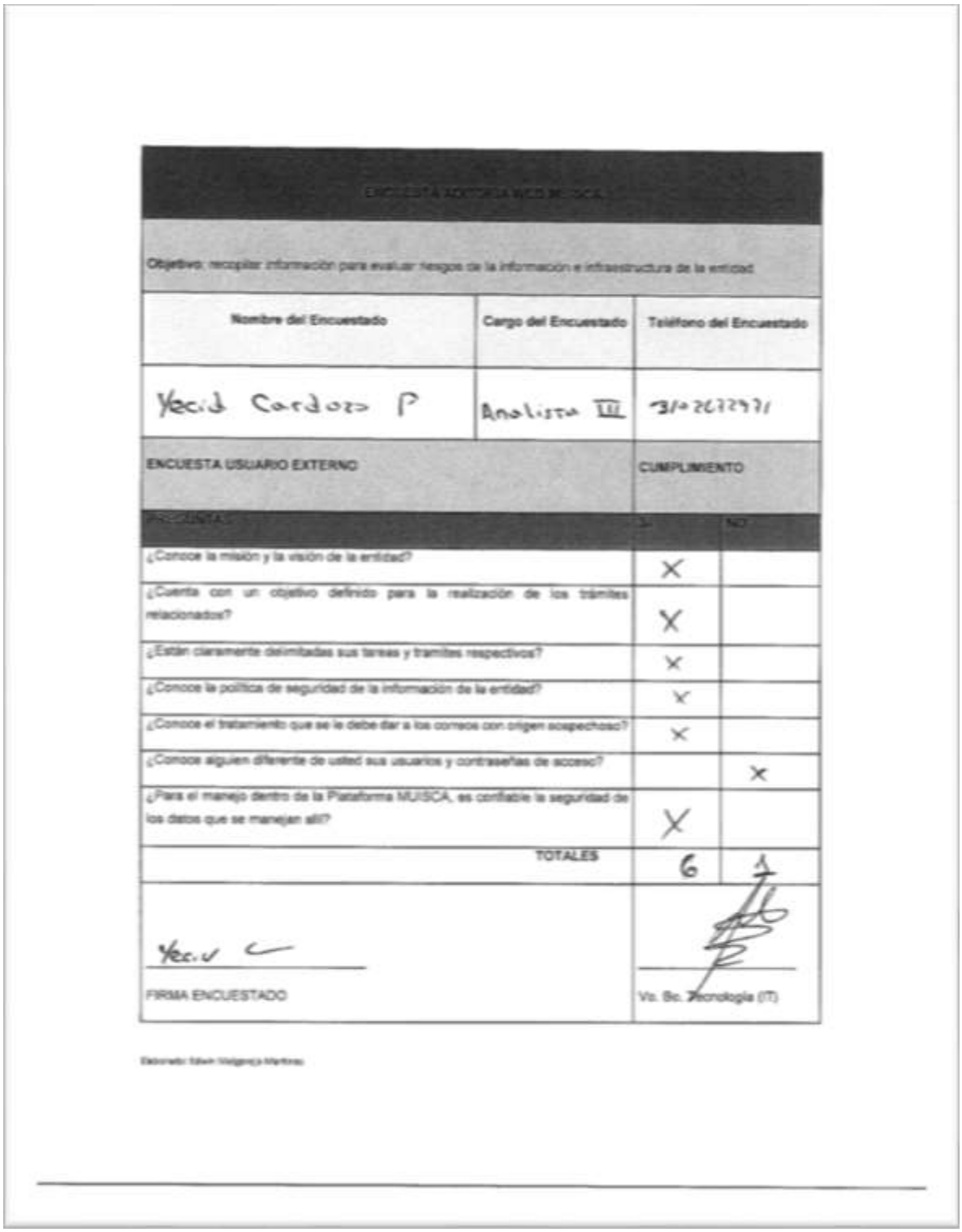
FIRMA ENCUESTADO

Vo. Bo. Tecnología (IT)

Elaborado: [redacted]

Fuente. El Autor

Anexo N°4. Encuesta 4



ENCUESTA AUDITORIA MUISCA

**Objetivo:** recopilar información para evaluar riesgos de la información e infraestructura de la entidad

| Nombre del Encuestado | Cargo del Encuestado | Teléfono del Encuestado |
|---|---|---|
| Yecid Cardozo P | Analista III | 3102672971 |

| ENCUESTA USUARIO EXTERNO | CUMPLIMIENTO | |
|---|---|---|
| PREGUNTAS | SI | NO |
| ¿Conoce la misión y la visión de la entidad? | X | |
| ¿Cuenta con un objetivo definido para la realización de los trámites relacionados? | X | |
| ¿Están claramente delimitadas sus tareas y tramites respectivos? | X | |
| ¿Conoce la política de seguridad de la información de la entidad? | X | |
| ¿Conoce el tratamiento que se le debe dar a los correos con origen sospechoso? | X | |
| ¿Conoce alguien diferente de usted sus usuarios y contraseñas de acceso? | | X |
| ¿Para el manejo dentro de la Plataforma MUISCA, es confiable la seguridad de los datos que se manejan allí? | X | |
| TOTALES | 6 | 1 |

Yecid C

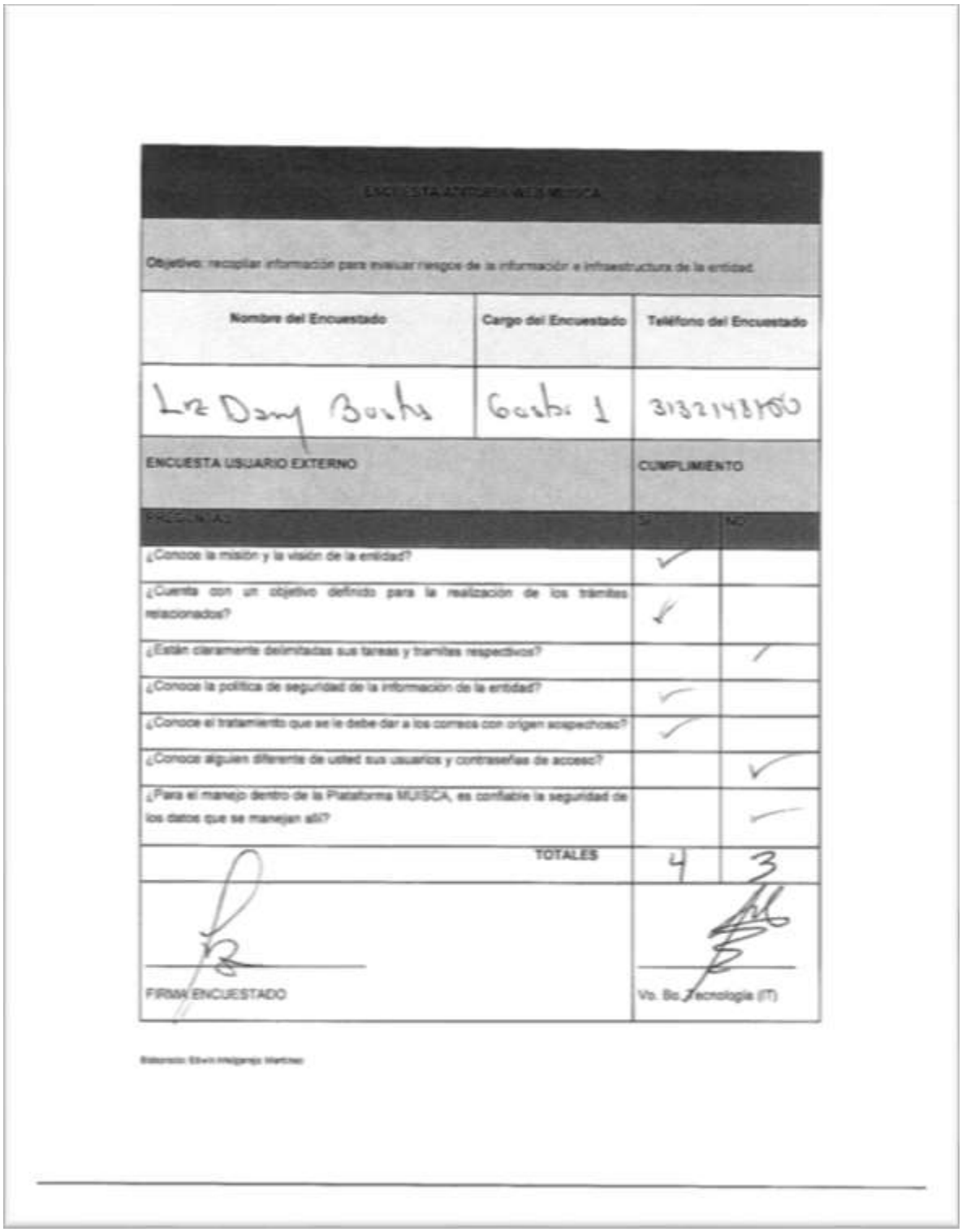
FIRMA ENCUESTADO

Vo. Bo. Tecnología (IT)

Elaborado: Edwin Vasquez Martinez

Fuente. El Autor

Anexo N°5. Encuesta 5



ENCUESTA ATENCIÓN MESA MUISCA

Objetivo: recopilar información para evaluar riesgos de la información e infraestructura de la entidad

| Nombre del Encuestado | Cargo del Encuestado | Teléfono del Encuestado |
|---|---|---|
| Liz Dany Bonilla | Gestor 1 | 3132148700 |

| ENCUESTA USUARIO EXTERNO | CUMPLIMIENTO | |
|---|---|---|
| PREGUNTAS | SI | NO |
| ¿Conoce la misión y la visión de la entidad? | ✓ | |
| ¿Cuenta con un objetivo definido para la realización de los trámites relacionados? | ✓ | |
| ¿Están claramente delimitadas sus tareas y trámites respectivos? | | ✓ |
| ¿Conoce la política de seguridad de la información de la entidad? | ✓ | |
| ¿Conoce el tratamiento que se le debe dar a los correos con origen sospechoso? | ✓ | |
| ¿Conoce alguien diferente de usted sus usuarios y contraseñas de acceso? | | ✓ |
| ¿Para el manejo dentro de la Plataforma MUISCA, es confiable la seguridad de los datos que se manejan allí? | | ✓ |
| TOTALES | 4 | 3 |

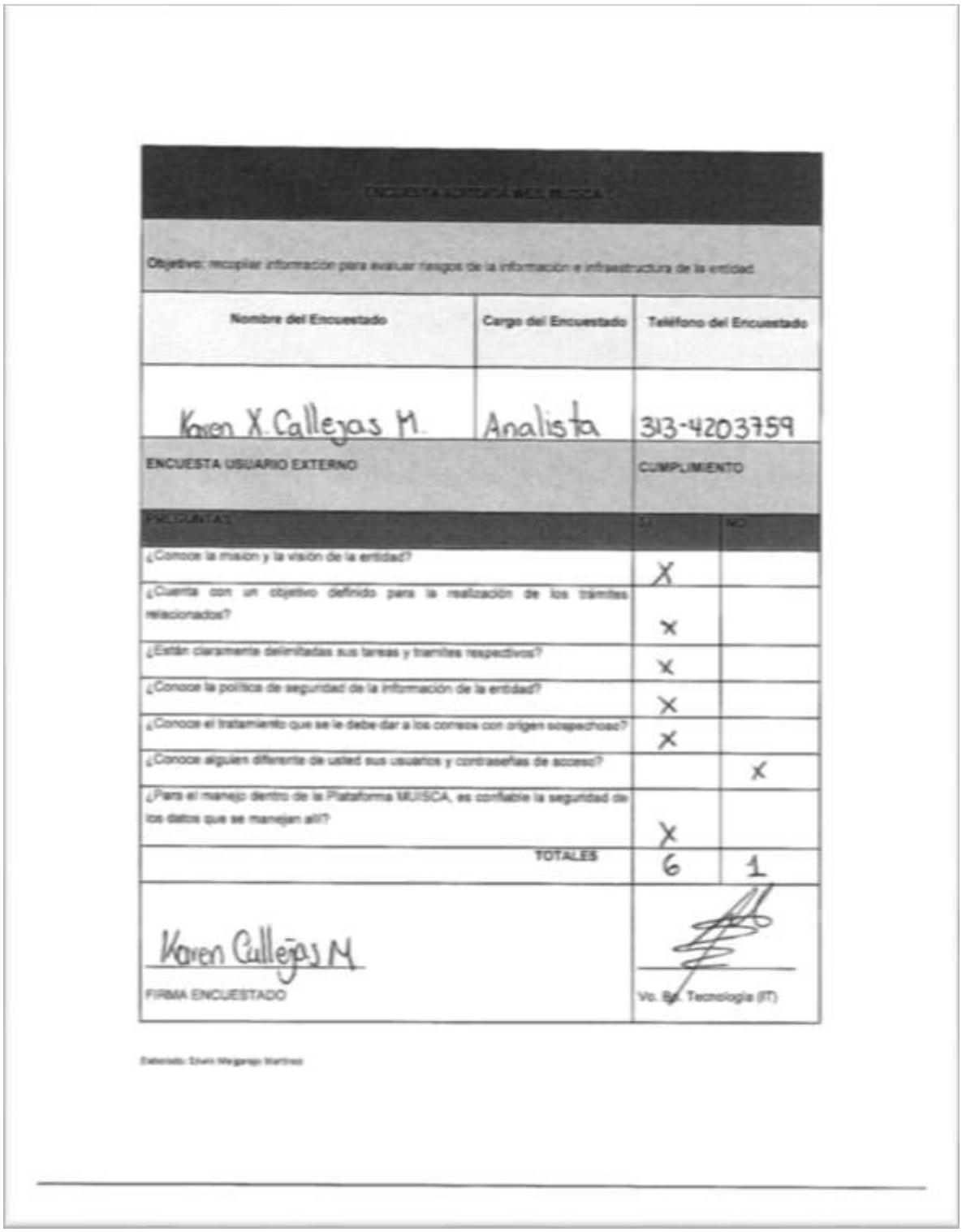
FIRMA ENCUESTADO

Vo. Bo. Tecnología (IT)

Elaborado: Edwin Melgarejo Martínez

Fuente. El Autor

Anexo N°6. Encuesta 6



ENCUESTA AUDITORIA MUISCA

**Objetivo:** recopilar información para evaluar riesgos de la información e infraestructura de la entidad

| Nombre del Encuestado | Cargo del Encuestado | Teléfono del Encuestado |
|---|---|---|
| Karen X. Callejas M. | Analista | 313-4203759 |

| ENCUESTA USUARIO EXTERNO | CUMPLIMIENTO | |
|---|---|---|
| PREGUNTAS | SI | NO |
| ¿Conoce la misión y la visión de la entidad? | X | |
| ¿Cuenta con un objetivo definido para la realización de los trámites relacionados? | X | |
| ¿Están claramente delimitadas sus tareas y trámites respectivos? | X | |
| ¿Conoce la política de seguridad de la información de la entidad? | X | |
| ¿Conoce el tratamiento que se le debe dar a los correos con origen sospechoso? | X | |
| ¿Conoce alguien diferente de usted sus usuarios y contraseñas de acceso? | | X |
| ¿Para el manejo dentro de la Plataforma MUISCA, es confiable la seguridad de los datos que se manejan allí? | X | |
| TOTALES | 6 | 1 |

Karen Callejas M

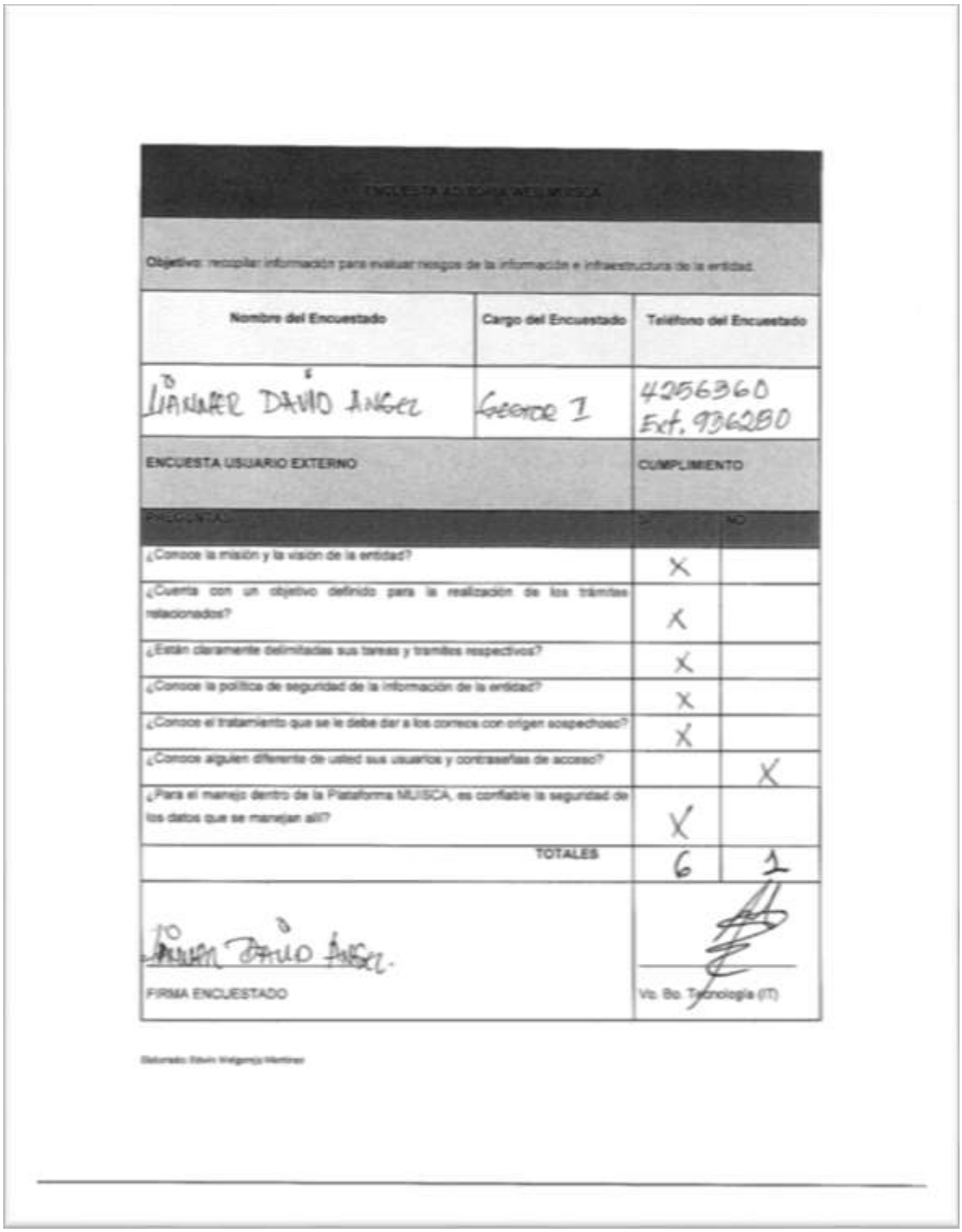
FIRMA ENCUESTADO

Vo. Bo. Tecnología (IT)

Elaborado: Edwin Mejiagrejo Martínez

Fuente. El Autor

Anexo N°7. Encuesta 7



ENCUESTA ACEPTACIÓN MUISCA

Objetivo: recopilar información para evaluar riesgos de la información e infraestructura de la entidad.

| Nombre del Encuestado | Cargo del Encuestado | Teléfono del Encuestado |
|---|---|---|
| LIANNER DAVID ANGEL | GERENTE I | 4256360 Ext. 936280 |

| ENCUESTA USUARIO EXTERNO | CUMPLIMIENTO | |
|---|---|---|
| PREGUNTAS | SI | NO |
| ¿Conoce la misión y la visión de la entidad? | X | |
| ¿Cuenta con un objetivo definido para la realización de los trámites relacionados? | X | |
| ¿Están claramente delimitadas sus tareas y trámites respectivos? | X | |
| ¿Conoce la política de seguridad de la información de la entidad? | X | |
| ¿Conoce el tratamiento que se le debe dar a los correos con origen sospechoso? | X | |
| ¿Conoces alguien diferente de usted sus usuarios y contraseñas de acceso? | | X |
| ¿Para el manejo dentro de la Plataforma MUISCA, es confiable la seguridad de los datos que se manejan allí? | X | |
| TOTALES | 6 | 1 |

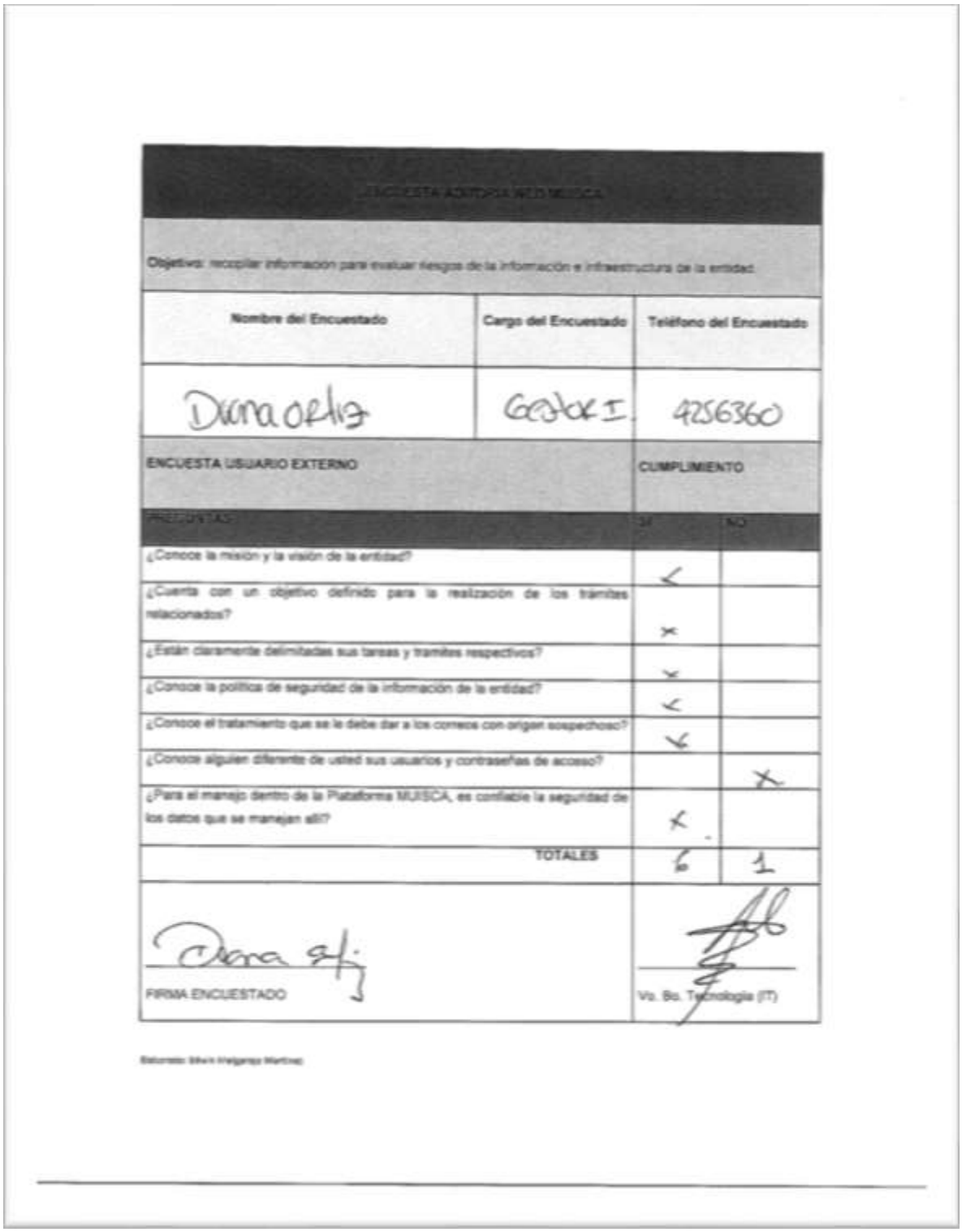
FIRMA ENCUESTADO

Vo. Bo. Tecnología (IT)

Elaborado: Edwin Holguín Martínez

Fuente. El Autor

Anexo N°8. Encuesta 8



ENCUESTA ADOPCIÓN MUISCA

Objetivo: recopilar información para evaluar riesgos de la información e infraestructura de la entidad.

| Nombre del Encuestado | Cargo del Encuestado | Teléfono del Encuestado |
|---|---|---|
| Diana Ortiz | Gestor I. | 4256360 |

| ENCUESTA USUARIO EXTERNO | CUMPLIMIENTO | |
|---|---|---|
| PREGUNTAS | SI | NO |
| ¿Conoce la misión y la visión de la entidad? | ✓ | |
| ¿Cuenta con un objetivo definido para la realización de los trámites relacionados? | x | |
| ¿Están claramente delimitadas sus tareas y trámites respectivos? | ✓ | |
| ¿Conoce la política de seguridad de la información de la entidad? | ✓ | |
| ¿Conoce el tratamiento que se le debe dar a los correos con origen sospechoso? | ✓ | |
| ¿Conoce alguien diferente de usted sus usuarios y contraseñas de acceso? | | x |
| ¿Para el manejo dentro de la Plataforma MUISCA, es confiable la seguridad de los datos que se manejan allí? | x | |
| TOTALES | 6 | 1 |

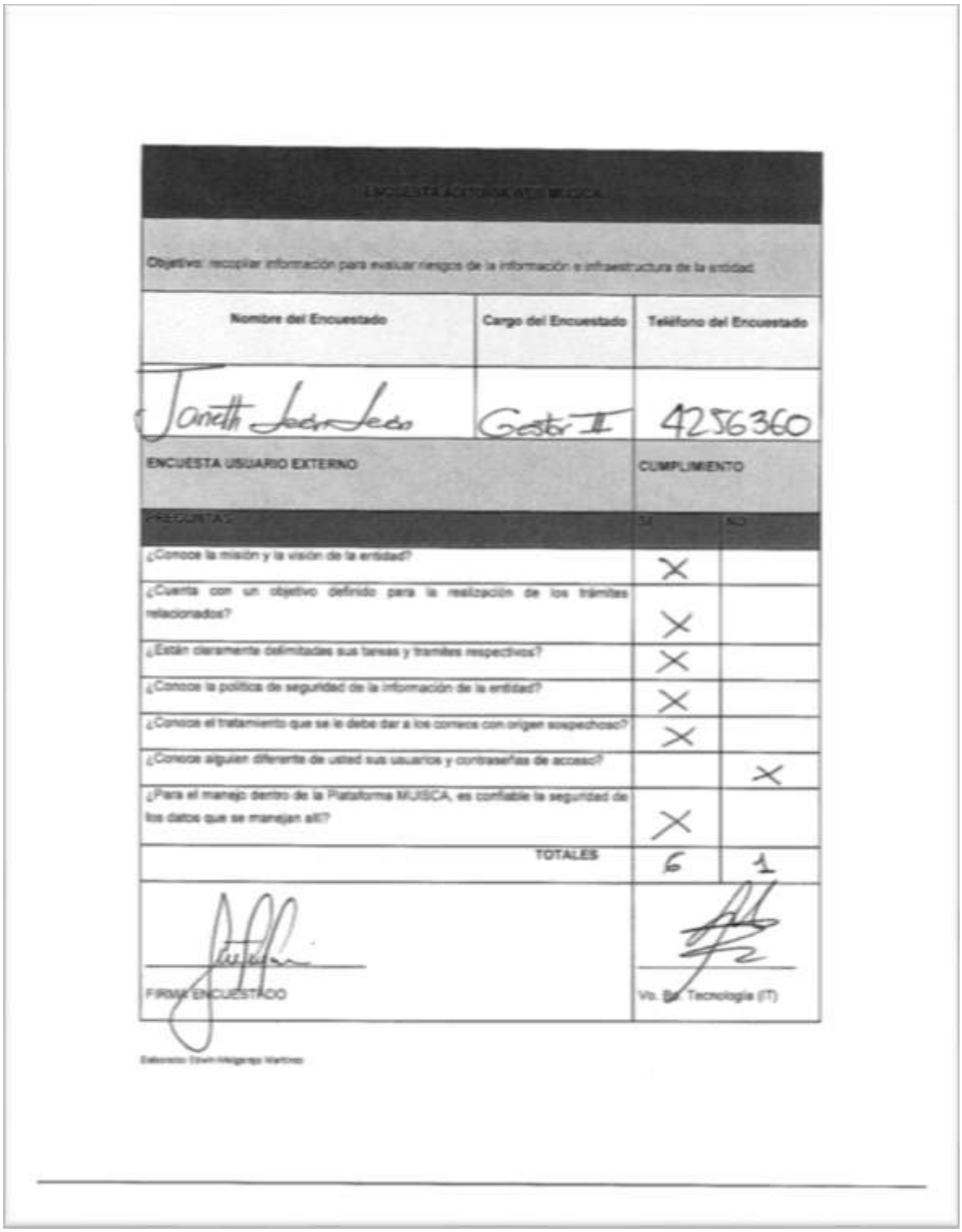
Diana Ortiz
FIRMA ENCUESTADO

Vo. Bo. Tecnología (IT)

Elaborado: Silvia Holguera Martínez

Fuente. El Autor

Anexo N°9. Encuesta 9

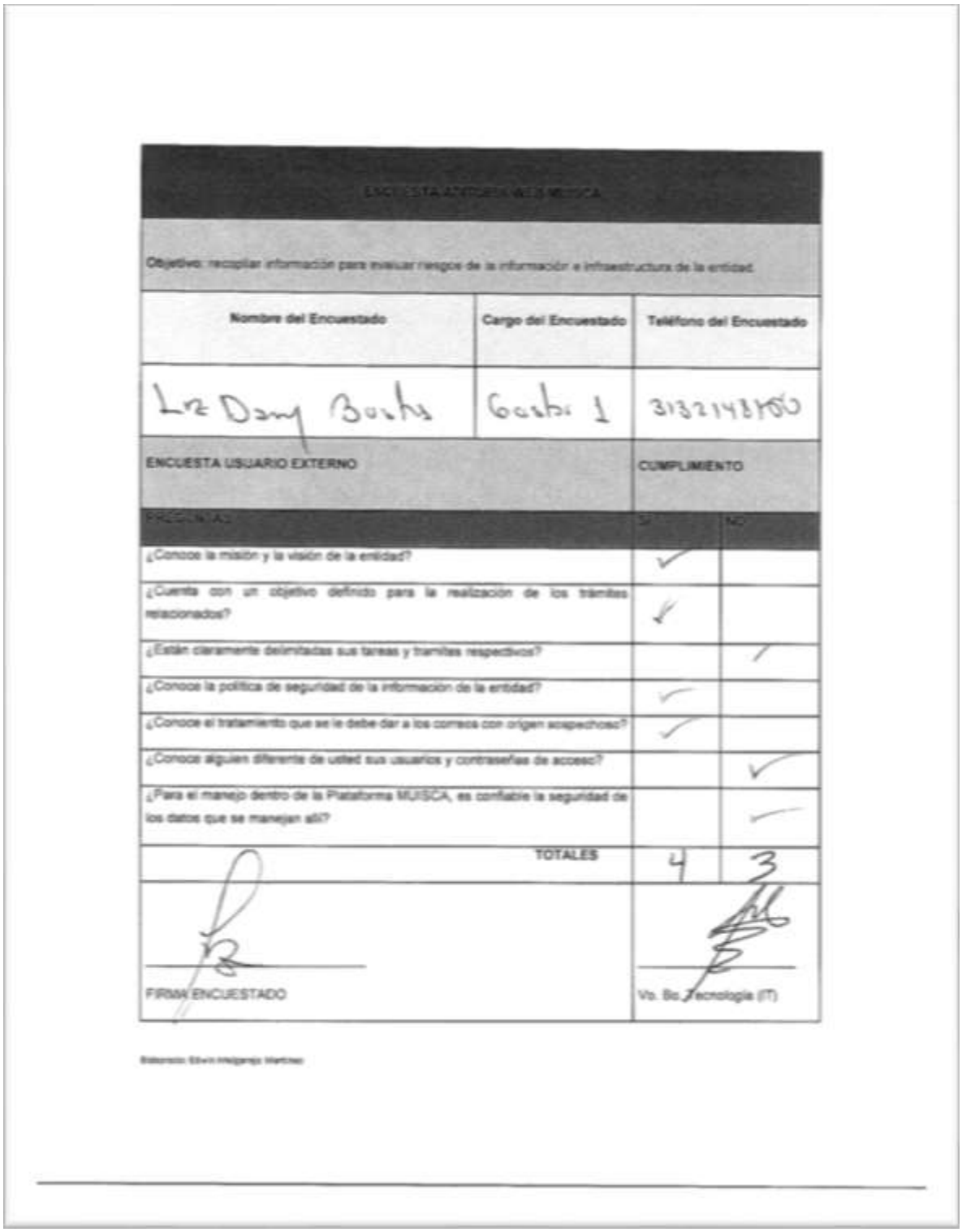


| [redacted] | |
|---|---|
| **Objetivo:** recopilar información para evaluar riesgos de la información e infraestructura de la entidad | |
| **Nombre del Encuestado** | **Cargo del Encuestado** | **Teléfono del Encuestado** |
| Janeth Jaramillo | Gestor II | 4256360 |
| **ENCUESTA USUARIO EXTERNO** | **CUMPLIMIENTO** | |
| **PREGUNTAS** | **SI** | **NO** |
| ¿Conoce la misión y la visión de la entidad? | X | |
| ¿Cuenta con un objetivo definido para la realización de los trámites relacionados? | X | |
| ¿Están claramente delimitadas sus tareas y trámites respectivos? | X | |
| ¿Conoce la política de seguridad de la información de la entidad? | X | |
| ¿Conoce el tratamiento que se le debe dar a los correos con origen sospechoso? | X | |
| ¿Conoce alguien diferente de usted sus usuarios y contraseñas de acceso? | | X |
| ¿Para el manejo dentro de la Plataforma MUISCA, es confiable la seguridad de los datos que se manejan allí? | X | |
| **TOTALES** | 6 | 1 |
| FIRMA ENCUESTADO | Vo. Bo. Tecnología (IT) | |

Elaborado: Edwin Melgarejo Martínez

Fuente. El Autor

Anexo N°10. Encuesta 10



| ENCUESTA ANTIGUEDAD MUISCA | | |
|---|---|---|
| Objetivo: recopilar información para evaluar riesgos de la información e infraestructura de la entidad | | |
| **Nombre del Encuestado** | **Cargo del Encuestado** | **Teléfono del Encuestado** |
| Lic Dany Bonilla | Gestor 1 | 3132148[illegible] |
| **ENCUESTA USUARIO EXTERNO** | | **CUMPLIMIENTO** |
| PREGUNTAS | | SI / NO |
| ¿Conoce la misión y la visión de la entidad? | ✓ | |
| ¿Cuenta con un objetivo definido para la realización de los trámites relacionados? | ✓ | |
| ¿Están claramente delimitadas sus tareas y tramites respectivos? | | ✓ |
| ¿Conoce la política de seguridad de la información de la entidad? | ✓ | |
| ¿Conoce el tratamiento que se le debe dar a los correos con origen sospechoso? | ✓ | |
| ¿Conoce alguien diferente de usted sus usuarios y contraseñas de acceso? | | ✓ |
| ¿Para el manejo dentro de la Plataforma MUISCA, es confiable la seguridad de los datos que se manejan allí? | | ✓ |
| TOTALES | 4 | 3 |
| FIRMA ENCUESTADO | Vo. Bo. Tecnología (IT) | |

Elaborado: Edwin Melgarejo Martinez

Fuente. El Autor

Anexo Nº 11. RAE

| | |
|---|---|
| **Título de Documento.** | Desarrollo de una auditoría a la aplicación web muisca basado en herramientas de software libre del proyecto Owasp en la entidad DIAN. |
| **Autor** | MELGAREJO MARTINEZ, Edwin |
| **Palabras Claves** | Guía Owasp, auditoria, aplicación web, Muisca, herramientas de análisis, vulnerabilidades, recomendaciones |
| **Descripción**<br><br>El presente trabajo de grado hace referencia a una auditoria informática con herramientas de software libre en la entidad DIAN, más específicamente en la aplicación web Muisca donde los usuarios tanto internos como externos realizan sus trámites relacionados con el tema de actualización de RUT, contestaciones de PQRS, elaboración y diligenciamiento de declaraciones de renta entre otros como de figura personal y/o jurídica, razón por la cual se maneja información sensible; se busca realizar este proceso con el fin de obtener resultados para observar el nivel de seguridad y aportar recomendaciones para mejorar las medidas de seguridad y protección de los activos más relevantes de la aplicación web. | |
| **Fuentes Bibliográficas** | DIAZ, Raúl (junio de 2013). Proyectos de seguridad informática. Disponible en http://es.slideshare.net/raulosj/proyectos-de-seguridad-informtica<br><br>Salgado Yánez, Á. L. (2014). Análisis de las aplicaciones web de la Superintendencia de Bancos y Seguros, utilizando las recomendaciones Top Ten de OWASP para determinar los riesgos más críticos de seguridad e implementar buenas prácticas de seguridad para el desarrollo de sus aplicativos (Doctoral dissertation, Universidad de las Fuerzas Armadas ESPE. Carrera de Ingeniería de Sistemas e Informática.). |

(www.mty.itsem.mx/externos/alaic/texto1html)

Díaz, V. A. (2013). OWASP Top 10 2013: actualización de los riesgos más extendidos asociados a las aplicaciones web. Revista SIC: ciberseguridad, seguridad de la información y privacidad, (106), 92

Zulueta, D. P., Ríos, M. Q., Aguilar, V. H., Gil, L., & Loro, M. F. L. Á. (2009). Procedimiento para pruebas de intrusión en aplicaciones Web. Innovación, Calidad e Ingeniería del Software, 5(2), 70.

Peña Torres, I. (2016). Auditoría Técnica de Seguridad de aplicaciones web (Master's thesis, Universitat Oberta de Catalunya).

**Contenido**

Los avances tecnológicos actuales y las aplicaciones web han tenido mayor presencia en el tema de la informática, estos se han convertido en activo importante para las compañías, dichos avances tienen la peculiaridad de ser utilizados para beneficio o perjuicio de las empresas, por lo tanto cuando se utiliza una herramienta de este calibre(optima seguridad) debe ser salvaguardada de una manera especial; pues tiene como finalidad revisar la seguridad en un aplicativo y observar el nivel aceptabilidad para que el personal de infraestructura y seguridad de la entidad vean su funcionalidad y así respeten sus principios, algunos de estos son, la confidencialidad, la integridad y por último la disponibilidad de la información con la cual se trabaja actualmente.

Es por ello que se propone desarrollar una auditoria a la aplicación web MUISCA en la DIAN, utilizando las metodologías OWASP de software libre en donde se busca indicar los procedimientos, técnicas y herramientas; esta nos ayudara a verificar la forma de auditar una aplicación Web, con el propósito de evidenciar la realización en el sistema de información seleccionado en este caso y a su vez realizar el informe final donde se centre las vulnerabilidades encontradas y las recomendaciones finales para el reforzamiento y estabilidad de la aplicación web.

Con este desarrollo, el proyecto, en primera instancia se centraliza en

ver el impacto de la actualización con los riesgos que se presentan ante los ataques a las aplicaciones web y ver los focos de seguridad que hay dentro de ellas. A raíz de esto se hace la evaluación a temas de auditorías realizadas anteriormente, y con este insumo se procede a realizar las pruebas pertinentes con las autorizaciones debidas por la entidad, con la investigación de la metodología Owasp se procede a revisar los diferentes procedimientos que nos permite analizar los resultados obtenidos para así reducir los riesgos de pérdida y corrupción de la información, también mantener un conjunto estructurado que permita definir el tratamiento que se le dará a las vulnerabilidades encontradas; el mejoramiento del nivel de seguridad de la red y con ello indicar una buena práctica para sugerir recomendaciones finales.

El proyecto va encaminado a ver la realidad del funcionamiento de la aplicación web y de la conservación de la información que maneja el muisca, el factor de seguridad y la oportunidad que tiene el cliente final al ver sus operaciones con datos verídicos y seguros.

**Metodología**

En este caso de investigación se enfatizará en detallar el paso a paso de la auditoria con la guía de proyecto OWASP para las aplicaciones web seguras en la entidad DIAN, también se realizarán todos los elementos importantes y comprendidos en una auditoria de este tipo.
Se aplicara la metodología OWASP que consiste en la investigación de la herramienta , su finalidad y la estabilidad para dar resultados que contribuyan a obtener aplicaciones web seguras y definidas en este entorno, después de ello, con la máquina virtual se hará el respectivo montaje del software y se realizara el estudio y pruebas requeridas , con este resultado se plasmaran las evidencias que sirven de punto de partida para la evaluación de las vulnerabilidades y las acciones a tomar , para luego ser documentados y especificados en el proyecto con la finalidad de aportar las recomendaciones, las cuales son un factor importante para la toma de decisiones y las mejoras respectivas para garantizar la protección de los datos y que estas a su vez conlleven a la entidad a tomar las decisiones necesarias, para que posteriormente tengan la autonomía de aplicar los desarrollos tecnológicos en los momentos donde se quieran dar a nuevas implementaciones o aplicaciones web que vallan a la vanguardia de la tecnología.

**Conclusiones**

La importancia de realizar estas auditorías refleja el estado actual de las aplicaciones web en materia de seguridad y ayuda a mitigar los

riesgos que se puedan presentar.

La metodología Owasp es en la actualidad una de los más confiables y seguras para reducir los riesgos de pérdida y corrupción de la información.

La aplicación de esta rama de la informática enriquece el quehacer profesional, pues fortalece las capacidades cognitivas y prácticas que desembocan en una visión más clara y por ende en una aplicabilidad valerosa para la entidad en la que se desarrolle esta labor.

**Recomendaciones.**

Tomando las recomendaciones generales del proyecto de seguridad, es conveniente hacer énfasis en lo siguiente:

- Aplicación de privilegios para permitir o restringir acceso a determinada información.

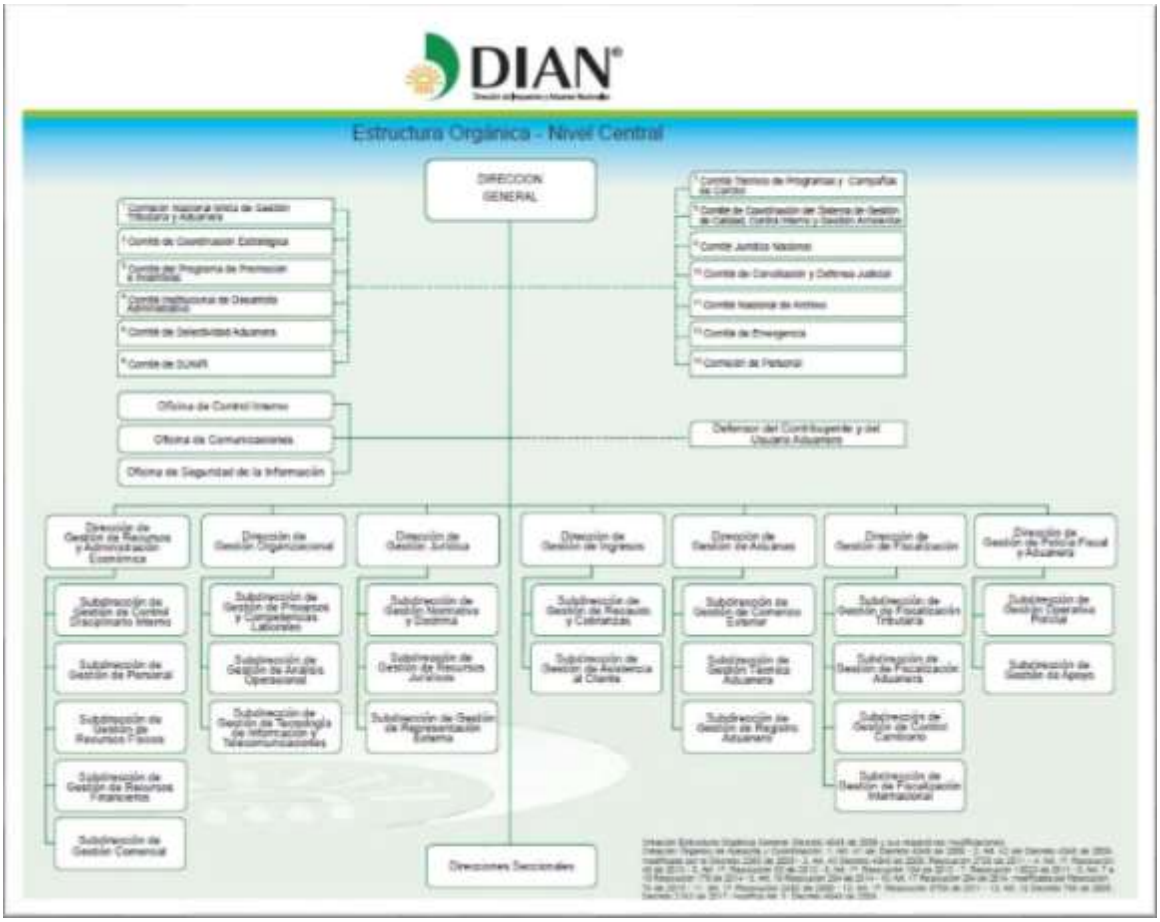
- Constante capacitación a los usuarios tanto internos y externos haciendo énfasis en consejos y buenas prácticas de seguridad de la información.

- Implementar una auditoria interna eficiente con el fin de garantizar que los procesos se estén cumpliendo a cabalidad.

- Aplicar políticas de seguridad estrictas con el fin de no tener ninguna extracción de parte de los atacantes para mitigar fugas de información.

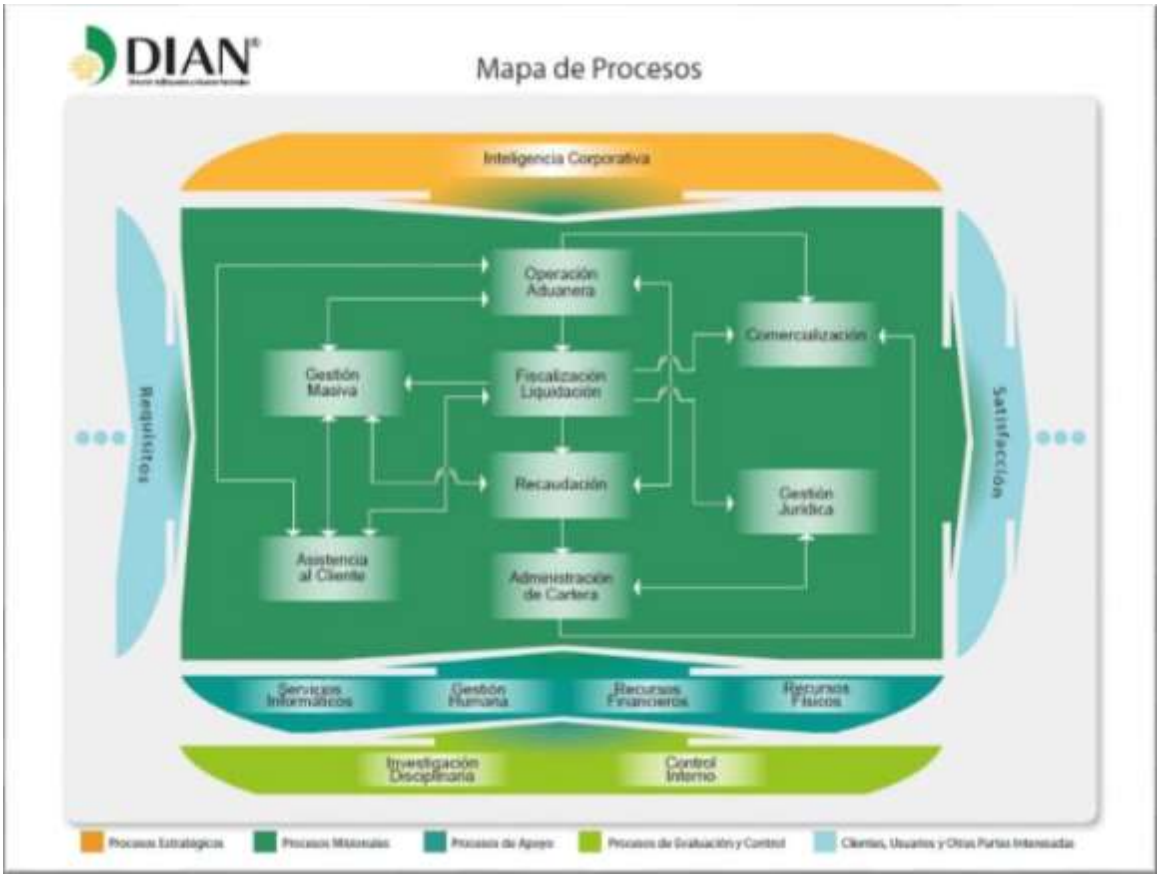
Fuente. El Autor

Anexo Nº 12. Organigrama



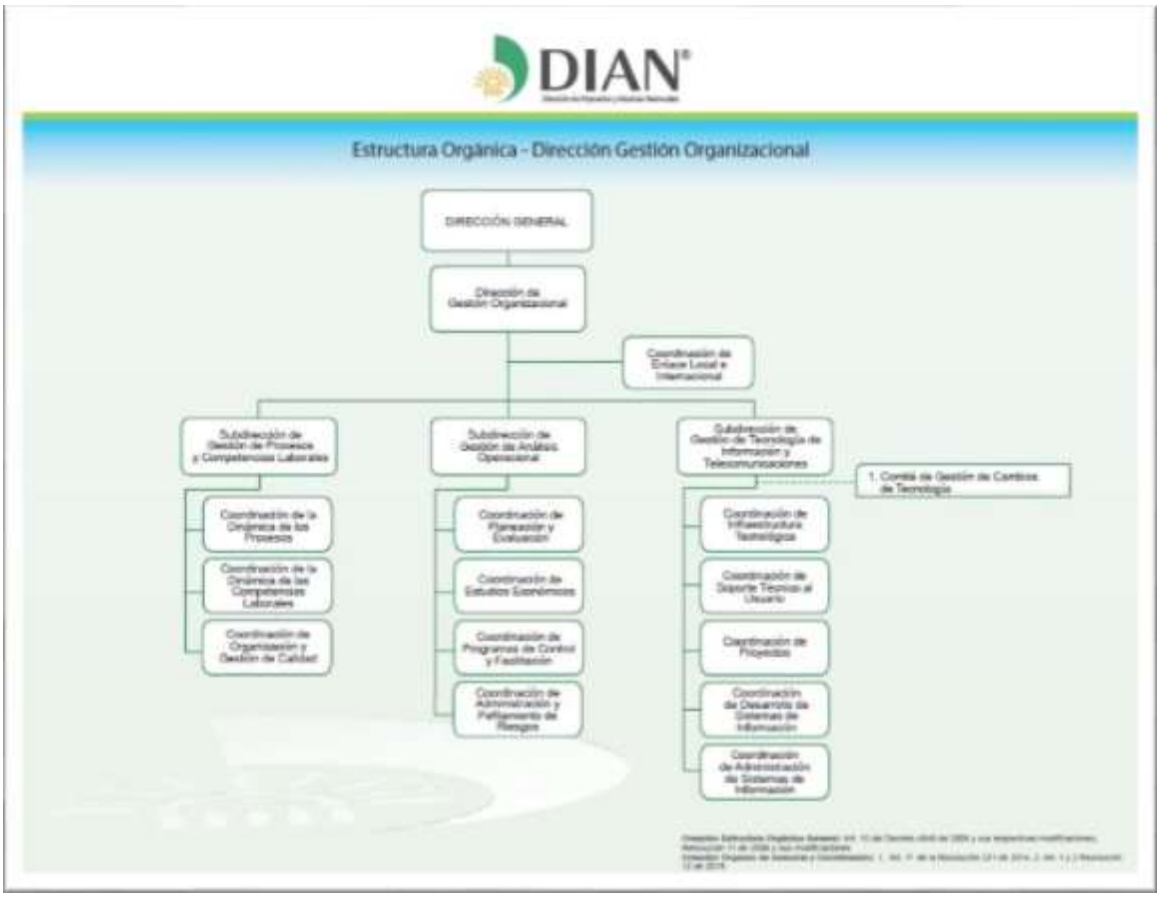

Fuente. https://www.diannet.dian.gov.co/mapas

Anexo Nº 13. Mapa Procesos




Fuente. https://www.diannet.dian.gov.co/mapas

Anexo Nº 14. Mapa Gestión Organizacional




Fuente. https://www.diannet.dian.gov.co/mapas

Anexo Nº 15. Relación de entrada GET

```
# owasp pantera https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces --color --output wapiti.html --format
html

OWASP Pantera-2.3.0 (pantera.sourceforge.net)

Note

========

Este escaneo se ha guardado en el archivo /root/.pantera/scans/www.shopathome.com.xml

Puedes usarlo para realizar ataques sin escanear de nuevo el website mediante el

parametro "-k"

[*] Cargando modulos:

mod_crlf, mod_exec, mod_file, mod_sql, mod_xss, mod_backup, mod_htaccess,

mod_blindsql, mod_permanentxss, mod_nikto

[+] Lanzando modulo exec

[+] Lanzando modulo file

[+] Lanzando modulo sql

Inyeccion MySQL en https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/includes/pop-up-help-context-
generator.php mediante inyeccion en el parametro pagename

          URL maliciosa: https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/includes/pop-up-help-context-
generator.php? pagename=%BF%27%22%28

Inyeccion MySQL en https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/level-1-hints-page-wrapper.php
medianteinyeccion en el parametro level1HintIncludeFile

          URL maliciosa: https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/level-1-hints-page-
wrapper.php?level1HintIncludeFile=%BF%27%22%28

[+] Lanzando modulo xss

Vulnerabilidad XSS en https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/webservices/soap/ws-user-
account.phpmediante inyeccion en la ruta al recurso

          URL maliciosa: https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/webservices/soap/ws-user-
account.php/%3Cscript%3Ephpselfxss()%3C/script%3E

Vulnerabilidad XSS en https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/webservices/soap/ws-lookup-
dnsrecord.php mediante inyeccion en la ruta al recurso

          URL maliciosa: https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/webservices/soap/ws-lookup-dns-
record.php/%3Cscript%3Ephpselfxss()%3C/script%3E

Vulnerabilidad XSS en https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/webservices/soap/ws-hello-world.php
mediante inyeccion en la ruta al recurso

          URL maliciosa: https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/webservices/soap/ws-hello-
world.php/%3Cscript%3Ephpselfxss()%3C/script%3E

Vulnerabilidad XSS en https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/includes/pop-up-help-
contextgenerator.php mediante inyeccion en el parametro pagename

          URL maliciosa: https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/includes/pop-up-help-context-
generator.php?pagename=%3Cscript%3Ealert%28%27wmtuO4i8z2%27%29%3C%2Fscript%3E

Vulnerabilidad XSS en https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/level-1-hints-page-wrapper.php
mediante inyeccion en el parametro level1HintIncludeFile

          URL maliciosa: https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces/level-1-hints-page-
wrapper.php?level1HintIncludeFile=%3Cscript%3Ealert%28%27wtqaxy2qs1%27%29%3C%2Fscript%3E

[+] Lanzando modulo blindsql

[+] Lanzando modulo permanentxss

Informe

------

Se ha generado un informe en el fichero pantera.html

Abrir pantera.html/index.html con el navegador para ver el informe
```

index.php?page=home.php&popUpNotificationCode=HPH0 index.php?page=login.php

index.php?do=toggle-hints&page=/-git/home.php

index.php?do=toggle-bubble-hints&page=/https://muisca.dian.gov.co-git/home.php

index.php?do=toggle-security&page=/https://muisca.dian.gov.co-git/home.php

index.php?do=toggle-enforce-ssl&page=/https://muisca.dian.gov.co-git/home.php

index.php?page=show-log.php

index.php?page=captured-data.php

index.php?page=user-info.php

index.php?page=add-to-your-blog.php

index.php?page=register.php

index.php?page=sqlmap-targets.php

index.php?page=view-someones-blog.php

index.php?page=pen-test-tool-lookup.php

index.php?page=pen-test-tool-lookup-ajax.php

index.php?page=add-to-your-blog.php

index.php?page=browser-info.php

index.php?page=dns-lookup.php

index.php?page=text-file-viewer.php

index.php?page=user-info-xpath.php

index.php?page=set-background-color.php

index.php?page=html5-storage.php

index.php?page=capture-data.php

index.php?page=document-viewer.php&PathToDocument=documentation/how-to-access-

Mutillidae-over-Virtual-Box-network.php

index.php?page=arbitrary-file-inclusion.php

index.php?page=user-poll.php

index.php?page=back-button-discussion.php

index.php?page=styling-frame.php&page-to-frame=styling.php%3Fpage-title
%3DStyling+with+muisca.dian.gov.co

index.php?page=password-generator.php&username=anonymous index.php?page=site-footer-xss-discussion.php
index.php?page=repeater.php

index.php?page=view-user-privilege-level.php&iv=6bc24fc1ab650b25b4114e93a98f1eba

index.php?page=xml-validato r.pp

index.php?page=source-viewer.php

index.php?page=privilege-escalation.php

Fuente. El autor

Anexo Nº 16. Relación de entrada POST

```
POST /index.php?page=add-to-your-blog.php HTTP/1.1

add-to-your-blog-php-submit-button=Save+Blog+Entry&csrf-token=

POST /index.php?page=login.php HTTP/1.1

username=usuario&password=contrase%F1a&login-php-submit-button=Login

POST /index.php?page=register.php HTTP/1.1

confirm_password=admin&username=admin&register-php-submit-button=register-php-submit-

button%3dCreate+Account&password=admin&csrf-token=

POST /index.php?page=source-viewer.php HTTP/1.1

page=source-viewer.php&source-file-viewer-php-submit-button=View+File&phpfile=databaseoffline.php

POST /index.php?page=text-file-viewer.php HTTP/1.1

textfile=http%3a%2f%2fwww.textfiles.com%2fhacking%2fatms&text-file-viewer-php-submi-tbutton=View+File
```

Fuente. El autor