ESCUELA DE INGENIERIA EN SISTEMAS

Tema:

ESTRATEGIAS PARA PROTECCIÓN DE LA INTEGRIDAD DE LA INFORMACIÓN DIGITAL DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE TISALEO

Proyecto de investigación previo a la obtención del título de

Ingeniera en Sistemas y Computación

Línea de Investigación:

Sistemas de Información y/o Nuevas Tecnologías de la Información y Comunicación y sus aplicaciones

Autora:

PAMELA JAZMÍN PARRA ZAMORA

Director:

ING. DARÍO JAVIER ROBAYO JÁCOME, MG.

Ambato – Ecuador

Enero 2021

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE AMBATO

HOJA DE APROBACIÓN

Tema:

ESTRATEGIAS PARA PROTECCIÓN DE LA INTEGRIDAD DE LA INFORMACIÓN DIGITAL DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE TISALEO

Línea de Investigación:

Sistemas de Información y/o Nuevas Tecnologías de la Información y Comunicación y sus aplicaciones

Autora:

PAMELA JAZMÍN PARRA ZAMORA

Dario Javier Robayo Jacome, Ing. Mg. f._____
CALIFICADOR

Santiago Alejandro Acurio Maldonado, Ing. Mg. f._____
CALIFICADOR

Enrique Xavier Garcés Freire, Ing. Mg. f._____
CALIFICADOR

Santiago Alejandro Acurio Maldonado, Ing. Mg. f._____
DIRECTOR ESCUELA DE SISTEMAS

Hugo Rogelio Altamirano Villarroel, Dr. f._____
SECRETARIO GENERAL PUCESA

Ambato – Ecuador

Enero 2021

DECLARACIÓN DE AUTENCIDAD Y RESPONSABILIDAD

Yo: **PAMELA JAZMÍN PARRA ZAMORA,** con **CC. 180404188-5,** autora del trabajo de graduación intitulado: "ESTRATEGIAS PARA PROTECCIÓN DE LA INTEGRIDAD DE LA INFORMACIÓN DIGITAL DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE TISALEO", previa a la obtención del título profesional de **INGENIERA EN SISTEMAS Y COMPUTACIÓN,** en la escuela de **INGENIERÍA EN SISTEMAS.**

1.- Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2.- Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través de sitio web de la Biblioteca de la PUCE Ambato, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de Universidad.

Ambato, enero 2021

PAMELA JAZMÍN PARRA ZAMORA

CC. 180404188-5

AGRADECIMIENTO

En primer lugar, agradezco a **Dios Padre**, por darme la vida, voluntad y persistencia necesaria para no dejarme abatir frente a las contrariedades. A mis padres, **Wilson Parra y Nancy Zamora**, por ser amarme, apoyarme y jamás dejarme rendir por mis sueños, a mi abuela materna **Blanca**, mis tías maternas **María Elena y Cumandá** quienes han sido un pilar fundamental en todas mis decisiones, con su gran amor y sabiduría me han enseñado a ser perseverante en la vida.

De manera muy especial quiero expresar un agradecimiento a mi director de trabajo el **Ingeniero Dario Robayo**, quien me ha brindado todo su apoyo, conocimiento y orientación para la elaboración de dicha investigación, muchas gracias por su paciencia y confianza.

Quiero expresar mi gratitud al **Gobierno Autónomo Descentralizado Municipal de Tisaleo,** principalmente a la **Unidad de Tecnología** y a su director **Ingeniero Hugo Freire**, quienes gustosamente abrieron sus puertas y me permitieron desarrollar el presente proyecto, además, debo agradecer por todas las lecciones aprendidas y el cariño.

Por último, a mi gran amiga **Lety**, el grupo "**Ravenclaw**" quienes creyeron en mí, me enseñaron tanto y siempre estuvieron ahí cuando más los necesité, y finalmente, a **Jorge** quiero decir gracias, mejor amigo por tu apoyo, tu amor, tus enseñanzas, por ser mi apoyo, me has impulsado a mejorar como profesional, y a continuar con **CrySeg**; quiero expresar un agradecimiento a mis hijos peludos.

Por otro lado, a aquellos que no creyeron en mí. ¡*Ni un saludo*!

DEDICATORIA

El proyecto lo dedicó a mis padres Nancy y Wilson, ustedes se merecen todo.

RESUMEN

El tema de investigación tiene como propósito desarrollar estrategias para la protección de la integridad de la información digital del Gobierno Autónomo Descentralizado Municipal de Tisaleo. El estudio evidencia como problema, el escaso conocimiento sobre seguridad informática y sus diferentes aplicaciones por parte del personal del GAD Municipal de Tisaleo. El marco conceptual, se sustenta a partir de recopilación, revisión y análisis de referencia en español e inglés de libros, capítulos, artículos indexados y estudios de organismos nacionales e internacionales referentes al tema. Así mismo, las metodologías teóricas y empíricas empleadas se fundamentan con la aplicación del análisis documental, bibliográfico, encuestas y entrevistas realizadas a los municipios y al Gobierno Provincial de Tungurahua. Como resultado, se destaca el análisis de las vulnerabilidades del sitio *web* que maneja la municipalidad, y posterior, se propone estrategias para mitigar las debilidades encontradas en la aplicación *web*.

Palabras clave: Seguridad, Informática, Ataque, Aplicación, *Web*, Estrategias.

ABSTRACT

The purpose of the following research is to develop protective strategies for the integrity of digital information of the Tisaleo municipal government. A main problem of information security in the study is the lack of knowledge of the personnel. The literature review was based on compilations, reviews and reference analysis of books, chapters, indexed articles, and studies made by national and international organizations in both Spanish and English. Likewise, the theoretical and empirical methodologies are based on documental analysis, bibliographical resources, surveys, and interviews that were applied to different municipalities in the province and the provincial government of Tungurahua. As result, the website's vulnerability analysis was managed by the mentioned entity. Finally, the strategies to mitigate the weaknesses discovered in the web application were proposed.

Keywords: Security, Informatic, Attack, Application, Web, Strategies

ÍNDICE DE CONTENIDOS

PRELIMINARES

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

La tecnología ha revolucionado el mundo de tal manera que las entidades gubernamentales adaptarían a la misma para poder proporcionar al cliente un servicio que esté acorde al mercado actual, su objetivo primordial es conseguir la satisfacción del usuario mediante los servicios prestados y para lograr este propósito, se pretende conceder servicios que posean un valor añadido, y que cubran una necesidad de manera sencilla, al realizar esto, se genera una ventaja competitiva.

El GAD Municipal de Tisaleo tiene como eje principal la gestión de procesos con tecnología, se realizó diseños correctivos para el sitio *web* que mitigan las diferentes vulnerabilidades que existen dentro de una red, por lo cual, para soportar el presente trabajo, se han estudiado más temas similares de análisis de riesgos y/o vulnerabilidades al de la presente investigación; para ayudar a fundamentar de mejor manera el estudio, que se realiza previo al desarrollo de este análisis.

La Unidad de Tecnología junto con la parte administrativa del GAD Municipal de Tisaleo y las demás unidades, están relacionados y generan información impresa, recopilada y almacenada de forma física en archiveros o digitalmente en las diferentes aplicaciones *web* que utilizan las entidades gubernamentales. Dichos documentos e información son requeridos por usuarios internos, como externos; los cuales iniciar sesión en alguna aplicación *web*, la cual, si está con información modificada por un intruso, afectará al correcto funcionamiento del GAD Municipal de Tisaleo y si los intrusos comprometen la información, toda la entidad, se encontrará en graves problemas, como, se conoce hay varias organizaciones que cobran por devolver la información robada/secuestrada.

Como dice Montenegro (2018) en su proyecto de investigación titulado: "*Simulación y Análisis de Vulnerabilidades del Software en los cajeros automáticos de las Instituciones Financieras ubicadas en la ciudad de Guayaquil utilizando Jackpotting como mecanismo de test de intrusión*", se muestra la utilidad de las metodologías de riesgos y cómo estás contribuyen con las instituciones para tener un mejor manejo sobre la minimización de las amenazas

que impactan, esto obliga a la institución a tomar medidas de seguridad que garanticen el éxito de sus técnicas y una mayor capacidad en el sector, que se desenvuelve.

En el proyecto, que se realizó, se ha concluido que utilizar metodologías para el análisis de riesgos son importantes para organizar y garantizar la seguridad de la información institucional, estos resultados aplicados al GAD Municipal de Tisaleo sustenta el presente proyecto de investigación.

Es por lo que realizar pruebas antes de hacerlo pública de un sistema ges decisivo para una organización, al seguir estas políticas de seguridad, se tiene un menor riesgo de poder ser atacados; y si lo son, se encuentran una capacidad de respuesta más alta para garantizar la integridad y fiabilidad de los datos manejados.

De acuerdo con la Superintendencia Nacional de Salud de Colombia (2018) en la Guía de: "*Metodología de Análisis de Riegos de Seguridad y Privacidad de la Información Superintendencia Nacional de Salud*", se menciona que la identificación de medidas de protección y remediación favorecen a la minimización de los riesgos a través de una adecuada correspondencia de controles. De esta forma, se sustenta al presente tema de investigación en la valoración de riesgos de la seguridad de la información en cuanto al impacto y el tratamiento de riesgos, identificación de las vulnerabilidades existentes en la aplicación *web*.

Reconocer con qué recursos cuenta el GAD Municipal de Tisaleo es importante, al momento de redirigirlos en dicho caso, se necesitará mayor seguridad, para lo cual un análisis de riesgos del entorno representara un importante aspecto para tomar en consideración, y mientras sea el momento de la toma las decisiones municipales, se consideran los riesgos, vulnerabilidades, amenazas, prevenir ataques y minimizar incidentes futuros es de suma significancia para los trabajadores del GAD Municipal de Tisaleo y para los usuarios.

Se tomarán en cuenta que *"nada es absolutamente seguro",* siempre existen puertas traseras o enlaces los cuales permiten a cualquier persona con

conocimientos en el campo, entrar sin ser autorizados y muchas veces realizar cambios sin autorización. Es por ello que existen protocolos a seguir, los cuales muchas veces son pasados por alto.

En la actualidad en el GAD Municipal de Tisaleo, la seguridad de la información no es una política institucional, existen dificultades al no mantenerla protegida; además, no se han establecido estrategias de seguridad para prevenir los posibles ataques a los datos que maneja la institución.

El reducido número de personal en la Unidad de Tecnología de la municipalidad hace difícil la implementación de políticas, técnicas y herramientas que garanticen la seguridad de la información haciéndose factible un nuevo ataque, que pueda ser más grave que el anterior, en el que se perdió información valiosa, y con mayor pérdida de información o cambios a la misma y, por lo tanto, los usuarios mal interpreten la información, que se encuentra digitalizada. Todo esto como consecuencia de que no existen mecanismos de seguridad implementados para prevenir cambios o eliminación de la información digital.

También, se desconocen los puntos vulnerables de la aplicación *web* del GAD Municipal de Tisaleo por parte de la unidad de tecnología, por lo que es necesario un análisis más detallado para detectar las falencias, los puntos débiles y propensos a sufrir un ataque en gran escala. Además, se tiene como consecuencia un mínimo nivel de seguridad y un alto riesgo de pérdida de la información.

La presente investigación es de sumo interés para la municipalidad, en dicha aplicación del GAD Municipal de Tisaleo, se encuentra valores a pagar, valores dimensionales de suma importancia que no son modificados, puesto que son muchos departamentos y usuarios de la municipalidad quienes cargan información sobre el sistema. De la misma manera, no se ha explorado el campo de la seguridad de la información dentro de la institución, por esta razón el proyecto de investigación representa innovación para la institución.

Mediante el desarrollo de estrategias para la protección de la integridad de la información digital, se pretende mitigar las amenazas informáticas existentes hacia la entidad para reducir el impacto de ataques internos y externos.

Para el cumplimiento del objetivo general, se desarrolló estrategias para la protección de la integridad de la información digital del Gobierno Autónomo Descentralizado Municipal de Tisaleo, con el fin de determinar qué área, se encuentra vulnerable y a cuál hay que prestarle más atención al momento de desarrollar las estrategias para la protección de la información.

Fundamentar de forma teórica, es primordial para comenzar a definir las estrategias por qué, se necesita ver qué información es modificable, además, de aportar con beneficios para el personal.

Realizar un análisis de riesgo que permita identificar las vulnerabilidades y amenazas existentes en la aplicación *web*, que se maneja en el GAD Municipal de Tisaleo, que a su vez permita identificar de mejor manera, cuáles son los riesgos con los, que se trabajará en la posterioridad y a los que está expuesta la información.

Además, hay que definir las estrategias orientadas a la protección de la integridad de la información y para minimizar de los riesgos identificados en el punto anterior, es necesario identificar y definir cuáles son las estrategias, que se usarán en el desarrollo del proyecto.

La forma de validación del presente proyecto se realizará a través del personal de la Unidad de Tecnología del GAD Municipal de Tisaleo, en el cual, se presentará las estrategias realizadas, para que el personal revise cada una de ellas.

Para el actual proyecto de investigación, se define en primer lugar, lo que representa Open Web Application Security Project (*OWASP)*, la cual es una organización que busca ofrecer soluciones y herramientas para crear, manejar, desarrollar, mantener y realizar pruebas de seguridad en aplicaciones *web*.

OWASP está influenciado por diferentes estándares de seguridad de la información como *COBIT* e *ISO27001*, es decir, combina dos de los mejores estándares, también, contiene otros estándares de información, pero menos

relevantes, que ayudaron a profundizar en el manejo de la seguridad hacia aplicaciones *web*.

Para Machaca (2018) *OWASP* la metodología especifica en el ámbito digital, que se tomarán en cuenta aspectos humanos relacionados a aplicaciones *web*, además, de poseer herramientas propias para realizar su análisis y pruebas de penetración.

La metodología de seguridad de aplicaciones *web* propuesta por *OWASP*, es usada como referente para el análisis y evaluaciones de riesgos, amenazas, vulnerabilidades y todo tipo de ataques, que se dan a una aplicación *web*; la revisión de controles, definidos por esta metodología, permite al equipo garantizar una revisión de la plataforma.

Dicha metodología consiente en la revisión de controles, definidos que admiten al equipo certificar una revisión de las aplicaciones, que se realiza de forma adecuada, la probabilidad de sufrir pérdidas por caídas tanto por *hardware* o por *software*, se realiza las pruebas pertinentes en diferentes fases.

El avance de la tecnología para mejorar la calidad de vida de las personas ha conllevado que personas con malas intenciones utilicen la misma para cambiar o eliminar datos de los catastros, valores a pagar en la municipalidad.

El afán de la investigación reside en contribuir con el GAD Municipal de Tisaleo para que pueda prevenir posibles ataques, minimizar los mismos, prestar un mejor servicio a la sociedad y concientizar sobre la seguridad informática y los riesgos que provoca no identificar los puntos débiles de la aplicación y fortalecer los mismo.

CAPÍTULO I. ESTADO DEL ARTE Y LA PRÁCTICA

1.1. Seguridad Informática

Seguridad Informática para Modarres et al., (2016) es un conjunto de procedimientos y herramientas encargadas de asegurar la integridad, disponibilidad y privacidad de la información de un sistema informático. Adicionalmente, Guallpa (2017) define a la seguridad informática como elemento fundamental en los sistemas informáticos, la integridad de la información se ve expuesta a la manipulación de factores externos, sin dejar de lado el peligro inminente que conlleva el acceso al sistema de un usuario no autorizado.

Por otra parte, para Gómez (2017) es el proceso de prevenir y detectar el uso no autorizado de un sistema informático e implica el proceso de garantizar el acceso no autorizado de personas que, no se encuentran autorizadas. Así mismo, agrega Patiño et al., (2017) mencionan que con el pasar de los años, la seguridad informática ha descubierto una necesidad urgente de proteger la integridad de los datos, que se manejan en las aplicaciones *web*, los fallos de energía continua, falta de sistemas de enfriamiento, falta de políticas de tratamiento de riesgos, ataques, entre otras más, y estas son algunas de las posibilidades de riesgos a los que está expuesto una aplicación.

De lo anterior expuesto, se define a la seguridad informática como un conjunto de procedimientos, técnicas y herramientas que son las responsables de asegurar la integridad, disponibilidad y privacidad de la información en un sistema informático, además, de intentar mitigar las amenazas que afectan al mismo.

Vulnerabilidad

Para Allsopp (2017) una vulnerabilidad es el fallo en un sistema de información que pone en riesgo la seguridad de la información que dejaría que un atacante pueda comprometer al sistema. Por añadidura, Barrio (2017) indica que los términos de informática es un fallo del sistema de información que ubica en riesgo la seguridad de los datos, por lo que permite que un intruso pueda comprometer la integridad de la entidad. Conjuntamente, Auditoría, Consejo, Instalación y Seguridad de Sistemas de Información (ACISSI) (2018) menciona la posibilidad de alterar el flujo del programa, se trasladó a realizar operaciones inesperadas por el programador original, dicha amenaza es aprovechada por

un usuario con malas intenciones para influenciar en el funcionamiento del sistema informático.

De lo anterior expuesto, se conceptualiza como vulnerabilidad al enflaquecimiento en el sistema, así, se da paso a un ataque que obtenga quebrantar el sistema informático de la organización, al enfrentarse a estas situaciones de peligro, desfavorecen la credibilidad de la empresa.

Amenaza

Cano (2016) manifiesta que las amenazas son el quebrantamiento de las seguridades por medio de un programa descargado de manera gratuita, una entrada al sistema por medio de credenciales por defecto, un atacante remoto, una *Universal Serial Bus (USB)* contaminada con un programa desconocido. Adicionalmente, Mastrian y McGonigle (2016) indica las amenazas informáticas son las, que se ocasionan como consecuencia de un intento deliberado de robo informático. Además, son aquellas en las que, por acción, se muestra una debilidad que pone insegura la información que dispones en el sistema. Simultáneamente Barrio (2017) menciona que una amenaza es todo elemento o acción capaz de atentar contra la seguridad de la información, además, surgen a partir de la existencia de debilidades, es decir, que una amenaza sin más existe, si hay alguna debilidad presente que alcance a ser aprovechada. Para que una amenaza sea considerada peligrosa, las empresas estarán expuestas a dichas amenazas que provocarían pérdidas de información, con la posibilidad de que dichos extravíos sean irreparables para la empresa, al infringirse el sistema, la información queda desprotegida y, se convierte en desconfiable.

Se determina que por las definiciones mencionadas con anterioridad una amenaza es el peligro inminente que surge de un acontecimiento que aún no ha sucedido, mientras, no se ven afectadas todas las extensiones que la recogen, además, que se aprecia cuan expuesta, se encuentra la organización, también, cuan perjudicial resultaría la perdida y cuánto costaría la restauración.

Ataque

Para Baca (2016) manifiesta que un ataque es la constitución de las amenazas más grandes que existen para las empresas en la actualidad, esto afectaría por igual a individuos externos a la empresa, organizaciones asociadas, y demás. Al mismo tiempo Cano (2016) alude que es el aprovechamiento de vulnerabilidades convergentes entre lo físico y digital que fragmenta la tecnología de información y la tecnología de operaciones que en conjunto instituyen un producto de forma digital: cuyas actividades están concentradas en mantener "*protegida*" la información de los usuarios. Así mismo, Barrio (2017) mencionan que un ataque, se origina con una dirección de internet en la, que se confía y ha sido suplantada, además, de una mala aplicación de la política de seguridad, también, se dice que un ataque, se genera por medio de engaños a los usuarios y de esta manera, se obtiene información con la cual existe la posibilidad de ingresar al sistema. Por otra parte, para McDonough (2019) señala que el riesgo de sufrir un ciberataque está en aumento para todas las empresas y todas las personas que coexistimos; además, se dice que la dependencia ha incrementado con el pasar de los años, las personas tienen una necesidad de emplear su tiempo en un celular, como consecuencia de la misma exponen la información personal que está guardada en el dispositivo móvil.

De lo anterior expuesto, se conceptualiza como ataque a la tentativa organizada y producida por una o más personas para infringir daños o problemas a un sistema informático. Un ataque consiste en aprovechar alguna debilidad o falla en el *software*, *hardware*, además, de las personas que forman parte de un ambiente informático; se originó un efecto negativo en la seguridad de los datos.

Riesgo

Por otra parte, Rocha et al., (2016) agrega que es la consecuencia que conlleva a la interrupción o la vulneración de la seguridad, la falta de protección, credenciales de acceso fáciles o por defecto, puertos abiertos, falta de actualización de paquetes. De otra forma Montenegro (2018) indica que un riesgo informático se produce por la desactualización del *software*, esto hace, que se encuentre más expuesta ante ataques, en donde, se ocasiona fallos en los sistemas que afectarán de manera económica y desestabilizarán a la empresa como tal. Para Romero et al., (2018) un riesgo es las

vulnerabilidades o amenazas que están por separado y no representan mayor peligro, pero cuando, se llegan a conectar, se convierte en un desastre de magnitudes inesperadas.

De las definiciones indicadas en el punto anterior, se establece a un riesgo como la posibilidad de que una amenaza se produzca, se da lugar a un ataque al equipo. Esto no es más que la posibilidad de que ocurra el riesgo porque, se materializo y cause grandes daños a los bienes o a la información de la empresa.

Incidente/Desastre

Mastrian, McGonigle (2016) sostiene que el resultado fallido en la infraestructura de *TI*, la destrucción de recursos físicos de la empresa, la causa de los incidentes es solucionada sin necesidad de inversiones futuras, mediante una reparación de cambio para solventar el error. A la vez, Romero et al., (2018) menciona que un incidente es la violación inminente a las políticas de seguridad de la información implícita o explicita; no previsto pone en peligro la infraestructura de Tecnologías de la Información (*TI*), conformada por *hardware*, *software*, redes, procesos, personal. Por otro lado, Montenegro (2018) alude que un incidente de seguridad de la información se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las actividades de la empresa.
Se conceptualiza como incidente/desastre a la destrucción de los recursos físicos y lógicos que pertenecen a la empresa; los recursos físicos son incendios, inundaciones, entre otros más; los recursos lógicos son *software*, sistemas, aplicaciones, datos, informaron en sí.

Técnicas de Protección de Datos

Existen diversas maneras de proteger la integridad de datos informáticos tanto a nivel de *hardware* como de *software*. Para profundizar en esta temática, se mencionarán algunas de ellas:

Replicación y Backups

La replicación para el Instituto Vasco de Estadística (2018) consiste en realizar una copia exacta de los datos existentes y el estado del servidor, existe la posibilidad de ser alojada en otro servidor de almacenamiento el cual, como medida de protección adicional, muchas veces, se encuentra desconectado de la red. Por otra parte, los *backups* almacenan datos mas no el estado, que se encontraba el servidor; los respaldos a diferencia de la replicación se hacen cada cierto tiempo y, no se necesita en caliente (con el servidor, se realizó las funciones programadas).

Capacitación al personal

En relación a la capacitación al personal el Instituto Vasco de Estadística (2018) dice que en toda empresa existe el riesgo de que personas mal intencionadas tengan la posibilidad de acceder a datos de gran importancia para la institución y puedan ser modificados o eliminados; muchas veces la forma en la que los atacantes tienen acceso a la entidad es mediante la explotación de la vulnerabilidad más grande que es el propio ser humano que utiliza ingeniería social la cual es una técnica con la que un atacante engaña al usuario para que éste de *click* hacia una página vulnerada, descargue programas maliciosos o sus credenciales de acceso. Es por lo cual una capacitación a todo el personal, tanto administradores de sistemas como usuarios en general, es necesaria para mitigar estas amenazas y preparar a los usuarios ante cualquier comportamiento sospechoso en la red.

Codificación Segura

La codificación segura como lo menciona el Instituto Vasco de Estadística (2018) es toda máquina electrónica lleva consigo un *software* que la controla y cuidar el desarrollo de *software* para que éste no presente errores y pueda causar fallos catastróficos son una prioridad en toda institución. Como preámbulo, se cita ejemplos tales como: Error de programación del módulo de gestión del cohete *Ariane 5* hace que el mismo, se autodestruya 37 segundos después de despegar (*1996*). Un error de control de transacciones en la bolsa de la empresa *Knight Capital* hizo que ésta perdiera 500 millones de dólares en media hora (2012).

Es por lo cual la seguridad dentro de la codificación es importante para las empresas. A raíz de estas necesidades; se crean principios para ayudar a los programadores a

desarrollar *software* seguro, se trata de *SD3 + C (Security by Default, Security by Design, Security in Deployment and Communication)* y la metodología *OWASP* a través de *SAMM (Software Assurance Maturity Model o Modelo de Madurez para el Aseguramiento del Software)* es la que usa estos principios para desarrollo de aplicaciones seguras.

Controles de roles y privilegios

El control de roles y privilegios como lo ensena el Instituto Vasco de Estadística (2018) a nivel de administradores. En el momento, que se crean usuarios, es importante conocer las funciones de los mismos y qué tipo de acceso tienen en la empresa, de ésta manera, existe la posibilidad de controlar de mejor manera los errores y de igual manera conocer desde qué departamento surgió un fallo de seguridad para que pueda ser corregido de una mejor manera, se tiene como ejemplo el evitar que un usuario del departamento de talento humano, tenga acceso al sistema financiero y pueda realizar compras a nombre de la empresa o de igual manera evitar la escala de privilegios de un usuario normal a administrador del servidor, lo cual presentaría una grave falla de seguridad informática institucional.

1.2. Objetivos de la Seguridad Informática

Integridad

Integridad para Baca (2016) es la modificación de los datos existentes que toman un valor incorrecto, como, por ejemplo, si se reasigna un precio elevado a un producto del almacén, esto generaría un cobro excesivo y por ende el cliente tendría una mala imagen del almacén. Por esta razón es necesario resguardar la integridad de la información porque un cambio o fallo en el sistema provocaría daños permanentes o temporales. Conjuntamente, Romero et al., (2018) enfatiza que la integridad son los componentes del sistema que permanecen intactos a menos que sean modificados por los usuarios que utilizan el sistema, si, se añade información no válida o, se elimina provocaría un descuadre de los datos manejados por la empresa. A la vez, Najera-Gutierrez y Ahmed (2018) define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos.

De lo anterior expuesto, se define a la integridad como la forma de mantener inalterada la información ante accidentes. El principal objetivo de la integridad es prevenir las modificaciones no autorizadas, los cambios provocados alterarían de forma radical el sentido valido de la información.

Disponibilidad

Guevara (2017) es mantener al sistema accesible en todo momento mientras sea el personal lo necesite, es un recurso indispensable en el normal funcionamiento de la organización. Paralelamente, ACISSI (2018) argumenta que la disponibilidad es la continuidad operativa de la entidad, la pérdida de recursos provocaría el fallo de la productividad o de la credibilidad de la empresa. Así mismo, disponibilidad para Romero et al., (2018) menciona que disponibilidad es el acceso al sistema y la información estará accesible para efectuar cualquiera de las etapas del proceso del negocio en cualquier momento sin interrupciones.

De lo previo expuesto, se establece a la disponibilidad como el acceso a los sistemas o aplicaciones que maneja la empresa. Es muy necesario, que se ofrezcan los recursos necesarios que requieren los usuarios autorizados, por esta razón la información permanece accesible al personal.

Confidencialidad/Autenticidad

Najera-Gutierrez y Ahmed (2018) acota que confidencialidad es la protección de datos frente a la difusión no autorizada, la perdida de confidencialidad implicaría problemas legales, además, de la pérdida del negocio y de la misma credibilidad. Adicionalmente, Aguilera et al., (2016) expresa que la información, que se utiliza y no comprometer a la empresa, con contraseñas débiles o por defecto, que se deducen por simple intuición, o al encontrarse con un *link* de dudosa procedencia, correos instantáneos; mantener la conformación segura generará mayor confianza en el personal y así, se podrá aportar un buen servicio. El autor Barrio (2017) agrega que la información es protegida para su posterior manejo, por esto, la misma está disponible en cualquier momento, esto garantiza un buen funcionamiento del sistema y del servicio en sí.

De lo previo mencionado, se establece que la confidencialidad es la manera de mantener segura la información para las personas autorizadas, es muy necesario que el acceso a la información se dé mediante autorización y, se realice un control cuidadoso, porque existe la posibilidad de ser mal utilizada.

No Repudio

El no repudio para Najera-Gutierrez y Ahmed (2018) es un servicio de seguridad que permite probar la participación de las partes en una comunicación, además, proporciona protección ante una interrupción de comunicación, por parte de algún factor externo, que se inmiscuya en el sistema. Así mismo, Baca (2016) plantea, que se permite la participación de las diferentes partes en una comunicación; sin perder datos, esto tendría consecuencias graves debido a la modificación, que se provocaría. Así mismo, para Patiño et al., (2017) señalan la participación de las diferentes partes en una comunicación, es decir, comienza en el momento que el emisor niega él envió, pero, también, se origina mientras el receptor, se niega a recibir la información.

De las definiciones indicadas, se establece al no repudio como la irrenunciabilidad a la comunicación, que permite probar la participación de las diferentes partes en una comunicación; la protección, que se efectúa por medio de una colección de evidencias irrefutables que permitan garantizar la transmisión de la información.

1.3. Integridad de la Información

¿Como garantizar la integridad de la información?

Los autores (Cano, 2016); (Modarres, Kaminskiy, & Krivtsov, 2016); (Montenegro, 2018) concuerdan que para evitar o minimizar la probabilidad de que la información sea vulnerada es necesario controlar los derechos y privilegios de acceso: se estableció niveles de interacción, se define roles y usuarios; también, es necesario delimitar responsabilidad en la empresa para evaluar las necesidades departamentales e implementar planes de acción.

Así mismo, la integridad de la información para Aguilera et al., (2016) indica que es la capacidad de garantizar que los datos no han sido modificados desde su creación, puesto que el añadir, eliminar o capturar datos no válidos, comprometería a la empresa. Por esta

razón es necesario resguardar la integridad de la información porque un cambio o fallo en el sistema provocaría daños temporales y hasta en el peor de los escenarios llegaría a ser permanente. Conjuntamente, Barrio (2017) considera que la integridad de la información es la responsabilidad de vigilar por el bienestar de los datos, por esa razón, se tiene un control de los derechos y privilegios de acceso al sistema para establecer niveles de interacción que, bien delimitados, se definan roles y usuarios, también, se delimita las responsabilidades, es decir, que ciertas partes del sistema no serán visibles para dicho personal.

Para una mejor explicación, se puede ilustrar con un sencillo ejemplo: Una persona necesita un tratamiento hospitalario que incluye la administración diaria de un medicamento en dosis de 10 miligramos (*mg*), el cual, se ingresa en un sistema que contiene los tratamientos de los pacientes. Accidental o intencional, se produce una modificación en el registro electrónico del tratamiento y las dosis quedan establecidas en 100 *mg*, con consecuencias mortales.

La integridad de la información proporciona privacidad en la comunicación entre dos puntos en una red de comunicación, de esta forma, se garantiza que la información transmitida no pueda ser interceptada, modificada o eliminada por elementos no autorizados y así conservar la información de manera íntegra.

Tipos de Amenazas

Físico

Para *Red Hat, Inc.* (2005) una amenaza física es la implementación de medidas de seguridad en una estructura definida utilizada para prevenir o detener el acceso no autorizado a material confidencial. Algunos ejemplos de controles físicos son: cámaras de circuito cerrado, identificación de fotos, puertas de acero con seguros especiales. El área de la seguridad informática dentro del ámbito local aun no es explorada a fondo, por lo cual, muchas entidades tanto públicas como privadas corren el riesgo de sufrir ataques de personas mal intencionadas que deseen sustraer información o causar algún tipo de daño informático mediante ataques cibernéticos hacia páginas *web*, computadoras o servidores. Es por lo que la presente investigación representa un gran interés, sienta bases

para que este campo sea explorado mediante el uso de nuevas tecnologías para análisis de vulnerabilidades, así como estándares y metodologías para mitigar amenazas.

Las amenazas físicas de acuerdo con *ACISSI* (2018) consisten en aplicar barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial. Las principales amenazas, que se prevén son: desastres naturales, incendios accidentales, tormentas e inundaciones, disturbios, sabotajes internos y externos.

Técnico

De acuerdo con *Red Hat, Inc.* (2005) señala que las amenazas técnicas utilizan la tecnología como una base para controlar el acceso y el uso de datos confidenciales a través de una estructura física sobre la red. Son mucho más extensos en su ámbito e incluyen tecnologías tales como: encriptación, tarjetas inteligentes, autenticación a nivel de red, listas de control de acceso, *software* de auditoria de integridad de archivos.

La seguridad lógica para *ACISSI* (2018) es la aplicación de barreras y procedimientos que protejan el acceso a los datos y solo, se permita el acceso a personas autorizadas. Además, algunos de los objetivos, que se emplean son: restringir el acceso a los programas y archivos, asegurar, que se utilicen los datos o archivos y programar correctos en el procedimiento correcto, que la información recibida sea la misma que ha sido transmitida.

Administrativo

Los controles administrativos para *Red Hat, Inc.* (2005) lo definen como los factores humanos de la seguridad, que incluyen todos los niveles del personal dentro de la organización y determina qué tipo de usuarios accederá a un determinado recurso e información aprovechada en medios tales como: entrenamiento, conocimiento, planes de recuperación, preparación para desastres, estrategias de selección de personal, registro y contabilidad de personal.

ACISSI (2018) manifiesta que una amenaza humana sobre todo trata de fallas provocadas por el mismo, que incluyen empleados que ingresan al trabajo sin presentar tarjeta de acceso, o personas externas a la empresa. Por otro lado, la tecnología utilizada para

realizar el trabajo, que permite la aparición de las condiciones ambientales peligrosas. Algunas de ellas, se presentan, a continuación: aumento de ritmo de producción, tecnología inadecuado de los equipos, normas de compras inadecuadas, desgaste normal de herramientas.

1.4. Análisis de Riesgos

Un análisis de riesgos como lo explica Cano (2016) ratifica que el análisis de riesgos consiste en identificar los activos, vulnerabilidades y amenazas a los, que se encuentran expuestos, así como la probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, trasferir o evitar la ocurrencia del riesgo. Adicionalmente, Modarres et al., (2016) revela que el análisis de riesgos es el hecho de calcular la probabilidad que ocurra cosas negativas, hay que obtener una evaluación económica del impacto de estos sucesos y la elaboración de un plan de continuidad de negocios. Y para Romero et al., (2018) menciona que es el estudio de las causas posibles como amenazas, probables eventos no deseados, que se producen; hay que tener en cuenta los requisitos legales identificados de negocios, la perdida de vulnerabilidad que conlleva a la toma de decisiones en la empresa.

De acuerdo con lo mencionado anterior, establece al análisis de riesgos como la comprobación de la coexistencia de controles de seguridad existentes, las pruebas con el *software* y el monitoreo de los sistemas de información permiten formar el estado actual de la organización, identificar los orígenes de las vulnerabilidades y proponer recursos de control que permitan su minimización.

1.5. *Metodologías de Análisis de Riesgos*

OCTAVE: (*Operationally Critical Threat, Asset and Vulnerability Evaluation*) sirve para la construcción de los perfiles de amenazas basados en activos, además, del desarrollo de planes y estrategias de seguridad, ayuda a determinar los activos relevantes para la organización, la estimación del impacto mientras, se define el daño causado al activo o la probabilidad de ocurrencia de una amenaza.

MAGERIT: (*Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*), se realiza una escala de valores cualitativos, cuantitativos e indisponibilidad del sistema, metodología relacionada con la difusión del uso de las

tecnologías de la información, los riesgos son minimizados con medidas de seguridad que generen mayor confianza y *MAGERIT* permite saber el valor que está en juego si existen fallos en el sistema.

OSSTMM: (*Open Source Security Testing Methodology Manual*) uno de los estándares más completos, la revisión de la privacidad es una parte imprescindible en una empresa, la búsqueda de vulnerabilidades, la prueba de intrusión y el *hacking* ético son actividades indispensables que permiten identificar en que falla su sistema de seguridad de la información.

OWASP: (*Open Web Aplicattion Security Project*) la revisión de controles, definidos que permiten al equipo garantizar una revisión de la plataforma, que se realiza de forma adecuada, la probabilidad de sufrir pérdidas por caídas tanto por el *hardware* o por el *software*, se realiza las pruebas de gestión de la configuración, es decir, se investiga la infraestructura de la arquitectura para revelar datos importantes sobre el sistema, también, se maneja una gestión de sesiones que cubre todos los controles a realizar sobre el usuario y las pruebas de lógica de negocio que consiste en probar si los pasos de autenticación son cumplidos o si el mecanismo no funciona en el orden predeterminado, y, se depende de las necesidades de cada empresa, se adapta a dichas organizaciones.

1.6. *The Open Web Application Security Project*

Mediante el análisis comparativo presentado en el punto anterior, se pudo concluir las herramientas que van a ser utilizadas.

Para el presente proyecto de investigación, se define en primer lugar, lo que representa *OWASP*, la cual es una organización sin fines de lucro; que busca ofrecer soluciones y herramientas para crear, manejar, desarrollar, mantener y asegurar aplicaciones para su mejoramiento continuo.

Open Web Application Security Project Foundation (OWASP) (2015) menciona que, al ser un proyecto de constante crecimiento, se utiliza su última versión 4.0 la cual fue creada el 17 de septiembre del 2014, y actualizada en abril del 2016, la versión 5.0 aún está en desarrollo.

CAPITULO II. DISEÑO METODOLÓGICO

2.1. Enfoque de la Investigación

Esta investigación tendrá un enfoque cuantitativo, debido a, que se trabajó mediante entrevista a los jefes del departamento de sistemas de los Municipios de los diferentes cantones y el Gobierno Provincial de Tungurahua, lo que permitió analizar la información aportada en las entrevistas realizadas, además, fue de utilidad para definir las estrategias de la presente investigación.

2.2. Métodos Teóricos

Análisis Documental

El presente estudio, se realizó mediante un análisis documental que, para Hernández Sampieri et al., (2014), consiste en un conjunto de operaciones que representan el contenido, cuya finalidad es extraer un conjunto de palabras que conforman la parte transcendental del documento, dicho conjunto es de utilidad para dar lugar a un subproducto o un instrumento de ayuda. Esta metodología permitió una revisión de los documentos que regulan la protección de datos en el Ecuador.

Análisis Bibliográfico

Este tipo de investigación fue de gran apoyo en el desarrollo del presente proyecto, como menciona Campos (2017), reúne los conocimientos técnicos y científicos que están en continuo cambio, además, que ayuda a obtener mayor aprendizaje sobre conceptos que son necesarios para el poder complementar la documentación.

El proyecto de investigación fue basado en información que es posible hallarla en libros técnicos, informes, artículos, los cuales proporcionan información relevante para llevar a cabo la misma.

Método Analítico-Sintético

Para el desarrollo de la investigación, se ha tomado en cuenta aplicar el método analítico-sintético, Rodríguez y Pérez (2017) refieren que dicho análisis une dos de los procesos

intelectuales los cuales son: analizar y sintetizar; esto quiere decir, que se parte de la separación de los factores antes mencionados de manera individual, para luego unirlos de una forma integral desde lo más sencillo hasta lo más complejo.

El presente proyecto necesitó del método analítico-sintético, porque un análisis del problema es imprescindible para establecer las causas y los efectos del problema planteado, además, de conocer su origen y diseñar una solución coherente para el presente. También, se basado en la recopilación de documentos, se analizó los diferentes análisis de riesgos para definir las estrategias más apropiada para la protección de la información digital del Gobierno Autónomo Descentralizado Municipal de Tisaleo.

Método de Observación

Respecto del método de observación, Hernández Sampieri et al., (2014) mencionan que, para una investigación cualitativa, se necesita de la observación, en donde, se explora, describir ambientes, comprender procesos, vinculaciones entre personas, patrones, que se desarrollan, identificar problemas sociales, generar hipótesis para futuros estudios y demás; de esta forma, se podrá analizar lo antes ya mencionado y analizar o reflexionar sobre ello.

Esta metodología, se aplicó para poder visualizar el comportamiento actual del sistema, la forma en la, que se guardan/manejan las claves, y de qué manera, se hallan ubicadas las computadoras personales en el departamento.

2.3. Método Empíricos

Entrevista

La entrevista para Hernández Sampieri et al.,(2014) es de forma cualitativa, además, de ser flexible y abierta para conseguir más información de las personas entrevistadas, como, se mencionó en el punto anterior, el conversar e intercambiar información entre una persona y otra u otros entrevistados; también, existe la posibilidad de dar otra forma a las preguntas y respuestas para obtener más información de un tema determinado.

La aplicación de las entrevistas se realizó a los directores de Sistemas/Tecnología de los diferentes municipios de la provincia tal como: Tisaleo, Ambato, Cevallos, Quero y el

Honorable Gobierno Provincial de Tungurahua con el objetivo de recopilar la mayor cantidad de información referente al uso de las aplicaciones *web* en dichas instituciones.

Población

La población la componen los jefes de sistemas/tecnologías de la información de los municipios de Tisaleo, Ambato, Cevallos, Quero y el Honorable Gobierno Provincial de Tungurahua

Resultados de las encuestas y entrevista

Primero, para la encuestas, se comenzó con una pregunta que es fundamental para la seguridad de las aplicaciones *web* como, se puede ver en el siguiente cuadro encuentra la pregunta y las respuestas aportadas por cada Municipio y el Gobierno Provincial; las respuestas se encuentran en distinto orden puesto que las mismas fueron realizadas bajo una cláusula de confidencialidad la cual, se encuentra detallada en el formato de las entrevistas en los Anexos 1; y, para finalizar, se encuentra un análisis.

Tabla 1. Medidas para asegurar la información de la aplicación web

Pregunta 1: ¿Qué medidas tiene para asegurar la información y el acceso de la aplicación *web* que maneja el municipio? ¿Y qué protocolos utiliza?
R1: La dirección de tecnologías del GADM- tiene sus políticas propias de seguridad de la información, que no sigue solo por los técnicos del área sino, también, los usuarios de los sistemas, ya que la mayor vulnerabilidad en cualquier empresa o institución son sus usuarios internos. Como complemento a las políticas internas de seguridad, se ha implementado infraestructura tanto en nivel de *hardware* como, por ejemplo, un *firewall* perimetral y un *firewall* interno; así como, también, de *software* como son los certificados de seguridad para garantizar que no exista un acceso inadecuado a la información. Como el GADM- presta sus servicios tecnológicos a nivel interno y externo, protegemos la información con protocolos *https* para la encriptación transaccional que realizan las aplicaciones *web*.
R2: *Firewall* y puertos 8080, 443.

R3: Tenemos nuestra página *web* en el extranjero en donde los técnicos que usan esos servidores son los encargados de proteger dicha página. Usamos *Cloudflare* que sirve para enmascaras nuestras *IPS* fijas y hacer un poco más complicado el acceso a los *DDNS* e *IPS* públicas del gobierno provincial, además, se tiene un *firewall* hacia el exterior. En nuestras aplicaciones la mayoría son de consulta y una es abiertamente de uso público.
R4: Los mecanismos para asegurar la información están basados en la normativa legal vigente y la norma 410 de las Normas de Control Interno emitidas por la contraloría general del estado debido a, que se tiene una infraestructura hibrida (Servicio local y en *outsourcing*).
R5: Al momento, no poseo de ninguna medida de seguridad. Se utiliza los protocolos *http, https,* los puertos 80, 8080 y 25, entre otros más.
Análisis: En algunos municipios existe una escasa seguridad por lo, que se implementa las mejoras del municipio y el gobierno provincial como son el *firewall* perimetral y el *firewall* interno que no permitirían que los ataques lleguen a los servidores; además, existe la posibilidad de utilizar un servicio externo (*outsourcing*) como *Cloudflare* que al momento de que un ataque ingrese a las aplicaciones, el servicio muestre la *IP* de dicho servicio externo, y así no tener mayores pérdidas.

Fuente: elaboración propia

Para la segunda pregunta, se realizó una consulta sobre cuantas personas tienen acceso de administrador hacia las aplicaciones *web*, es fundamental contar con ello para determinar que personas con frecuencia son las que tienen acceso completo a dichas aplicaciones. Como, se puede ver en la tabla 2 los Municipios y el Gobierno Provincial aportaron sus respuestas completas.

Tabla 2. Personas con acceso de administrador de la aplicación

Pregunta 2: ¿Cuántas personas existen con acceso de administrador de la aplicación? y ¿cuáles son las razones?
R1: La dirección de tecnologías del GADM- está dividido en dos unidades: la primera es la unidad de infraestructura y la segunda de desarrollo de *software*, para brindar seguridad a las aplicaciones web es necesario que sean complementarias y es así existen

cada una de esas unidades dos personas que son responsables de administrar los servicios y las aplicaciones *web*.
R2: La página *web* tiene un administrador y la otra aplicación local del municipio existe dos administradores: uno por parte del municipio y otro del servicio *outsourcing*.
R3: Una.
R4: Una sola persona con acceso de administrador, ya que en el área de sistemas solo hay una persona.
R5: Dos personas, son los desarrolladores de las aplicaciones.
Análisis: Las personas con acceso de administrador de la aplicación *web* son dos principales, uno de los jefes del municipio supo explicar que uno de ellos está en la unidad de infraestructura y, se complementa con una persona de la unidad de desarrollo porque es fundamental tener más personal que brinde seguridad a las aplicaciones, por otra parte contestaron en la entrevista que como administrador a la aplicación *web* existe dos personas los desarrolladores, ellos son los responsables de estructurar la misma.

Fuente: elaboración propia

En la pregunta tres, se realizó una consulto sobre normas o estándares de seguridad que utilizan en los Municipios y el Gobierno Provincial, es primordial tener el conocimiento de las mismas, por ello, se detalla, a continuación, las respuestas que las instituciones aportaron:

Tabla 3. Normas/estándar para garantizar la seguridad informática

Pregunta 3: Se basa en alguna norma/estándar para garantizar la seguridad informática?
R1: Si, se basa en la norma *ISO/IEC* 270001.
R2: De acuerdo con las normas de control interno de la contraloría general del estado.
R3: No, ya que el municipio cuenta con limitados recursos para la unidad de tecnología.
R4: Si, en la norma 410 de contraloría sobre sistemas informáticos.
Análisis: La mayoría de los municipios y el Gobierno Provincial, se basa en las Normas de Control Interno de la Contraloría General del Estado, además, un municipio, se basa en una norma de seguridad de la información la *ISO/IEC* 27001, por otra parte, se ve

las limitaciones que tienen los municipios, lo cual afecta a la seguridad de las aplicaciones *web* que manejan los mismos.

Fuente: elaboración propia

Posterior para la pregunta cuatro, se examinó si necesitarían consultoría externa puesto que esto es fundamental para obtener mejores procesos de seguridad informática, y, se ve las respuestas la mayoría de los municipios y el Gobierno Provincial respondieron que es necesario, pero el presupuesto les impide, adquirir dicho servicio.

Tabla 4. Consultoría externa para garantizar procesos de seguridad informática

Pregunta 4: ¿Cree usted que necesitaría de consultoría externa para garantizar mejores procesos de seguridad informática?
R1: Si, porque sucede que hay muchas personas especializadas en seguridad que saben cuáles son los posibles ataques.
R2: Si, porque se necesita de personal especializado para realizar cierto tipo de pruebas y mitigar fugas de información e identificar ataques específicos, que se puedan tener.
R3: Si.
R4: No, se necesita presupuesto.
R5: Si, es muy necesario contar con ayuda externa. Para garantizar el correcto funcionamiento de los procesos de seguridad.
Análisis: La mayoría de las jefes han respondido que es fundamental contar con consultoría externa para garantizar los procesos de seguridad informática. También, se ve que por falta de presupuesto no prestar mayor seguridad a sus aplicaciones *web*, por lo que deja el libre acceso a las mismas y se expone la información a manipulaciones de terceros.

Fuente: elaboración propia

La quinta pregunta trata sobre la capacitación del personal en los últimos dos años sobre protocolos de respuesta a incidentes informáticos, es decir, si asistieron a algún taller, foro o algo por el estilo, es imprescindible para la continua mejora del departamento, a continuación, se detalla las respuestas:

Tabla 5. Capacitaciones en protocolos de respuesta e incidentes informáticos

Pregunta 5: Se ha capacitado en éstos últimos 2 años en protocolos de respuesta a incidentes informáticos?
R1: Si, en los últimos 3 - 4 meses.
R2: Si.
R3: No.
R4: No, por la misma razón que el municipio cuenta con pocos recursos para la unidad de tecnología.
R5: No. Pero hemos asistido a muchas conferencias.
Análisis: La mayoría de los jefes de sistemas/tecnologías de los municipios y el Gobierno Provincial, no se ha capacitado en protocoles de respuesta a incidentes, por lo que, no brindan una mejor seguridad en el entorno del sitio *web*, además, la constante capacitación ayuda a adquirir nuevos conocimientos sobre el tema ya mencionado. En algunos municipios solo han asistido a conferencias referentes al tema, lo que no es tan bueno, pero tampoco, se actualiza al personal en el tema.

Fuente: Elaboración propia

La pregunta seis, se refiere a accesos indebidos hacia las aplicaciones web, porque es fundamental conocer si existió dicho evento, el conocer cómo mitigaron en el pasado dichos accesos para tener una base en la cual comenzar a establecer principios para minimizar futuros eventos, de esta forma, se podrá ayudar a mejorar la seguridad en el tema de estudio de la presente investigación, en la siguiente tabla, se demuestras las respuestas:

Tabla 6. Ataques o accesos indebidos a la aplicación web

Pregunta 6: Ha sufrido la aplicación algún ataque o un acceso indebido?
R1: Si, se recibe ataques externos hacia nuestra página *web*, pero con las políticas de seguridad que tenemos obligamos a mantener respaldos diarios de la información por lo cual, se pudo solventar prontamente, además, la infraestructura con el *firewall* perimetral ha impedido que lleguen directamente a nuestros servidores.
R2: Hace dos años, por un ataque general *DDOS* que sufrió *CNT* a nivel general.
R3: Si, hacia la página *web*, hace unos 7 años, por tener una plataforma desactualizada.
R4: No.

R5: Si, a la página *web*.
Análisis: Casi todas las instituciones han sufrido ataques, ya sea por desactualización de la plataforma o por un ataque general de Denegación de Servicios que sufrió *CNT* a nivel general. Esto hace notar que es necesario contar con una buena infraestructura que no permita accesos indebidos o redireccione las *IPS* a otro sitio, esas personas manipulan, cambiar información sensible al público.

Fuente: elaboración propia

Si la pregunta anterior, fue positiva, en la presente pregunta, se ve qué la información y que cantidad, se perdió, en la siguiente tabla, se demuestra lo, que se investigó en los Municipios y el Gobierno Provincial:

Tabla 7. Ataque a la aplicación e información perdida

Pregunta 7: Si hubo un ataque a la aplicación, ¿qué información y que cantidad, se perdió?
R1: Información sensible nunca, se perdió ya que la infraestructura perimetral no ha permitido que lleguen a nuestros servidores.
R2: No se perdió información y, solo afectó al *índex* de la página *web*.
R3: Ninguna.
R4: Se perdió un mes de trabajo, un mes de actualización.
R5: Ninguna, porque atacaron a las *IPS* público, no se perdió información.
Análisis: La mayoría de los municipios y el Gobierno Provincial dieron a notar que la información perdida fue poco relevante, por una parte, un municipio cuenta con un *firewall* perimetral que no permitió que el ataque llegara a los servidores; por otro lado, se contaba con el servicio de *Cloudflare* que mantuvo la *IP* fija de dicho servicio, lo que no permitió que el ataque llegara a los servidores. Además, se nota que un municipio no contaba con mucha seguridad por lo que sí perdió información sensible y tuvo que trabajar mucho en la recuperación de la misma.

Fuente: elaboración propia

En la octava pregunta, se ve que los Municipios y el Gobierno Provincial, aportaron con valiosas respuestas, en donde, se ve el tiempo que tardaron en recuperar la información que

fue vulnerada, que serán de utilidad para contribuir con las estrategias, que se desarrollan en la presente investigación para el GAD Municipal de Tisaleo.

Tabla 8. Información perdida por un ataque y tiempo de recuperación de la misma

Pregunta 8: ¿Si la información se perdió, cuanto tiempo se tardó en recuperarla? Y del 100% de información perdida cuanto recupero?
R1: Ninguna. Pero hasta mitigar el ataque *DOS,* se tardó 4 días.
R2: Se recupero el 100 % de una hora y, no se perdió ninguna información realmente.
R3: Un 70 % se recuperó y me demore 15 días.
R4: Ninguna.
R5: El 1 % se perdió, luego, se procedió a reconstruir.
Análisis: El contar con una buena infraestructura ayudó a que uno de los municipios, no se tarde mucho en recuperar la información que los atacantes trataron de vulnerar, lo anterior expuesto, se contrasta con la situación actual del tema de estudio, al no contar con una buena infraestructura, el no contar con un, servicio externo en las aplicaciones *web,* dejo mucho tiempo sin servicio de la aplicación, es así que causa molestias hacia los clientes internos y externos, también, se tardó mucho en recuperar la información, el volver a estabilizarla y ponerla en funcionamiento para su posterior uso al público, dio molestias a los usuarios.

Fuente: elaboración propia

Por otro lado, el resultado de las preguntas puntuales realizadas a la persona encargada del departamento de *TI* del GAD Municipal de Tisaleo motivo de estudio, es el siguiente:

Pregunta1: ¿Cuál es el proceso de creación de nuevos usuarios?

Se asigna usuarios con perfiles al grado de responsabilidad en cada área.

¿Qué tipo de credenciales usa para la creación de los usuarios?

Se realiza de forma libre.

¿Existe exigencias por parte de la aplicación para el tipo de contraseñas, que se ingresa?

No existe restricciones.

Pregunta2: ¿Tiene usted respaldos de la información sensible del municipio? Y ¿En dónde la almacena?

Si, se almacena en otro equipo y, se graba en *DVD*.

Pregunta3: ¿Cómo gestiona los respaldos en caso de existir un incidente informático?

Describa el proceso.

El respaldo está programado en la base de datos diariamente, en el caso de ocurrir un incidente informático, se restauraría del día anterior. Todos los días 6 de la tarde.

Pregunta 4: Considera adecuado el grado de seguridad general que ofrece la aplicación?

No, ya que la aplicación es sensible a ataques.

Aspectos importantes por notar:

Positivos:

- Uso de un *firewall* perimetral e interno.
- Uso de servicio *outsourcing*.
- Servicio *Cloudflare*, *IPS* fijas.
- Basarse en normas *ISO/IEC* 270001.
- Capacitación constante al personal en incidentes informáticos.
- Varias personas en el área de sistemas.
- Existe al menos dos personas con acceso de administrador a las aplicaciones *web*.
- Plantear políticas de seguridad.
- Diseñar un plan de contingencia.
- Asignación de usuarios con perfiles con grado de responsabilidad de cada área.
- Respaldos diarios.
- Aplicación *web* solo de consultas.

Negativos:

- Desactualización de la plataforma.
- No hay exigencias en las contraseñas de usuario.
- Falta de personal especializado en determinadas áreas.
- Falta de presupuesto para capacitaciones en incidentes informáticos.
- Los respaldos, se almacenan en otro equipo y en *DVD*.
- Escaso personal en la unidad de tecnología del GAD Municipal de Tisaleo.
- No hay seguridad en la aplicación *web*.

2.4. Metodología para Auditoria de la Seguridad de la Información *OWASP*

Para el presente proyecto de investigación, se define en primer lugar, lo que representa *OWASP* (2019) como menciona en su propia página *web*, busca ofrecer soluciones y herramientas para crear, operar, desarrollar, mantener y asegurar aplicaciones para su mejoramiento continuo. Organización fundada en diciembre del 2001 y obtuvo en Estados Unidos un estatus de organización benéfica sin fines de lucro en 2004. "Es un gran recurso para el aprendizaje y la fijación de la seguridad de la aplicación *web*".

OWASP (2018) no está afiliado a ninguna compañía tecnológica, apoya el uso informado de tecnologías de seguridad, también, recomienda encaminar la seguridad de aplicaciones informáticas que considera todas sus dimensiones tales como personas, procesos y tecnologías.

Además, (Halton, Weaver, Ahmed, Rao, & Imran, 2017); (Coronado, 2017) concuerdan que los proyectos de *OWASP*, se dividen en dos categorías: el primero en proyectos de documentación y el segundo en proyectos de desarrollo los cuales, se detallan, a continuación:

Proyectos de Documentación

a) Guía *OWASP*: Documento que proporciona una guía detallada sobre seguridad de las aplicaciones *web*.
b) *OWASP TOP* 10: Documento de alto nivel, que se centró en las vulnerabilidades más críticas de las aplicaciones *web*.
c) Métricas: Proyecto para definir métricas aplicables de seguridad de aplicaciones *web*.

d) Legal: Un proyecto para ayudar a los vendedores y compradores de *software* a negociar de acuerdo con los aspectos de seguridad en sus contratos.
e) Guía de pruebas: Guía centrada en la prueba efectiva de la seguridad de aplicaciones *web*.
f) *ISO/IEC 27002*: Guía de buenas prácticas que describe los objetivos de control recomendables en cuanto a seguridad de la información.
g) *AppSec FAQ*: Preguntas y respuestas frecuentes sobre seguridad de aplicaciones *web*.

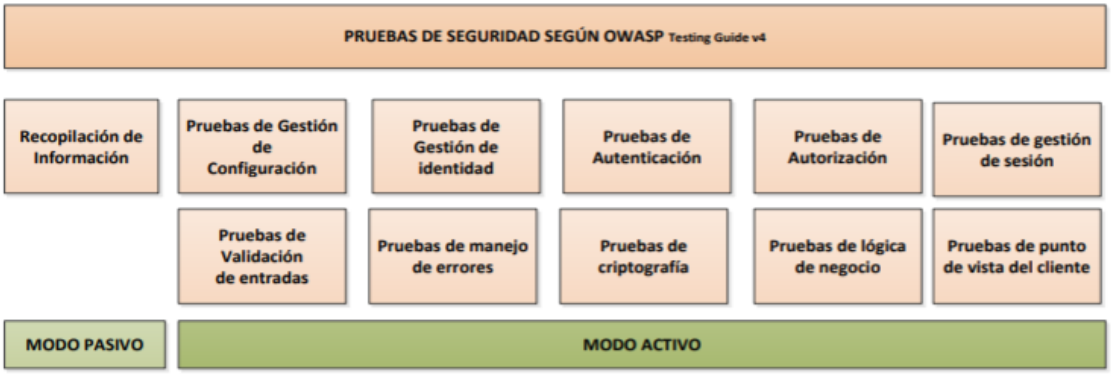
Proyectos de Desarrollo

a) *WebScarab*: Aplicación de chequeo de vulnerabilidades de aplicaciones *web* que incluyen herramientas *proxy*.
b) Filtros de validación (*Stringer* para *J2EE, filters* para *PHP*): Son filtros genéricos de seguridad perimetral que los desarrolladores usan en sus propias aplicaciones.
c) *WebGoat*: Herramienta interactiva de formación y *benchmarking* para que los usuarios aprendan sobre seguridad de aplicaciones *web* de forma segura y legal.
d) *DotNet*: Conjunto de herramientas para explorar y mejorar la seguridad en los entornos *NET*.

Según *OWASP* (2008) el desarrollar un *software* inseguro tiene graves consecuencias, las aplicaciones *web* están expuestas a miles de usuarios a través de *internet*, que representan una debilidad por parte de programador, da apertura a personas mal intencionadas a atacar dichas aplicaciones *web*.

Las pruebas de intrusión se dividen en dos fases, que se encuentran en la siguiente figura, representados como Modo Activo y Pasivo, en las que cada una maneja diferentes pruebas, que se encuentran sobre las fases especificadas.

Figura 1. Fases de las Pruebas de Seguridad OWASP



Fuente: Mora Ortega (2017)

A continuación, se describe a breves rasgos las fases de la metodología de desarrollo, por lo cual, se tomó en consideración la guía de desarrollo que aporta *Open Web Application Security Project (OWASP)* (2017) en su sitio *web* que permite visualizar las mismas y sin costo alguno; a continuación, se detalla las fases:

Fase I – Recolección de Información

En esta fase, se recolecta información mediante un análisis al servidor, en dicha fase ,se determina quién fue la víctima, el presente análisis establece qué recursos, se encuentran habilitados y enlistados para posterior ser explotados.

Además, se realiza un análisis a la infraestructura de la aplicación *web* que resulta muy necesario, es un pilar fundamental dentro de la seguridad, pero un simple error de configuración provocaría una pérdida total de datos del GAD Municipal de Tisaleo.

Fase II – *Test* de Manejo de Configuración y Desarrollo

Dentro de la segunda fase, se realiza una prueba que determina las herramientas administrativas que manejan los contenidos de la aplicación para establecer las configuraciones adecuadas para cada una, así mismo, muchas veces un mínimo error conlleva a mayores riesgos de seguridad. También, se identificó las extensiones de los archivos que manejan información sensible, así como, se hizo una revisión de los archivos viejos y *backups* del GAD Municipal de Tisaleo.

Fase III – *Test* de Manejo de Identidad

En la fase de pruebas de manejo de identidad, se detalla los roles que el sistema maneja, es imprescindible saber a qué información accede cada usuario, qué es modificable, y si los cambios afectan a otra información. Además, se visualiza cómo es el proceso de creación de nuevos usuarios y nuevas cuentas, igualmente la forma de otorgar roles y permisos para el correcto funcionamiento de la aplicación *web*.

Fase IV – *Test* de Autenticación

La autenticación dentro de la aplicación *web* es necesaria, en todas las cuentas pasan por un filtro de verificación para comprobar que existen en la base de datos y así acceder a su perfil. Así mismo, la encriptación de datos es necesaria porque un ataque, se realiza con un análisis completo de la red e intervenir en las peticiones, que se realizan hacia la aplicación *web*.

También, se aplica una prueba al mecanismo de cierre de sesión, que se refiere a un ataque de fuerza bruta, existe el suceso donde cabe la posibilidad que se vulnere la aplicación, después de generar un número determinado de intentos de acceso, se podrá ingresar con credenciales generadas en dicho ataque.

Fase V – *Test* de Manejo de Sesiones

Una prueba de manejo de sesiones se lleva a cabo de la siguiente forma, se verifica en las computadoras del GAD Municipal de Tisaleo, los navegadores guardan las *cookies* y con una correcta configuración de estas, se las bloquea. También, se realiza una prueba a la funcionalidad de cierre de sesiones, se identifica si hay usuarios activos, y prevenirlos de ataques.

Fase VI – *Test* de Validación de Entradas

Las validaciones de entradas son más comunes por un fallo de la validación de datos del cliente, dichas vulnerabilidades llevan a grandes riesgos de seguridad de un sistema tal como inyecciones de código, ataques de sistema o sobrecarga de *buffer*. Por esta razón el realizar una prueba de validación de entradas es fundamental, una falsificación de una

página por parte de un atacante para obtener las credenciales sucede muy con gran frecuencia.

Fase VII – *Test* de Manejo de Errores

La prueba de manejo de errores es el momento en, que se hace un análisis de riesgos hacia un sitio o aplicación *web*, existe la posibilidad que la causa de equivocaciones sea mediante solicitudes específicas, estas faltas son muy importantes para el analista debido a que los mismos revelan considerable información acerca de la base de datos, errores y componentes tecnológicos afines a dicha aplicación *web*.

Fase VIII - *Test* del Lado del Cliente

Las pruebas del lado del cliente se ocupan en la ejecución del código en el mismo, con regularidad de forma nativa desde un navegador *web* o algún complemento del navegador. Dicha ejecución del código es distinta de la ejecución del servidor, se hizo inyecciones *SQL, HTML y JavaScript* que es un subtipo de *Cross Site Scripting - XSS*, redireccionamiento de *URL*, manipulaciones de recursos por parte del cliente, entre otras más.

2.5. Lista de Herramientas

1. Navegadores (*Google Hacking* y *Firefox for Developers*)
2. Máquinas Virtuales (*Oracle VM VirtualBox* y *VMware Workstation*)
3. Sistemas Operativos (*Kali Linux y Microsoft Windows XP, 7, 10*)
4. *Netcraft*
5. *VirusTotal*
6. *Name System Lookup set type = A*
7. *Name System Lookup set type = any*
8. *Whois*
9. *Network Mapper*
10. *FOCA*
11. *OWASP ZAP*
12. *Whatweb*
13. *Joomscan*

14. Crunch

15. Hydra

CAPÍTULO III. RESULTADOS Y VALIDACIÓN

En el presente capítulo, se puntualiza los resultados obtenidos a través de la metodología para Auditoria de la Seguridad de la Información *OWASP*, como menciona *OWASP* (2019) en su sitio web; la metodología esta divida en diferentes pruebas a modo de fases, pero para el presente tema de estudio algunas de las pruebas no fueron utilizadas, a continuación, se detalla las pruebas y las respectivas razones por la que, no se utilizaron:

- Introducción y Objetivos: se encuentran explicados en el Capítulo 1 de este documento.
- *Test* de Autorización: Al ser pocos usuarios en la Unidad de Tecnología del tema de estudio esto, se contempla en la entrevista realizada al jefe de la unidad y, además, esta explicado en el análisis de roles del sitio de administración.
- *Test* de Criptografía Débil: Al ser una entidad gubernamental que maneja un sitio web mientras, se usa un cifrado *SSL*, la prueba es irrelevante al ser un conocimiento empírico.
- *Test* del Lado del Cliente: Se encuentra explicado en la prueba de *Cross Site Scripting* y en la inyección de *SQL* al no haber sido explotados con éxito, quiere decir que el sitio está protegido en contra de ataques del lado del cliente por lo que, no se continuaron con otras pruebas al considerarlos irrelevantes.

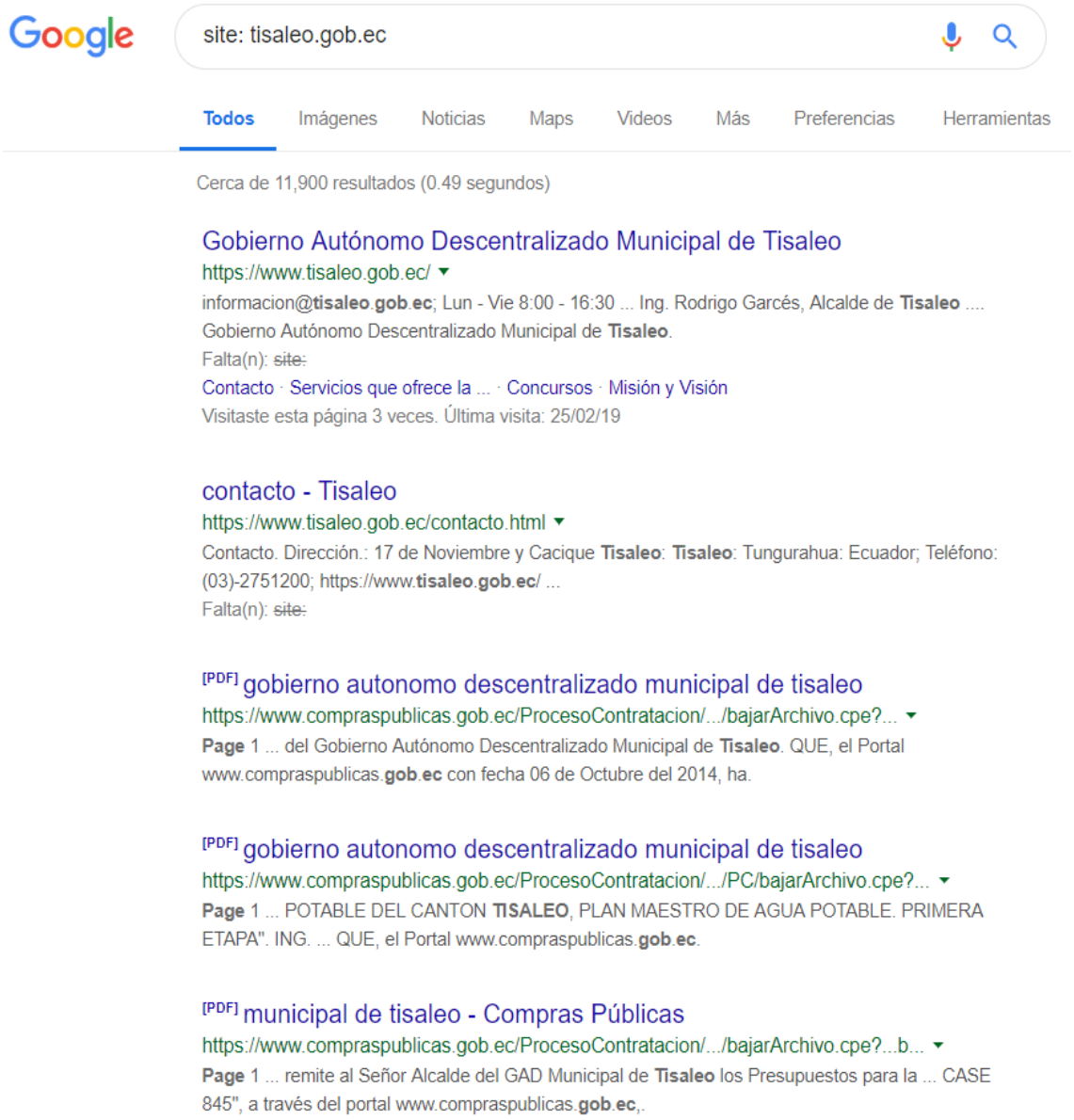
3.1. Desarrollo de la Metodología *OWASP*

3.1.1. Fase I – *Test* de recolección de Información

Uso de un motor de búsqueda para verificación de existencia de información vulnerable

Algunos de los elementos directos o indirectos son obtenidos mediante un motor de búsqueda, si dicha aplicación no contiene una configuración adecuada que resguarde los mismos; por ejemplo, los elementos directos hacen referencia a los índices de búsqueda, por otro lado, los elementos indirectos representan información sensible que se utiliza para una explotación.

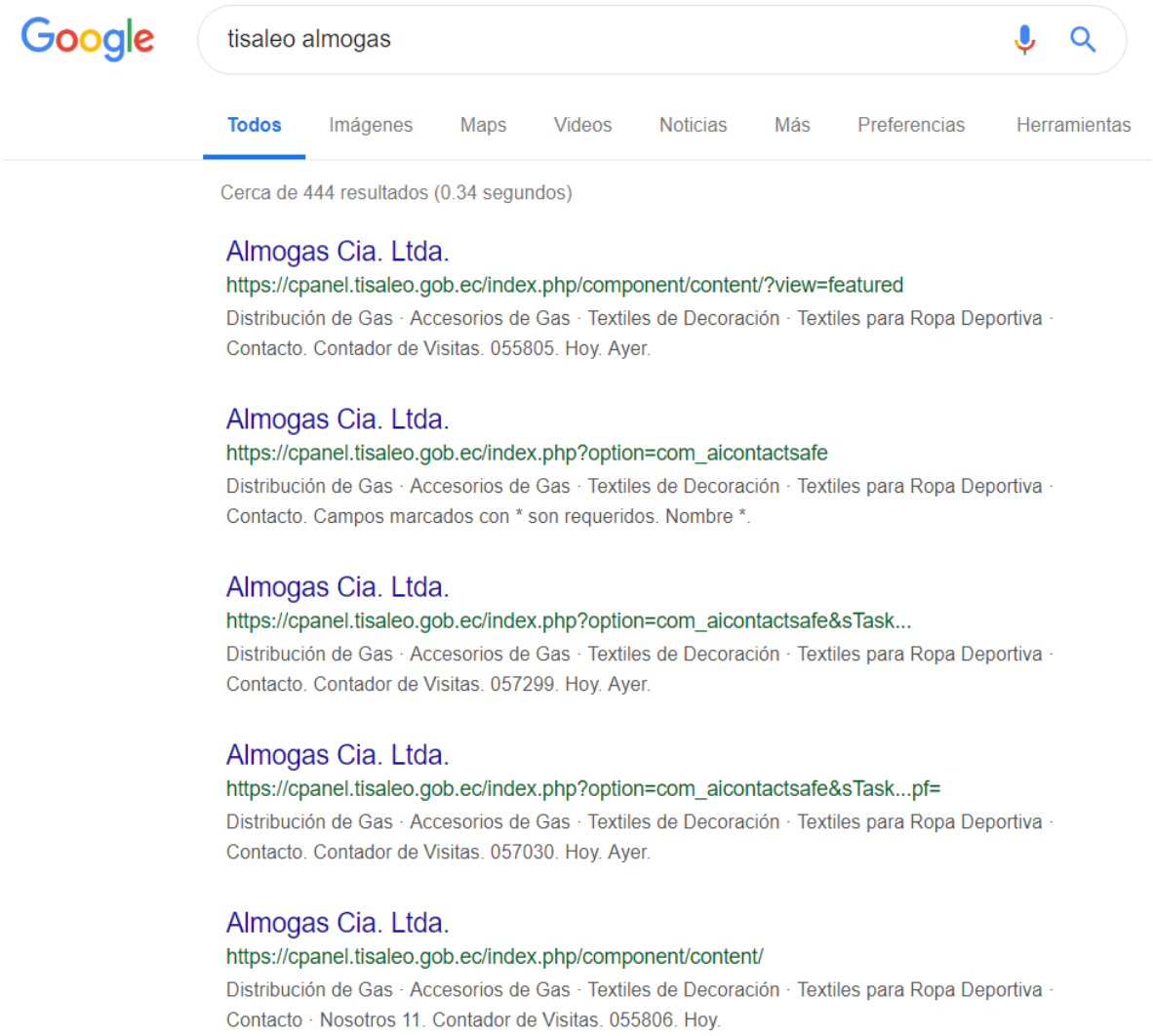
Figura 2. Resultados de la búsqueda del sitio web en Google (1)



Fuente: elaboración Propia

En las primeras páginas de búsqueda como, se puede ver en la imagen anterior, se encontró información pública, la cual no es de mucha utilidad en la presente investigación, pero en páginas posteriores, se encontró una página llamada: Almogas la cual es sospechosa, por dicha razón, se realizó la búsqueda en *Google* y como, se puede ver en la siguiente imagen, dicha página tiene acceso al *Cpanel*:

Figura 3. Resultados de búsqueda del sitio web en Google (2)

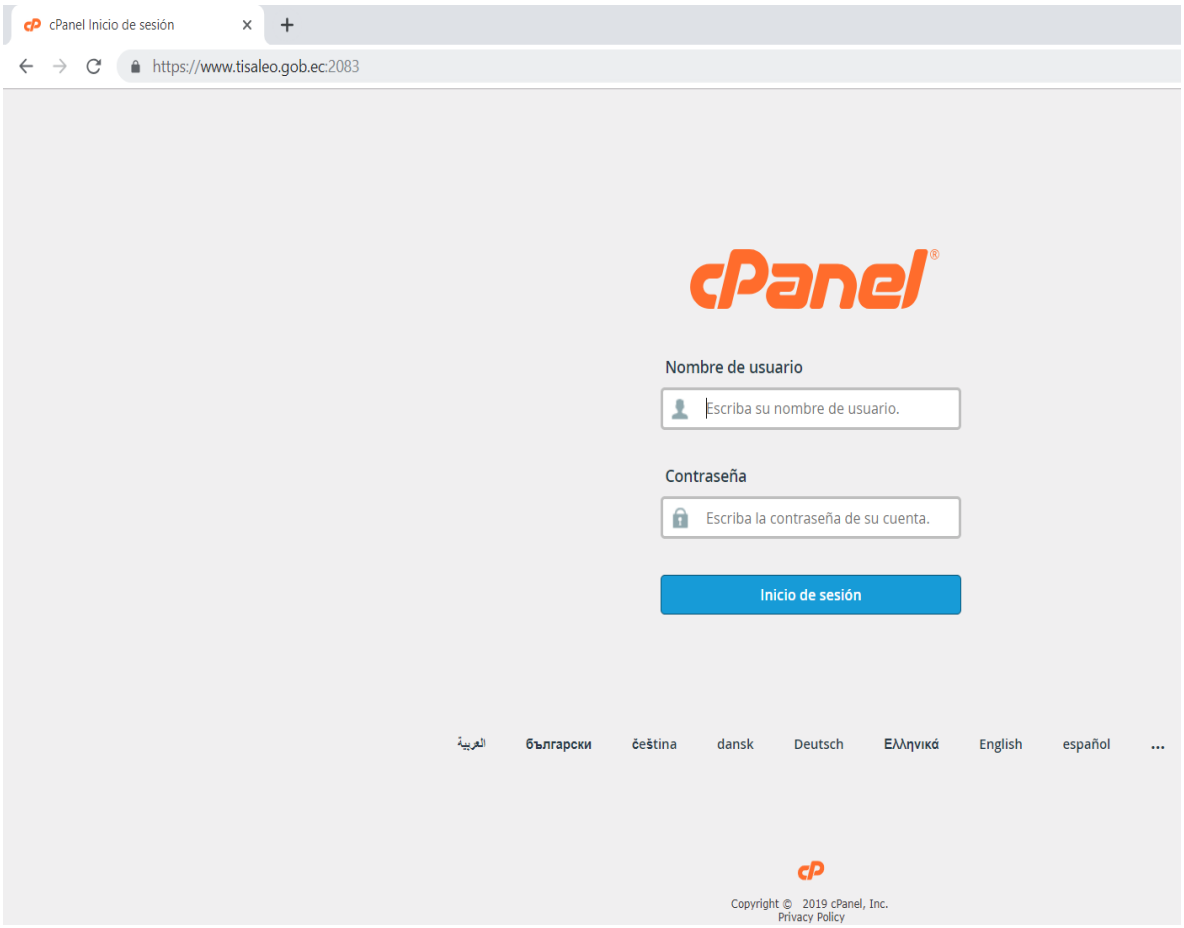


Fuente: elaboración propia

Además, después de la anterior búsqueda en las próximas páginas, se encontró importante información como lo siguiente:

Primero, se visualizó el sitio *web* del GAD Municipal de Tisaleo, junto, se pudo ver el puerto *2083* que pertenece al servicio de *Cpanel* sobre *SSL*, el mismo compromete la información sensible que contiene el sitio web del GAD Municipal de Tisaleo.

Figura 4. Servicio de Cpanel sobre SSL

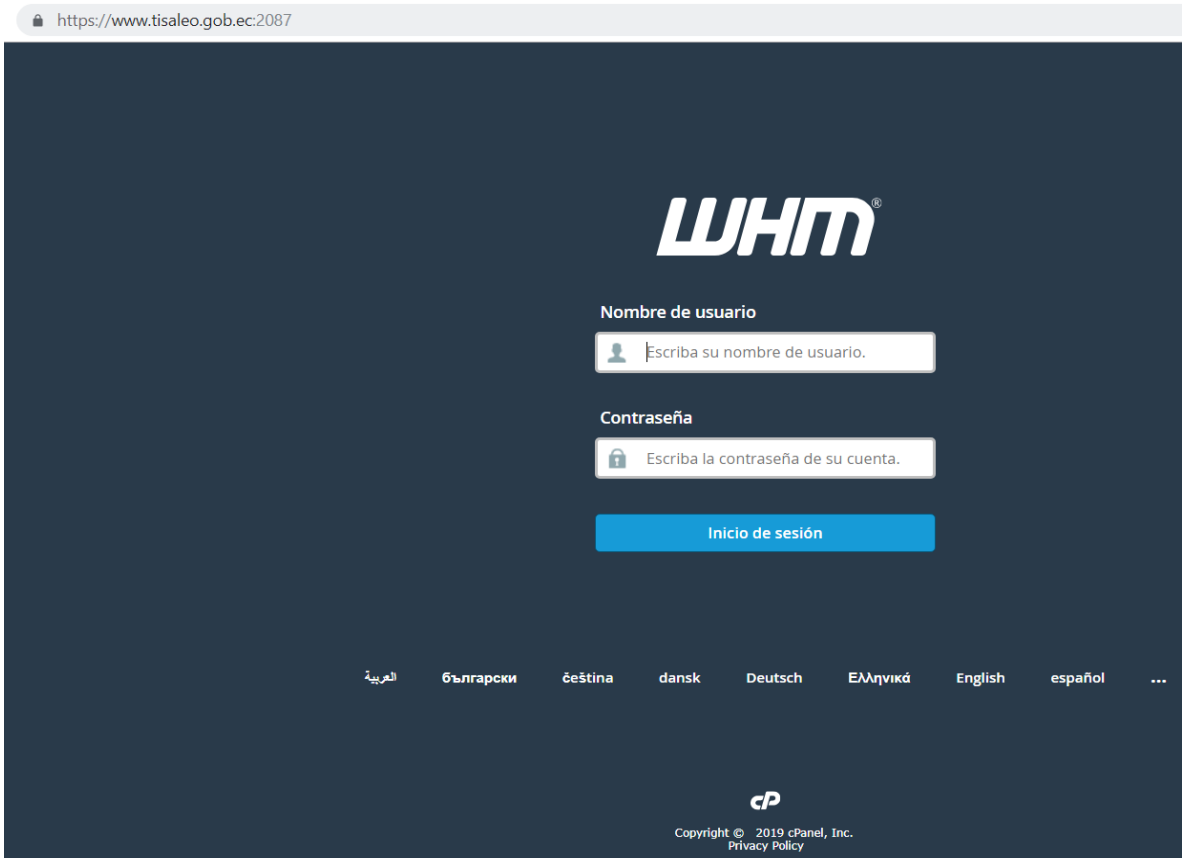


Fuente: elaboración propia

En la imagen anterior, se puede observar que, en la *URL*, se presenta el puerto al, que se dirige la consulta, puesto que pertenece a un servicio de *web hosting* que requiere autenticación de usuario y contraseña para proceder al ingreso en dicho servicio.

Así mismo, como, se puede apreciar en la captura de pantalla de continuación, se encuentra una dirección similar a la anterior, con facilidad, se cambia el puerto que sería el *2087*, el cual pertenece a un servicio *de Cpanel WebHost Manager* sobre *SSL*, que también, necesita de autenticación.

Figura 5. Servicio de Cpanel WebHost Manager sobre SSL

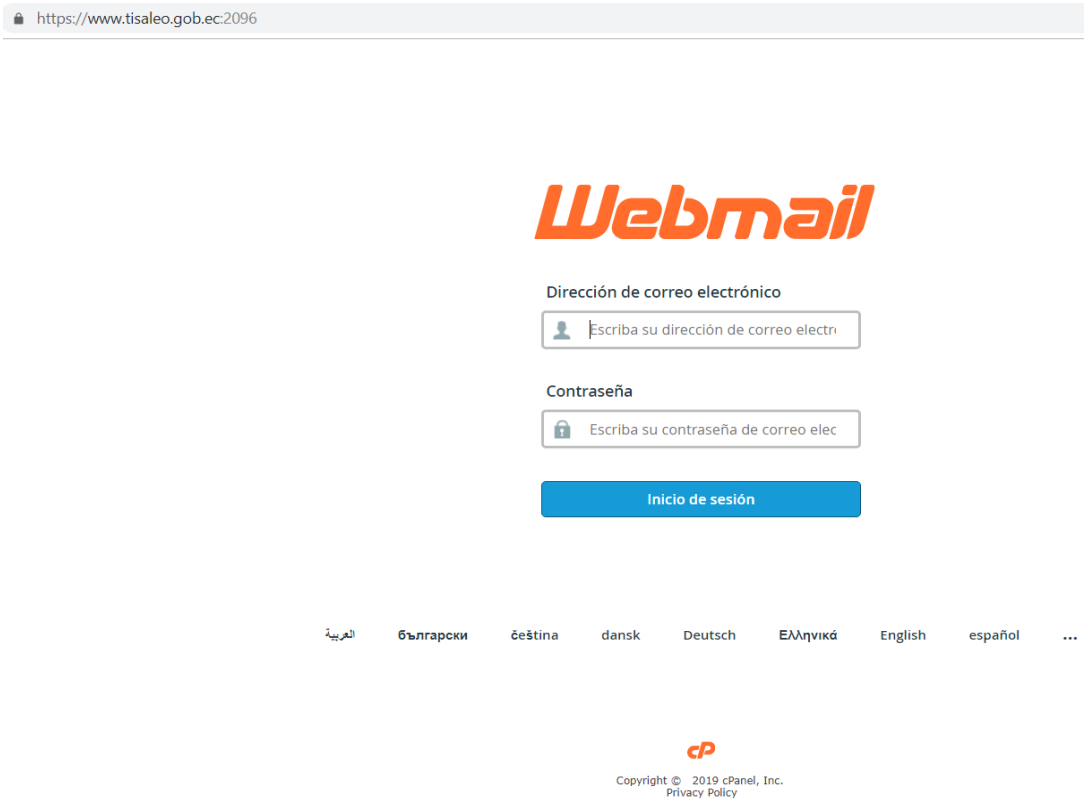


Fuente: elaboración propia

También, se encontró, el servicio de correo electrónico, el cual tenía asignado el puerto *2096*, dicho servicio, además, necesita de un usuario y contraseña para ingresar a dicho servicio.

Además, dicho riesgo incrementa, el dejar el servicio por defecto es una grave vulnerabilidad para el GAD Municipal de Tisaleo, porque los correos institucionales y gubernamentales que, por medio de un ataque es posible, que se acceda a ellos con resultados las credenciales para ingresar a dicho servicio.

Figura 6. Cpanel WebMail sobre SSL



Fuente: elaboración propia

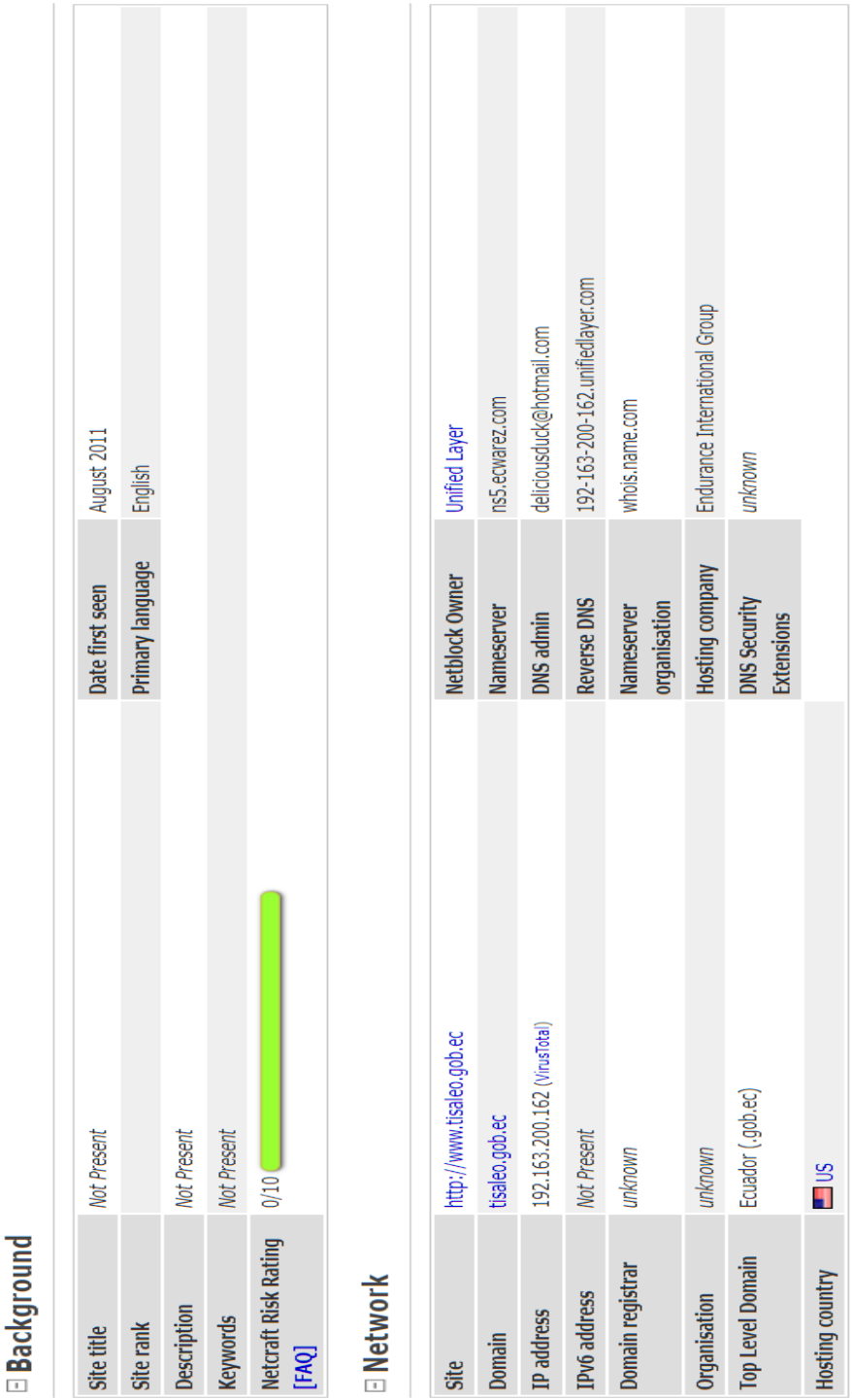
Con lo, que se concluye que existe un proceso el cual, se corrige y tiene referencia al sitio *web* del GAD Municipal de Tisaleo el cual dirige un puerto especifico, se proporciona una pauta para focalizar su intrusión hacia los puertos, que se encuentran abiertos.

Análisis general de las aplicaciones *web*

Se conoce el servidor que va a ser atacado, está es una etapa crítica en el proyecto puesto que ahí, se encuentra el que posterior será la víctima, de esta forma, se conocerá las características y tipo de sitio y servidor. Obtener el conocimiento de la *IP*[1] del sitio web a ser atacado y el servidor que lo maneja es fundamental en primera instancia para proceder, se utilizará la herramienta *Netcraft*[2], la misma que proporciona información básica del sitio *web*.

[1] *Protocolo de Internet (IP*): Es un estándar, que se utiliza para él envió y recepción de información mediante una red que reúne paquetes transformados.
[2] *Netcraft:* Servicio de internet el cual es utilizado para obtener información completa de una aplicación web, así mismo, tiene otras características como prestador de servicios anti-phishing, hosting, auditorias de seguridad informática y entre otras soluciones a nivel de redes.

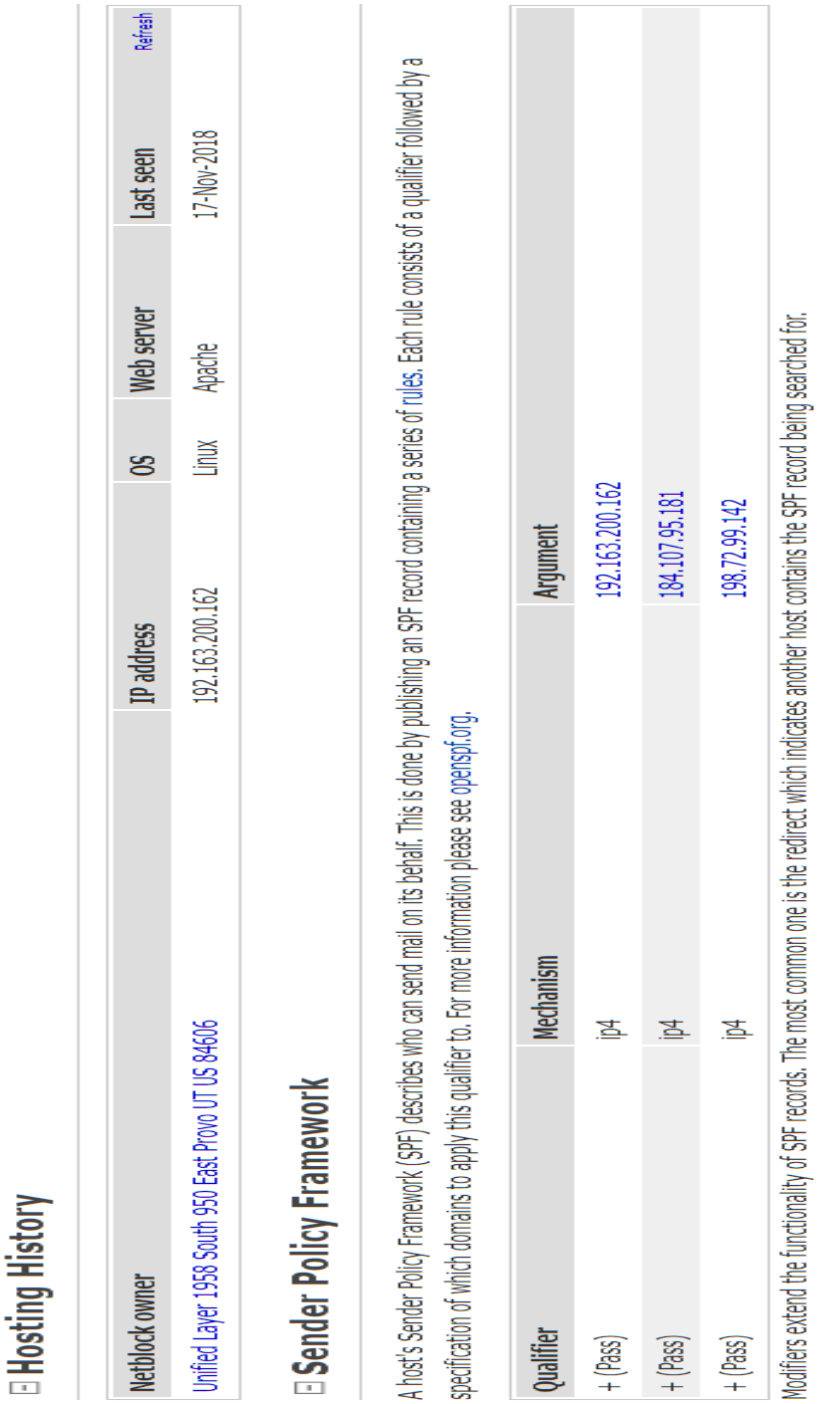
Figura 7. Información de Netcraft del dominio del sitio web del GAD Municipal de Tisaleo (1)



Fuente: elaboración propia

Como, se puede observar en la figura 7 la herramienta *Netcraft* demostró información varia del servidor del GAD Municipal de Tisaleo tal como el sistema operativo, el servidor *web*, el mecanismo (*IP4*), además, de mostrar el *VirusTotal.*

Figura 8. Información de Netcraft del dominio del sitio web del GAD Municipal de Tisaleo (2)



Hosting History

Netblock owner	IP address	OS	Web server	Last seen	Refresh
Unified Layer 1958 South 950 East Provo UT US 84606	192.163.200.162	Linux	Apache	17-Nov-2018	

Sender Policy Framework

A host's Sender Policy Framework (SPF) describes who can send mail on its behalf. This is done by publishing an SPF record containing a series of rules. Each rule consists of a qualifier followed by a specification of which domains to apply this qualifier to. For more information please see openspf.org.

Qualifier	Mechanism	Argument
+ (Pass)	ip4	192.163.200.162
+ (Pass)	ip4	184.107.95.181
+ (Pass)	ip4	198.72.99.142

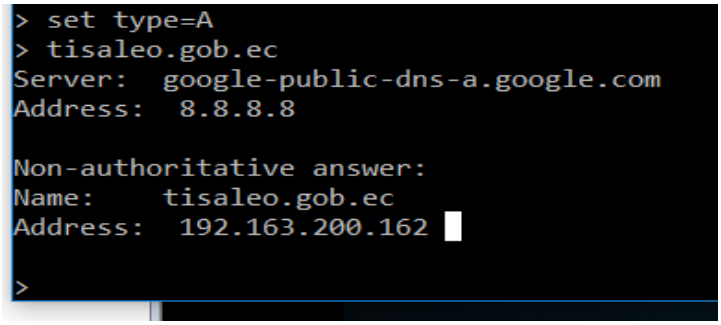
Modifiers extend the functionality of SPF records. The most common one is the redirect which indicates another host contains the SPF record being searched for.

Fuente: elaboración propia

La herramienta *Virus Total* indica el lugar donde, se aloja el sitio, exhibe *URL* sospechosas que contienen caracteres que no contengan propósitos maliciosos. En este caso, se pudo ver un análisis de todas las páginas que han tenido algún contacto con el sitio *web* del GAD Municipal de Tisaleo.

Por otro lado, la herramienta *Name System Lookup*[3] que sirve para visualizar información sobre el sitio *web*, por lo cual, se utilizó para mostrar la dirección *IP* del sitio *web* del tema de estudio en el cual, se utiliza el comando *set type=A*, la a mayúscula sirve para mostrar dicha información.

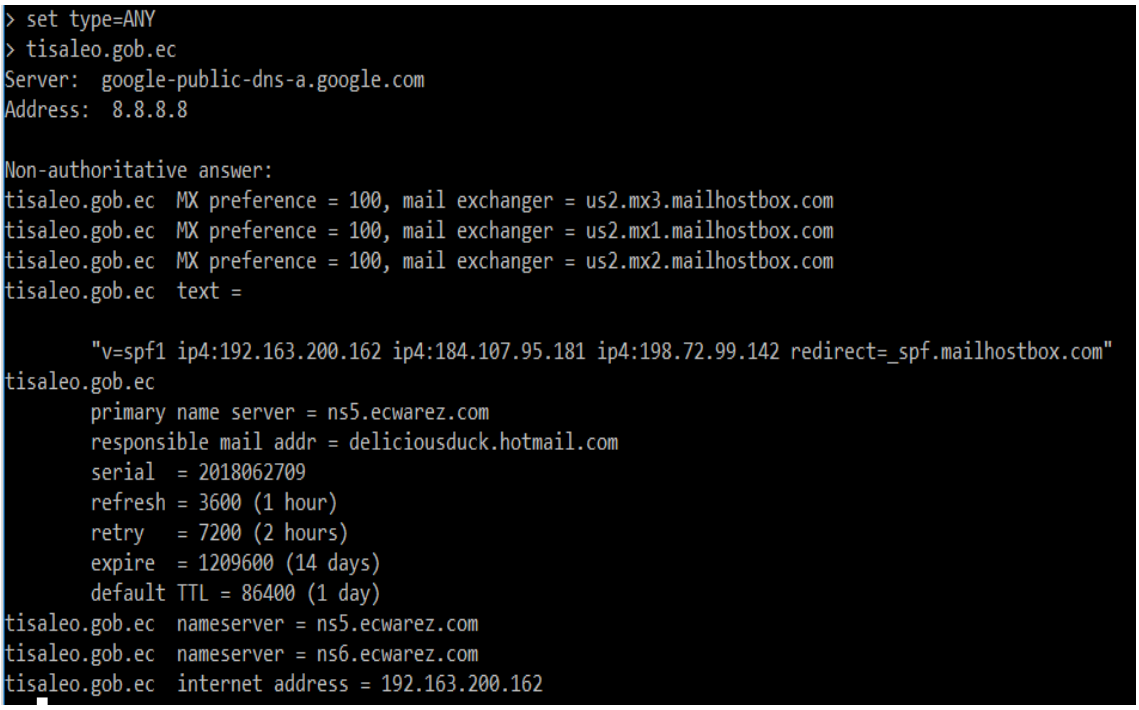
Figura 9. Información de la herramienta nslookup set type =A



Fuente: elaboración propia

Sin embargo, existen otras instrucciones que son útiles en la presentes investigación, como, por ejemplo, el comando *ANY* que fue de utilidad para encontrar otros servicios que están alojados en el sitio *web* con sus respectivas direcciones *IP*.

Figura 10. Información de la herramienta nslookup set type = any



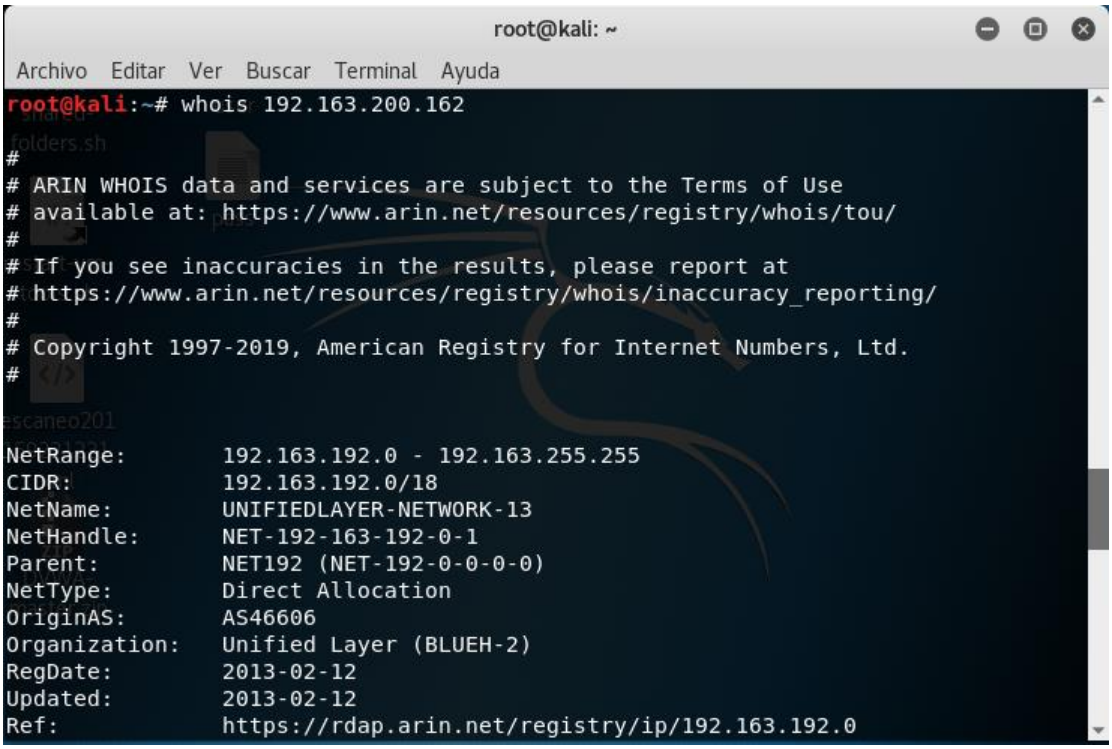
[3] *Name System Lookup (Nslookup):* Herramienta que permite consultar un servidor de nombres y obtener información del dominio, *host* y, además, diagnosticar los problemas de configuración con el *DNS*.

Fuente. elaboración propia

Kali Linux es una distribución de *Linux* basada en *Debian* destinada para pruebas de penetración y auditoria de seguridad. Además, contiene más de 600 herramientas que están orientadas a diversas tareas de seguridad de la información, como pruebas de penetración, investigación de seguridad informática, forense e ingeniería inversa. Desarrollado, financiado y mantenido por *Offensive Security* empresa líder en capacitación en seguridad de la información.

Luego de haber obtenido la *IP* de la aplicación *web,* se procede a realizar una consulta, mediante la instrucción *whois* [4] en *Kali Linux*, para verificar.

Figura 11. Respuesta del servidor acerca de la consulta whois

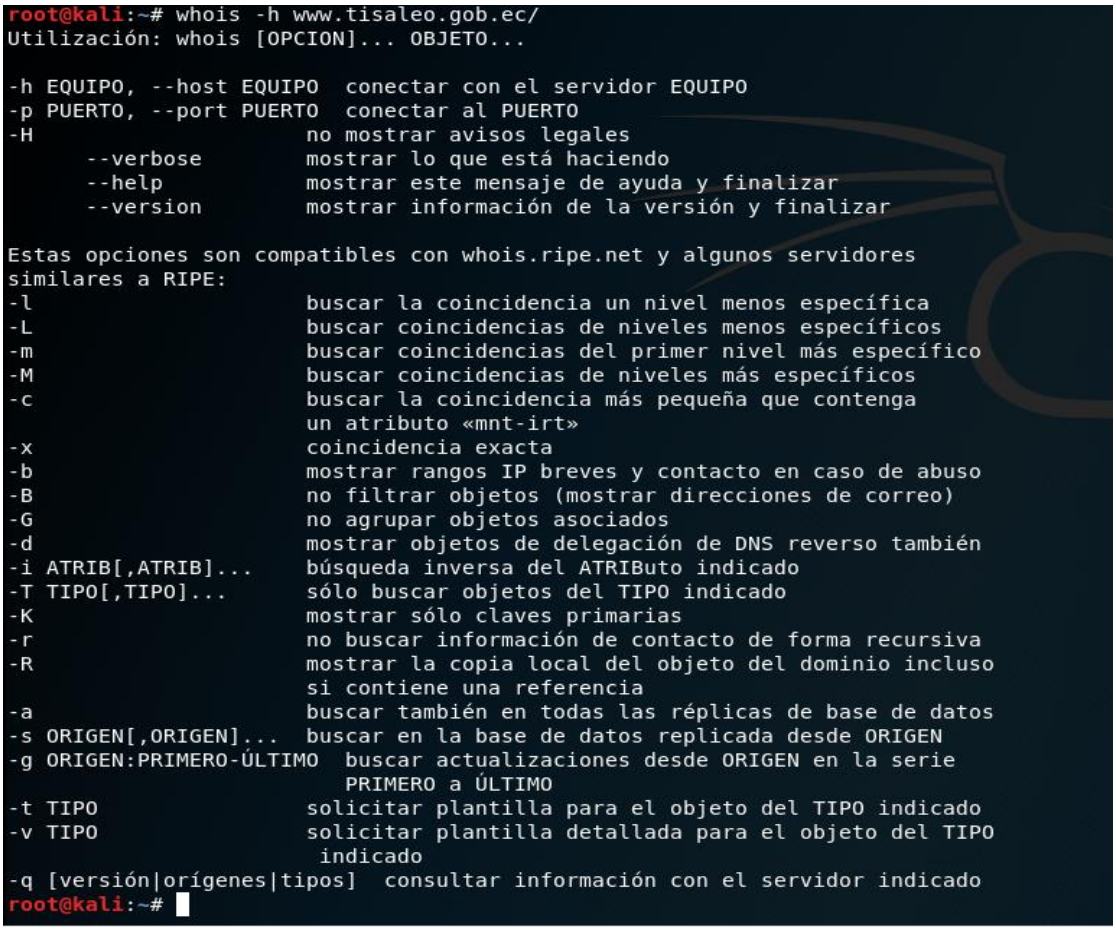


Fuente: elaboración propia

Así mismo, se continuo con el comando *-h* el cual permite definir al host quien realiza la conexión para hacer consultas de un dominio. Como podemos ver en la respuesta, se obtiene los registros de la primera fuente del mismo.

[4] *Whois:* Nombre para un servicio y herramienta *TCP*, y de cierta manera una base de datos, que contiene información acerca del nombre del servidor de un dominio y más información.

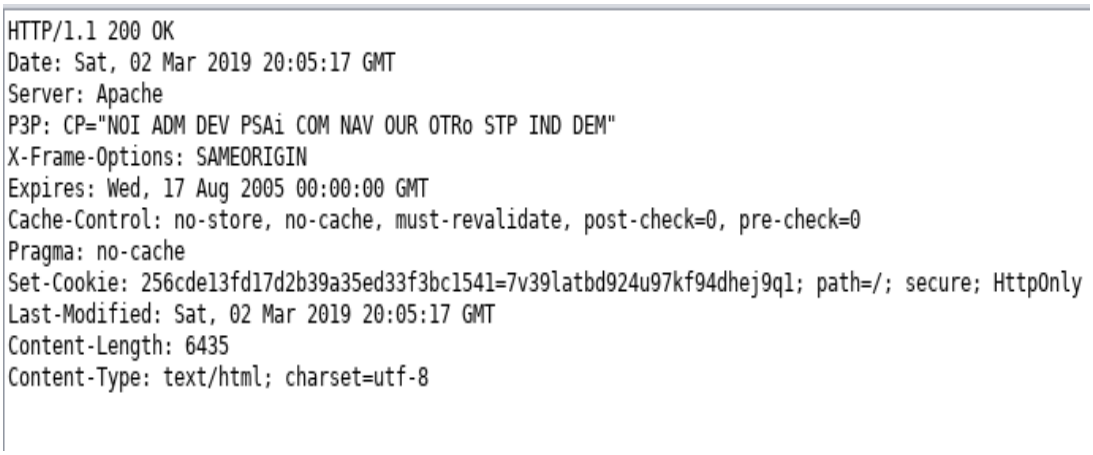
Figura 12. Respuesta del servidor acerca de la consulta whois -h



Fuente: elaboración propia

Posterior, se procedió a realizar una consulta a las cabeceras de la aplicación web para obtener información sobre el mismo.

Figura 13. Respuesta de consulta de cabecera del sitio web del GAD Municipal de Tisaleo



Fuente: elaboración propia

El resultado obtenido como, se ve en la figura 13, en la cual, se nota varias características, que se utiliza para un ataque.

Figura 14. Respuesta de consulta de cabecera de la ampliación web del GAD Municipal de Tisaleo (1)

Fuente: elaboración propia

De esta manera, algunos de los resultados obtenidos en las cabeceras obtenidos como, se puede ver las capturas de pantalla anterior fueron valiosa información para los fines pertinentes, tales como:

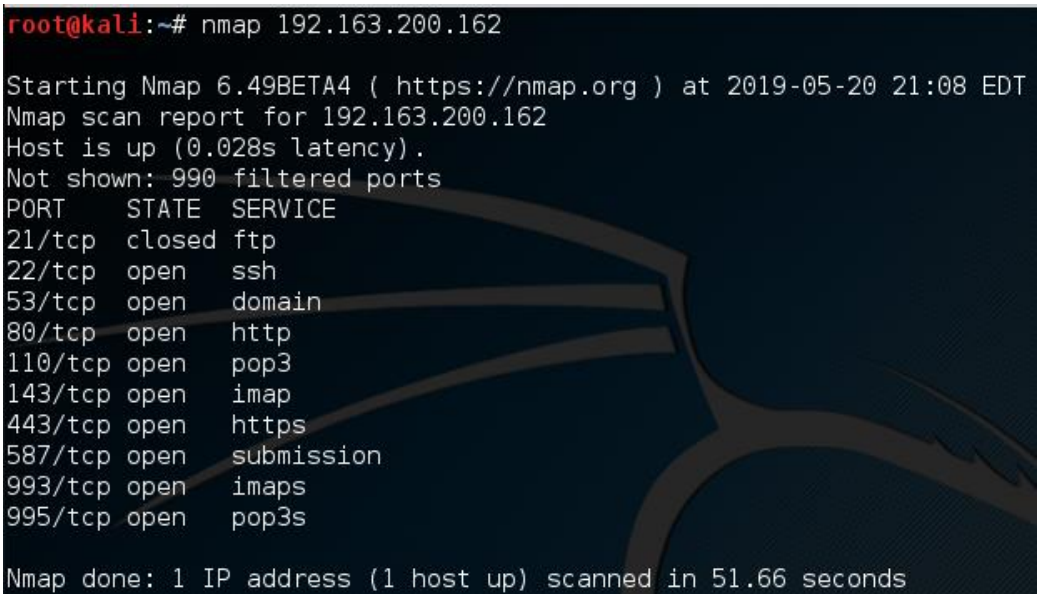
- Direcciones *IP* de los servidores
- Direcciones de los proveedores
- Nombre del servidor
- Herramientas de funcionamiento y sus versiones
- Contactos de proveedores y administradores
- Sistema Operativo del servidor

Para finalizar, se utilizó la herramienta *Network Mapper (Nmap)*[5] en la cual, se ve los puertos abiertos y cerrados que contiene el sitio *web*, la mayoría de los puertos son

[5] *Nmap:* comando utilizado para escanear host y servicios dentro de una red, con el tiempo ha evolucionado y ahora, se usa para descubrir las aplicaciones a más de los servicios y los sistemas operativos de los servidores de la red.

utilizados para correo electrónico, pero el puerto *22 ssh* [6] sirve para acceder de forma remota al servidor a través de una red, manejar por completo el sistema mediante comandos, además, se obtiene copiar datos y algo muy importante en este puerto es en donde, se consigue realizar los ataques por fuerza bruta o denegación de servicios.

Figura 15. Respuesta del servidor acerca de la consulta Nmap



Fuente: elaboración propia

Recolección de metadatos del sistema para la comprobación de existencia de información vulnerable

Por la presente prueba, se analiza que el archivo *robots.txt* y al archivo *htaccess.txt* con el fin de encontrar información acerca de las carpetas y características básicas existentes dentro del servidor respectivo y comprobar si existe la posibilidad de acceder a archivos de información sensible de los mismos.

El encontrar las direcciones de carpetas, así como la creación de una lista de directorios que son usados para sobrepasar las seguridades de la aplicación *web*.

[6] *SSH – Secure Shell*: protocolo que facilita las comunicaciones seguras entre dos sistemas que utilizan una arquitectura cliente/servidor, que permite a los usuarios conectarse a un *host* remoto.

Para comenzar, se ingresa a la siguiente *Uniform Resource Locator*[7] http://www.tisaleo.gob.ec/robots.txt en donde se encuentra la información, que se puede visualizar en la siguiente captura de pantalla:

Figura 16. Archivo robots.txt de la página web del GAD Municipal de Tisaleo (1)

```
# If the Joomla site is installed within a folder such as at
# e.g. www.example.com/joomla/ the robots.txt file MUST be
# moved to the site root at e.g. www.example.com/robots.txt
# AND the joomla folder name MUST be prefixed to the disallowed
# path, e.g. the Disallow rule for the /administrator/ folder
# MUST be changed to read Disallow: /joomla/administrator/
#
# For more information about the robots.txt standard, see:
# http://www.robotstxt.org/orig.html
#
# For syntax checking, see:
# http://tool.motoricerca.info/robots-checker.phtml

User-agent: *
Disallow: /administrator/
Disallow: /bin/
Disallow: /cache/
Disallow: /cli/
Disallow: /components/
Disallow: /includes/
Disallow: /installation/
Disallow: /language/
Disallow: /layouts/
Disallow: /libraries/
Disallow: /logs/
Disallow: /modules/
Disallow: /plugins/
Disallow: /tmp/
```

Fuente: elaboración propia

[7] *Uniform Resource Locator (URL):* Es una secuencia de caracteres que sigue un estándar y que permite denominar recursos dentro del entorno de internet para que los usuarios puedan localizarla en un navegador, que, además, muestra información.

Figura 17. Archivo htaccess.txt de la página web del GAD Municipal de Tisaleo (2)

https://www.tisaleo.gob.ec/htaccess.txt

```
##
# @package    Joomla
# @copyright  Copyright (C) 2005 - 2018 Open Source Matters. All rights reserved.
# @license    GNU General Public License version 2 or later; see LICENSE.txt
##

##
# READ THIS COMPLETELY IF YOU CHOOSE TO USE THIS FILE!
#
# The line 'Options +FollowSymLinks' may cause problems with some server configurations.
# It is required for the use of mod_rewrite, but it may have already been set by your
# server administrator in a way that disallows changing it in this .htaccess file.
# If using it causes your site to produce an error, comment it out (add # to the
# beginning of the line), reload your site in your browser and test your sef urls. If
# they work, then it has been set by your server administrator and you do not need to
# set it here.
##

## No directory listings
<IfModule autoindex>
  IndexIgnore *
</IfModule>

## Can be commented out if causes errors, see notes above.
Options +FollowSymlinks
Options -Indexes

## Mod_rewrite in use.

RewriteEngine On

## Begin - Rewrite rules to block out some common exploits.
# If you experience problems on your site then comment out the operations listed
# below by adding a # to the beginning of the line.
# This attempts to block the most common type of exploit `attempts` on Joomla!
#
# Block any script trying to base64_encode data within the URL.
RewriteCond %{QUERY_STRING} base64_encode[^(]*\([^)]*\) [OR]
# Block any script that includes a <script> tag in URL.
RewriteCond %{QUERY_STRING} (<|%3C)([^s]*s)+cript.*(>|%3E) [NC,OR]
# Block any script trying to set a PHP GLOBALS variable via URL.
RewriteCond %{QUERY_STRING} GLOBALS(=|\[|\%[0-9A-Z]{0,2}) [OR]
# Block any script trying to modify a _REQUEST variable via URL.
RewriteCond %{QUERY_STRING} _REQUEST(=|\[|\%[0-9A-Z]{0,2})
# Return 403 Forbidden header and show the content of the root home page
RewriteRule .* index.php [F]
#
```

Fuente: Elaboración propia

Se halló información en el archivo *htacceess.txt* sobre las configuraciones básicas del servidor, dicho archivo, se modifica, con un ataque, se revisa que contiene y que no, lo que resultaría muy perjudicial para el GAD Municipal de Tisaleo, el dejar expuesta esta información da paso a que, se vulnere la información sensible del mismo.

Figura 18. Archivo htaccess.txt de la página web del GAD Municipal de Tisaleo (3)

```
## End - Rewrite rules to block out some common exploits.

## Begin - Custom redirects
#
# If you need to redirect some pages, or set a canonical non-www to
# www redirect (or vice versa), place that code here. Ensure those
# redirects use the correct RewriteRule syntax and the [R=301,L] flags.
#
## End - Custom redirects

##
# Uncomment the following line if your webserver's URL
# is not directly related to physical file paths.
# Update Your Joomla! Directory (just / for root).
##

# RewriteBase /

## Begin - Joomla! core SEF Section.
#
RewriteRule .* - [E=HTTP_AUTHORIZATION:%{HTTP:Authorization}]
#
# If the requested path and file is not /index.php and the request
# has not already been internally rewritten to the index.php script
RewriteCond %{REQUEST_URI} !^/index\.php
# and the requested path and file doesn't directly match a physical file
RewriteCond %{REQUEST_FILENAME} !-f
# and the requested path and file doesn't directly match a physical folder
RewriteCond %{REQUEST_FILENAME} !-d
# internally rewrite the request to the index.php script
RewriteRule .* index.php [L]
#
## End - Joomla! core SEF Section.
```

Fuente: elaboración propia

A continuación, se observa el resultado, que se obtuvo a través de la información expuesta en el archivo *robots.txt* el cual fue de gran utilidad, se consiguió ingresar a la herramienta de creación de *webs Joomla* tal como, se ve en la figura, a continuación.

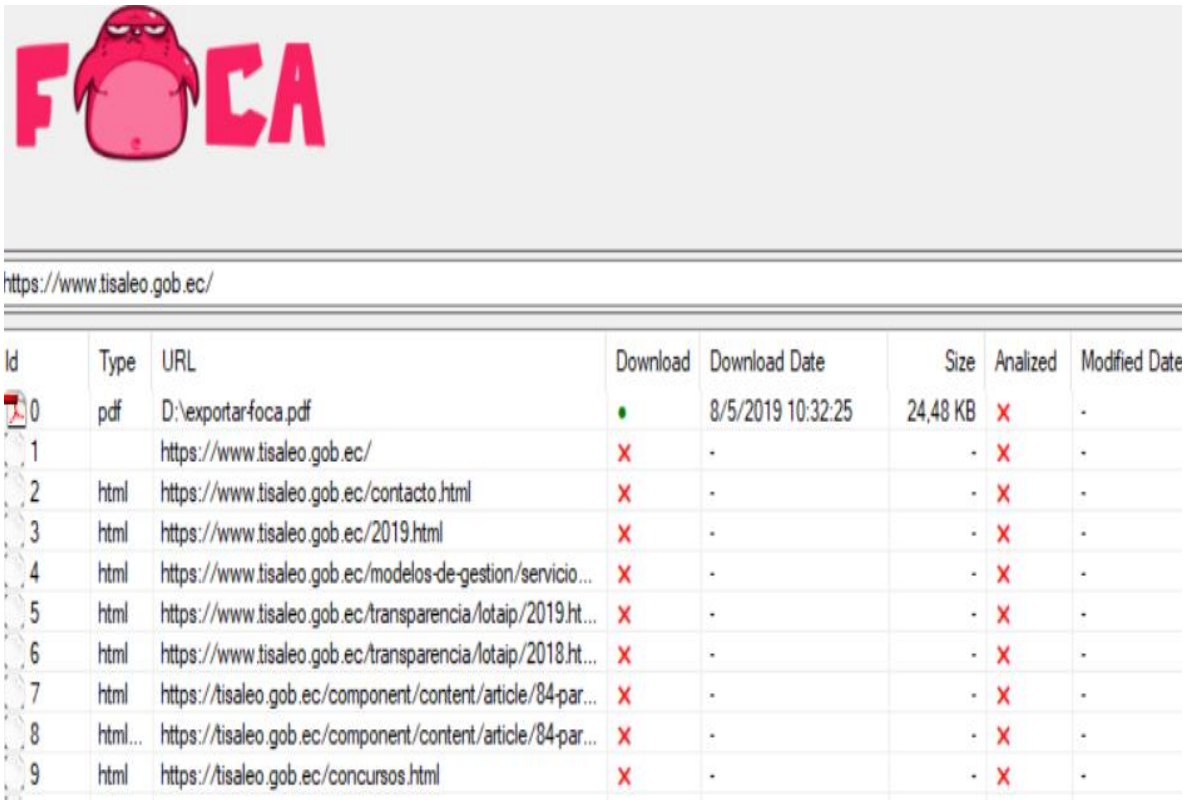
Figura 19. Resultado del archivo robots.txt/administrator/

Fuente: elaboración propia

El presente análisis da a notar, que se pudo comprobar que la mayoría de los recursos están deshabilitados, excepto uno que permite ingresar a la página de administrador de *Joomla*[8], con un análisis a las mismas, se encontró dicho recurso, que posterior fue explotado para la presente investigación.

Luego de probar otra herramienta para búsqueda de metadatos[9], *FOCA*[10], en la cual los resultados encontrados fueron los siguientes: no existe ninguna vulnerabilidad por parte de los metadatos alojados en el sitio *web*, por lo, que se concluye que este es un gran punto a favor para el GAD Municipal de Tisaleo, por medio de los metadatos, se encontró valiosa información la misma que pone en riesgo a las diferentes aplicaciones internas y externas que operan en el GAD Municipal de Tisaleo.

Figura 20. Análisis de metadatos en la herramienta Foca (1)



Fuente: elaboración propia

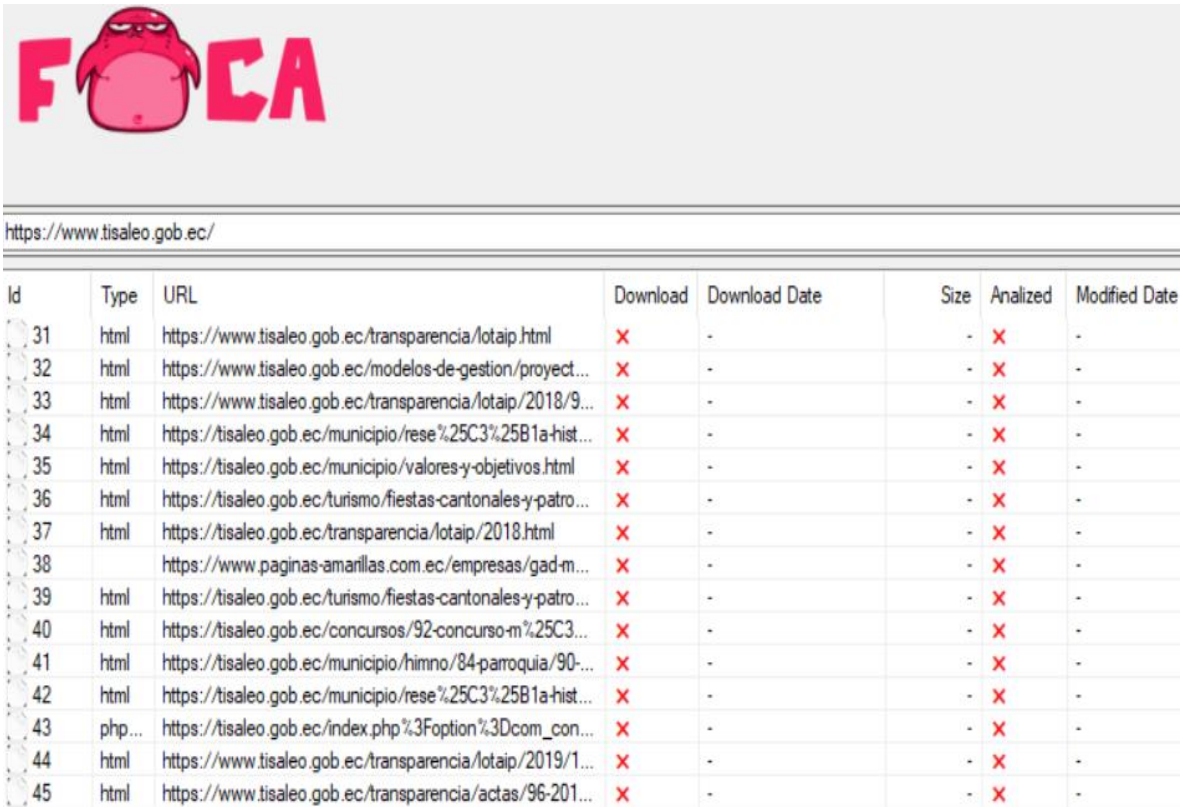
[8] *Joomla*: Sistema de gestión de contenido libre y de código abierto para la creación y publicación de contenidos *web*.
[9] *Metadatos*: Son datos acerca de los datos, es decir, son datos altamente estructurados que describen características de los datos, se los clasifica en función de distintos criterios.
[10] *FOCA:* Herramienta de auditoria de seguridad informática la cual examina los metadatos de los dominios, también, analiza archivos encontrados en un sitio *web* o utilizar archivos locales.

Figura 21. Análisis de metadatos en la herramienta Foca (2)

10	html	https://www.tisaleo.gob.ec/municipio/mision-vision-valor...	✗	-	-	✗	-
11	html	https://www.tisaleo.gob.ec/modelos-de-gestion/proyect...	✗	-	-	✗	-
12	html	https://www.tisaleo.gob.ec/municipio/valores-y-objetivo...	✗	-	-	✗	-
13	html	https://www.tisaleo.gob.ec/modelos-de-gestion/cultura....	✗	-	-	✗	-
14	html	https://www.tisaleo.gob.ec/quejas.html	✗	-	-	✗	-
15	html	https://www.tisaleo.gob.ec/turismo/fiestas-cantonales-y-...	✗	-	-	✗	-
16	html	https://www.tisaleo.gob.ec/transparencia/lotaip/2019/1...	✗	-	-	✗	-
17	php...	https://www.tisaleo.gob.ec/index.php%3Foption%3Dco...	✗	-	-	✗	-
18		https://www.tisaleo.gob.ec/index.php%3Foption%3Dco...	✗	-	-	✗	-
19	html	https://www.tisaleo.gob.ec/turismo/gastronomia.html	✗	-	-	✗	-
20	html	https://www.tisaleo.gob.ec/municipio/himno.html	✗	-	-	✗	-
21		https://www.tisaleo.gob.ec/index.php%3Foption%3Dco...	✗	-	-	✗	-
22		https://www.tisaleo.gob.ec/index.php%3Foption%3Dco...	✗	-	-	✗	-
23		https://www.tisaleo.gob.ec/index.php%3Foption%3Dco...	✗	-	-	✗	-
24	html	https://www.tisaleo.gob.ec/turismo/atractivos-turisticos/...	✗	-	-	✗	-
25		https://www.tisaleo.gob.ec/index.php%3Foption%3Dco...	✗	-	-	✗	-
26	html	https://tisaleo.gob.ec/modelos-de-gestion/cultura.html	✗	-	-	✗	-
27	html	https://tisaleo.gob.ec/municipio/autoridades.html	✗	-	-	✗	-
28		https://tisaleo.gob.ec/parqueinf2/	✗	-	-	✗	-
29		https://www.tisaleo.gob.ec/index.php%3Foption%3Dco...	✗	-	-	✗	-
30	html	https://www.tisaleo.gob.ec/transparencia/actas.html	✗	-	-	✗	-

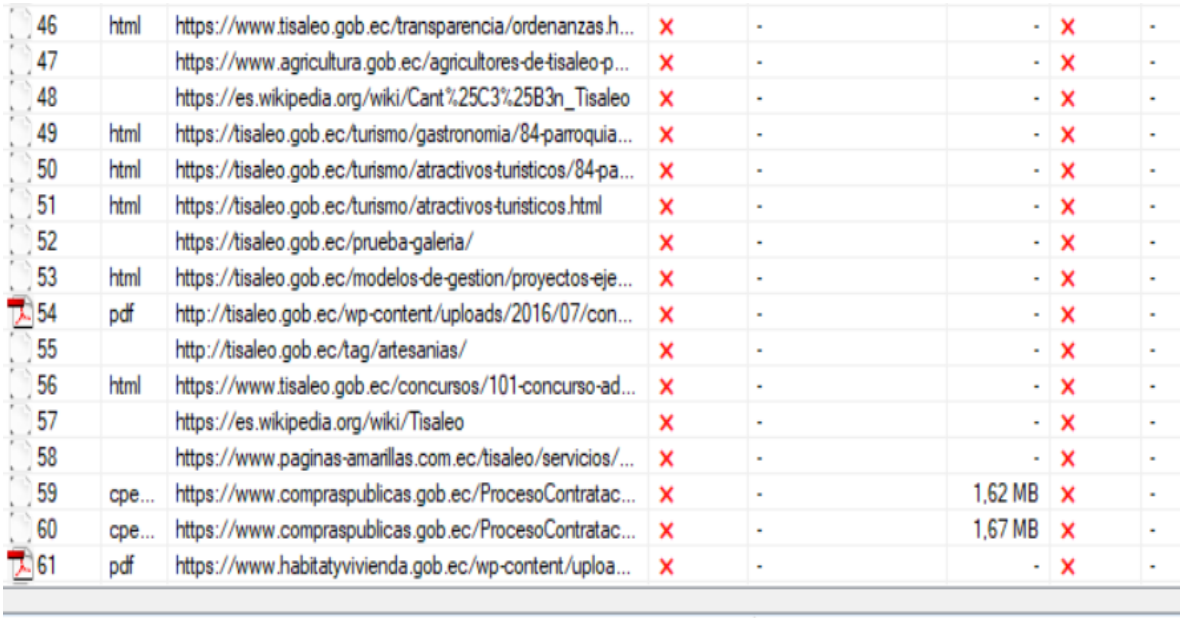
Fuente: elaboración propia

Figura 22. Análisis de metadatos en la herramienta Foca (3)



Fuente: elaboración propia

Figura 23. Análisis de metadatos en la herramienta Foca (4)



46	html	https://www.tisaleo.gob.ec/transparencia/ordenanzas.h...	X	-	-	X	-
47		https://www.agricultura.gob.ec/agricultores-de-tisaleo-p...	X	-	-	X	-
48		https://es.wikipedia.org/wiki/Cant%25C3%25B3n_Tisaleo	X	-	-	X	-
49	html	https://tisaleo.gob.ec/turismo/gastronomia/84-parroquia...	X	-	-	X	-
50	html	https://tisaleo.gob.ec/turismo/atractivos-turisticos/84-pa...	X	-	-	X	-
51	html	https://tisaleo.gob.ec/turismo/atractivos-turisticos.html	X	-	-	X	-
52		https://tisaleo.gob.ec/prueba-galeria/	X	-	-	X	-
53	html	https://tisaleo.gob.ec/modelos-de-gestion/proyectos-eje...	X	-	-	X	-
54	pdf	http://tisaleo.gob.ec/wp-content/uploads/2016/07/con...	X	-	-	X	-
55		http://tisaleo.gob.ec/tag/artesanias/	X	-	-	X	-
56	html	https://www.tisaleo.gob.ec/concursos/101-concurso-ad...	X	-	-	X	-
57		https://es.wikipedia.org/wiki/Tisaleo	X	-	-	X	-
58		https://www.paginas-amarillas.com.ec/tisaleo/servicios/...	X	-	-	X	-
59	cpe...	https://www.compraspublicas.gob.ec/ProcesoContratac...	X	-	1,62 MB	X	-
60	cpe...	https://www.compraspublicas.gob.ec/ProcesoContratac...	X	-	1,67 MB	X	-
61	pdf	https://www.habitatyvivienda.gob.ec/wp-content/uploa...	X	-	-	X	-

Fuente: elaboración propia

Como, se puede visualizar en las *figuras 20, 21, 22 y 23*, no existe ningún metadato que comprometa la seguridad del sitio *web* del GAD Municipal de Tisaleo, como ya, se mencionó con anterioridad, excepto que existe un mínimo detalle el cual fue que algunos enlaces, se transportan en canal *Hypertext Transfer Protocol*[11] y otros en canal *Hypertext Transfer Protocol Secure* [12] el cual tiene es un canal encriptado y presta mayor seguridad a los datos, que se envían por dicho canal.

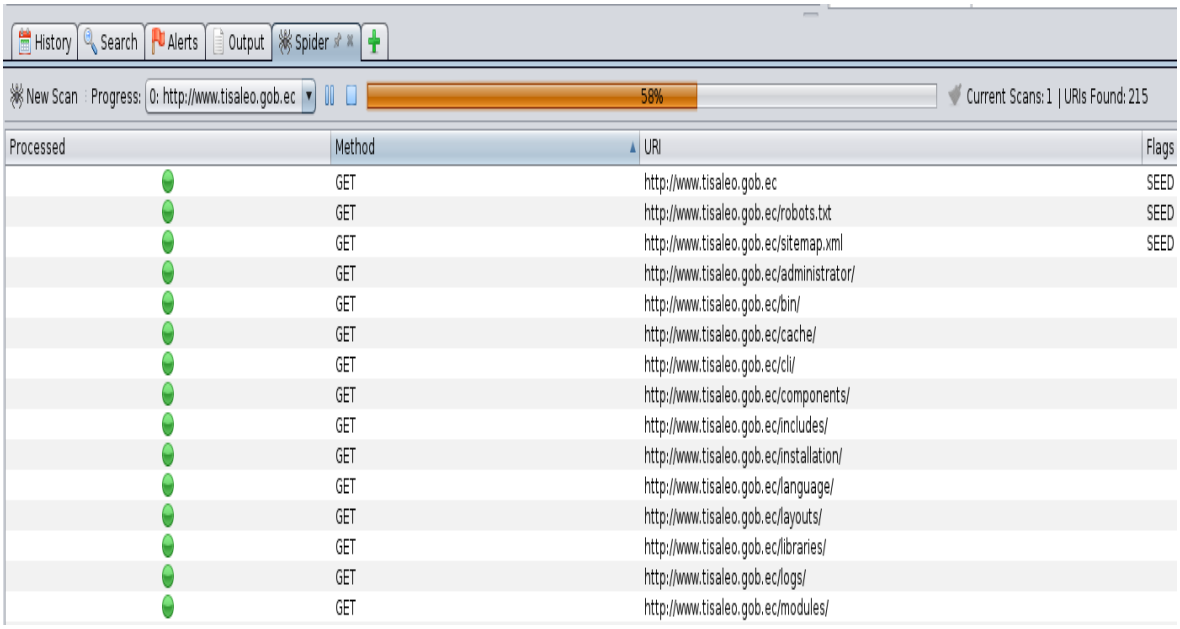
Identificación de puntos de entrada a la aplicación

Enlistar cuales son los puntos de entrada existentes y conocer cada uno de ellos es un parte primordial para todo analista, así, se encontró vulnerabilidades en las entradas existentes para fortalecerlas con diversos procesos.

[11] *Hypertext Transfer Protocol (HTTP):* Protocolo de transferencia de hipertexto, dicho protocolo, se usa en todo tipo de transacciones a través de internet.
[12] *Hypertext Transfer Protocol Secure (HTTPS):* Protocolo seguro de transferencia de hipertexto, es la versión segura de *http*.

Analizar las peticiones y respuestas desde el sitio *web* mediante el manejo de la herramienta *OWASP ZAP*[13], en la herramienta, se encontró información de los métodos *GET* y *POST* que realiza en el sitio *web* con resultados como las siguientes imágenes:

Figura 24. Métodos GET existentes en distintas URL's del sitio web del GAD Municipal de Tisaleo (1)



Fuente: elaboración propia

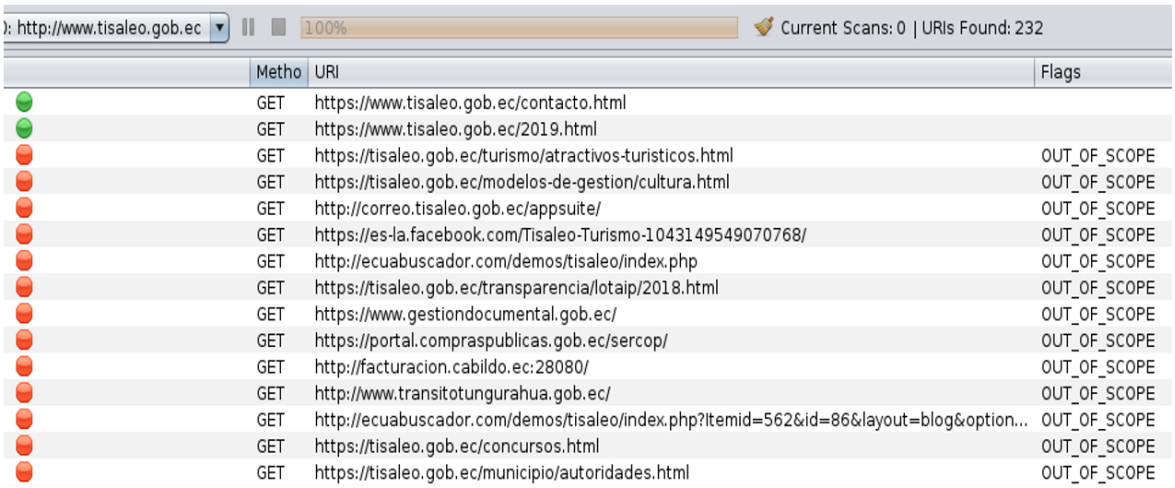
[13] *OWASP ZAP: ZAP = Zed Attack Proxy*; herramienta usada para analizar vulnerabilidades de seguridad informática mediante el escaneo total de una aplicación *web*, la que da como resultados las vulnerabilidades y su grado de riesgo, con lo cual el administrador realiza cambios.

Figura 25. Métodos GET existentes en distintas URL's del sitio web del GAD Municipal de Tisaleo (2)

	GET	http://www.tisaleo.gob.ec/modules/	
	GET	https://www.tisaleo.gob.ec/	
	GET	http://www.tisaleo.gob.ec/plugins/	
	GET	http://www.tisaleo.gob.ec/tmp/	
	GET	https://www.tisaleo.gob.ec/sitemap.xml	
	GET	https://www.tisaleo.gob.ec/administrator/	
	GET	https://www.tisaleo.gob.ec/installation/	
	GET	http://www.facebook.com/	OUT_OF_SCOPE
	GET	https://www.youtube.com/watch?t=364s&v=ezBk3ykr0tk	OUT_OF_SCOPE
	GET	https://www.tisaleo.gob.ec/municipio/reseña-histórica.html	
	GET	https://www.tisaleo.gob.ec/municipio/mision-vision-valores-y-objetivos.html	
	GET	https://www.tisaleo.gob.ec/municipio/autoridades.html	
	GET	https://www.tisaleo.gob.ec/municipio/himno.html	
	GET	https://www.tisaleo.gob.ec/municipio/valores-y-objetivos.html	
	GET	https://www.tisaleo.gob.ec/modelos-de-gestion/servicios-que-ofrece-la-municipalidad.html	

Fuente: elaboración propia

Figura 26. Métodos GET existentes en distintas URL's del sitio web del GAD Municipal de Tisaleo (3)



http://www.tisaleo.gob.ec | 100% | Current Scans: 0 | URIs Found: 232

	Metho	URI	Flags
	GET	https://www.tisaleo.gob.ec/contacto.html	
	GET	https://www.tisaleo.gob.ec/2019.html	
	GET	https://tisaleo.gob.ec/turismo/atractivos-turisticos.html	OUT_OF_SCOPE
	GET	https://tisaleo.gob.ec/modelos-de-gestion/cultura.html	OUT_OF_SCOPE
	GET	http://correo.tisaleo.gob.ec/appsuite/	OUT_OF_SCOPE
	GET	https://es-la.facebook.com/Tisaleo-Turismo-1043149549070768/	OUT_OF_SCOPE
	GET	http://ecuabuscador.com/demos/tisaleo/index.php	OUT_OF_SCOPE
	GET	https://tisaleo.gob.ec/transparencia/lotaip/2018.html	OUT_OF_SCOPE
	GET	https://www.gestiondocumental.gob.ec/	OUT_OF_SCOPE
	GET	https://portal.compraspublicas.gob.ec/sercop/	OUT_OF_SCOPE
	GET	http://facturacion.cabildo.ec:28080/	OUT_OF_SCOPE
	GET	http://www.transitotungurahua.gob.ec/	OUT_OF_SCOPE
	GET	http://ecuabuscador.com/demos/tisaleo/index.php?Itemid=562&id=86&layout=blog&option...	OUT_OF_SCOPE
	GET	https://tisaleo.gob.ec/concursos.html	OUT_OF_SCOPE
	GET	https://tisaleo.gob.ec/municipio/autoridades.html	OUT_OF_SCOPE

Fuente: elaboración propia

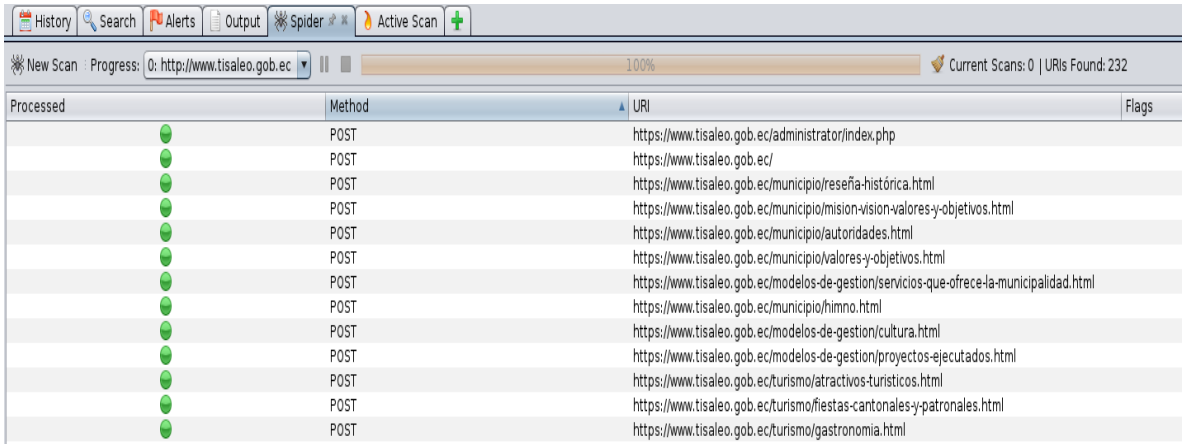
Figura 27. Métodos GET existentes en distintas URL's del sitio web del GAD Municipal de Tisaleo (4)

	GET	https://tisaleo.gob.ec/municipio/rese%C3%B1a-hist%C3%B3rica.html	OUT_OF_SCOPE
	GET	http://www.ame.gob.ec/	OUT_OF_SCOPE
	GET	http://www.tungurahua.gob.ec/main/	OUT_OF_SCOPE
	GET	http://www.iess.gob.ec/	OUT_OF_SCOPE
	GET	http://www.turismo.gob.ec/	OUT_OF_SCOPE
	GET	http://www.connectambato.com/	OUT_OF_SCOPE
	GET	https://www.google.com/maps/embed?pb=!1m18!1m12!1m3!1d127638.27226269722!2d-7...	OUT_OF_SCOPE
	GET	https://www.youtube.com/embed/rtzziPGha_w?controls=0&rel=0&showinfo=0	OUT_OF_SCOPE
	GET	https://www.tisaleo.gob.ec/component/search/?Itemid=437&format=opensearch&id=1	
	GET	https://www.tisaleo.gob.ec/images/favicon.png	
	GET	https://www.tisaleo.gob.ec/components/com_sppagebuilder/assets/css/font-awesome.min.css	
	GET	https://www.tisaleo.gob.ec/components/com_sppagebuilder/assets/css/animate.min.css	
	GET	https://www.tisaleo.gob.ec/components/com_sppagebuilder/assets/css/sppagebuilder.css	
	GET	https://www.tisaleo.gob.ec/components/com_sppagebuilder/assets/css/sppagecontainer.css	

Alerts 0 2 5 0

Fuente: elaboración propia

Figura 28. Métodos POST existentes en distintas URL's del sitio web del GAD Municipal de Tisaleo (5)



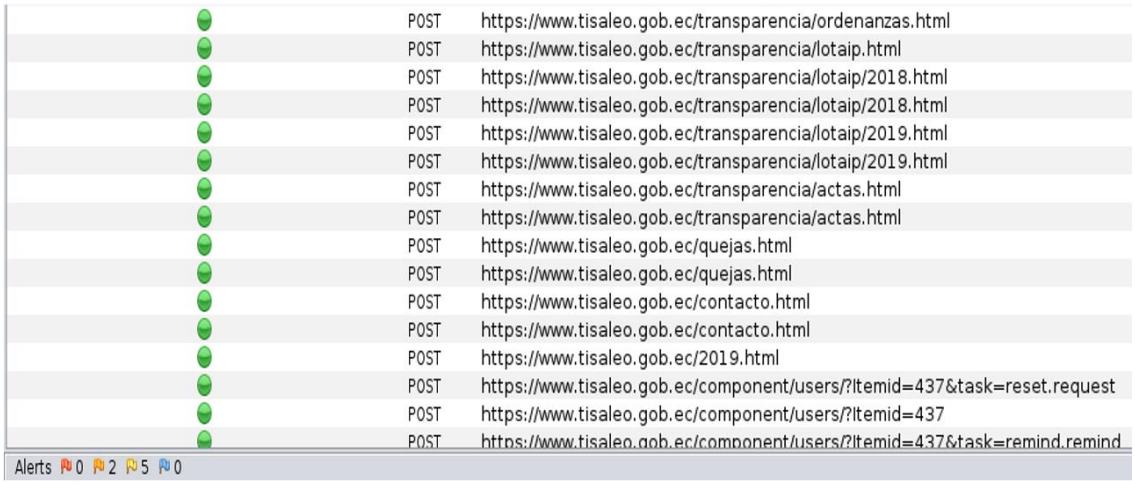
History | Search | Alerts | Output | Spider | Active Scan

New Scan | Progress: 0: http://www.tisaleo.gob.ec | 100% | Current Scans: 0 | URIs Found: 232

Processed	Method	URI	Flags
	POST	https://www.tisaleo.gob.ec/administrator/index.php	
	POST	https://www.tisaleo.gob.ec/	
	POST	https://www.tisaleo.gob.ec/municipio/reseña-histórica.html	
	POST	https://www.tisaleo.gob.ec/municipio/mision-vision-valores-y-objetivos.html	
	POST	https://www.tisaleo.gob.ec/municipio/autoridades.html	
	POST	https://www.tisaleo.gob.ec/municipio/valores-y-objetivos.html	
	POST	https://www.tisaleo.gob.ec/modelos-de-gestion/servicios-que-ofrece-la-municipalidad.html	
	POST	https://www.tisaleo.gob.ec/municipio/himno.html	
	POST	https://www.tisaleo.gob.ec/modelos-de-gestion/cultura.html	
	POST	https://www.tisaleo.gob.ec/modelos-de-gestion/proyectos-ejecutados.html	
	POST	https://www.tisaleo.gob.ec/turismo/atractivos-turisticos.html	
	POST	https://www.tisaleo.gob.ec/turismo/fiestas-cantonales-y-patronales.html	
	POST	https://www.tisaleo.gob.ec/turismo/gastronomia.html	

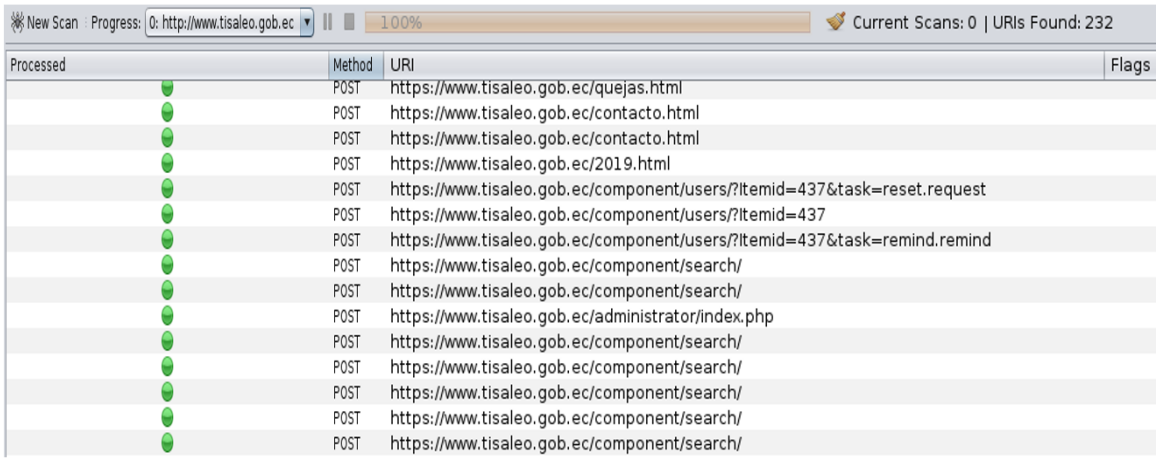
Fuente: elaboración propia

Figura 29. Métodos POST existentes en distintas URL's del sitio web del GAD Municipal de Tisaleo (6)



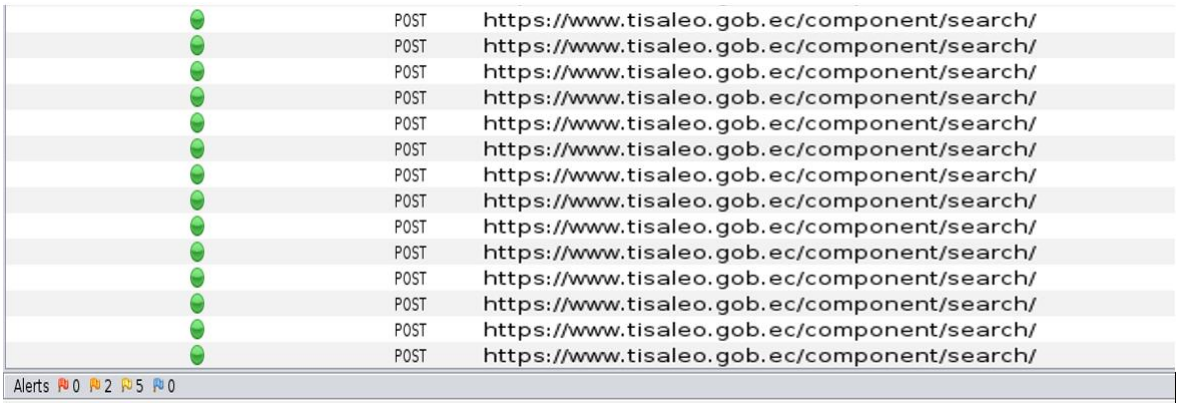
Fuente: elaboración propia

Figura 30. Métodos POST existentes en distintas URL's del sitio web del GAD Municipal de Tisaleo (7)



Fuente: elaboración propia

Figura 31. Métodos POST existentes en distintas URL's del sitio web del GAD Municipal de Tisaleo (8)

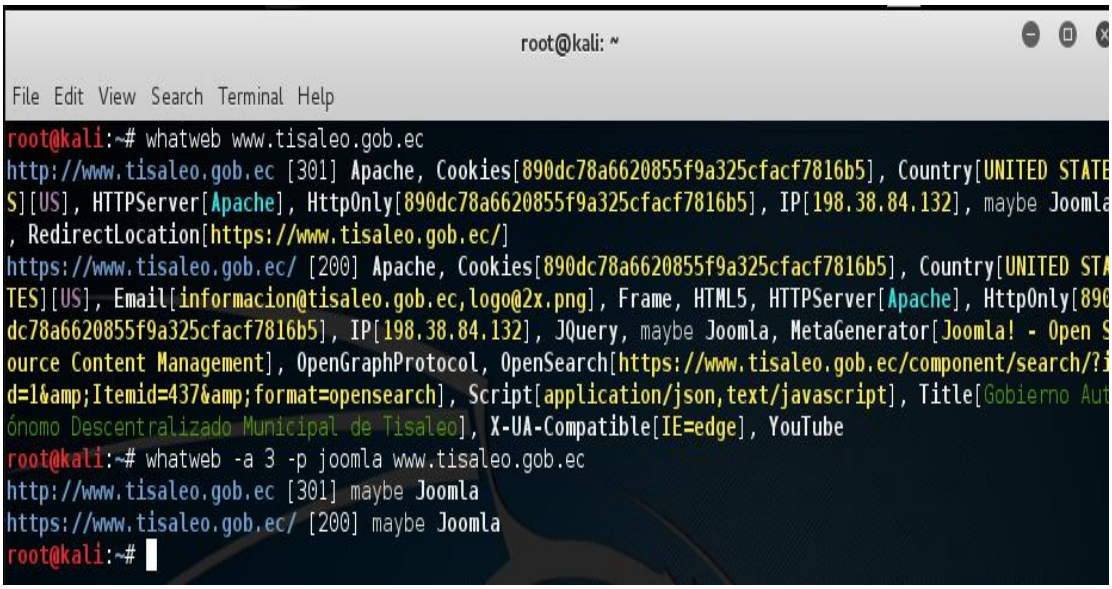


Fuente: elaboración propia

Análisis al entorno de la aplicación *web*

Es fundamental conocer el entorno del sitio *web*, es una tarea importante dentro de la recolección de requerimientos, por lo, que se otorga al analista información que resulta útil al momento de realizar las distintas pruebas, tal como configuraciones deficientes dentro del entrono o el uso de las configuraciones antiguas y sin parches que resguarden la información sensible que contiene el sitio *web*, lo cual representa una vulnerabilidad muy fuerte dentro de una dirección *web*.

Figura 32. Resultado del comando whatweb [14] al sitio web del GAD Municipal de Tisaleo



Fuente: elaboración propia

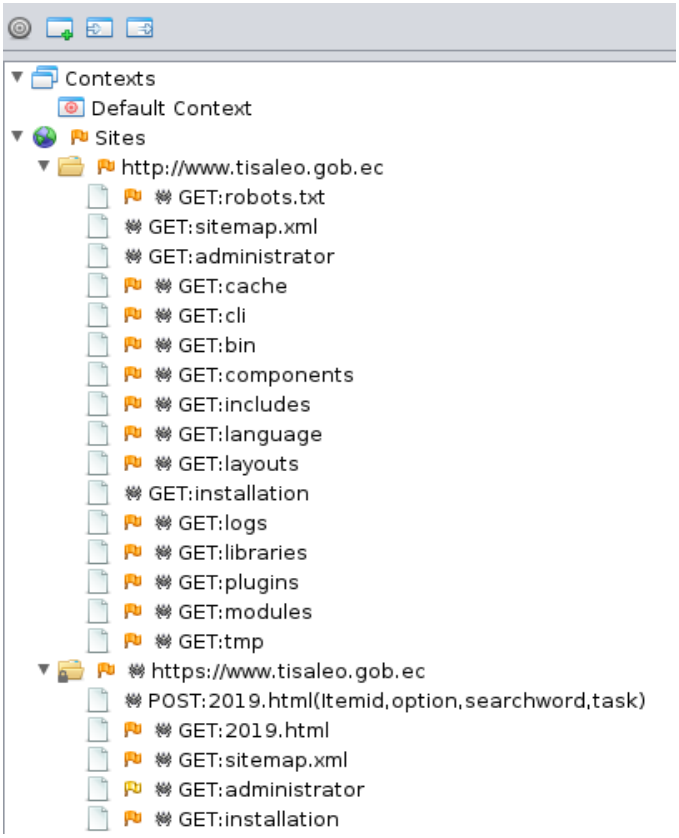
La búsqueda realizada dió como resultado la información acerca del servidor que ejecuta al sitio *web* que al ser analizado y conocer bajo que lenguaje fue realizada, su versión y el tipo de sistema de gestión de contenidos que maneja y que en este caso es *Joomla.*

Análisis y mapa de arquitectura de la aplicación

Es fundamental visualizar la infraestructura de un sitio *web*, a simple vista resulta complicado analizar partes, que se encuentra vulnerable, pero representa un pilar fundamental dentro del análisis de seguridad, un simple error de configuración causaría la caída/perdida parcial o total de valiosos datos del tema de estudio.

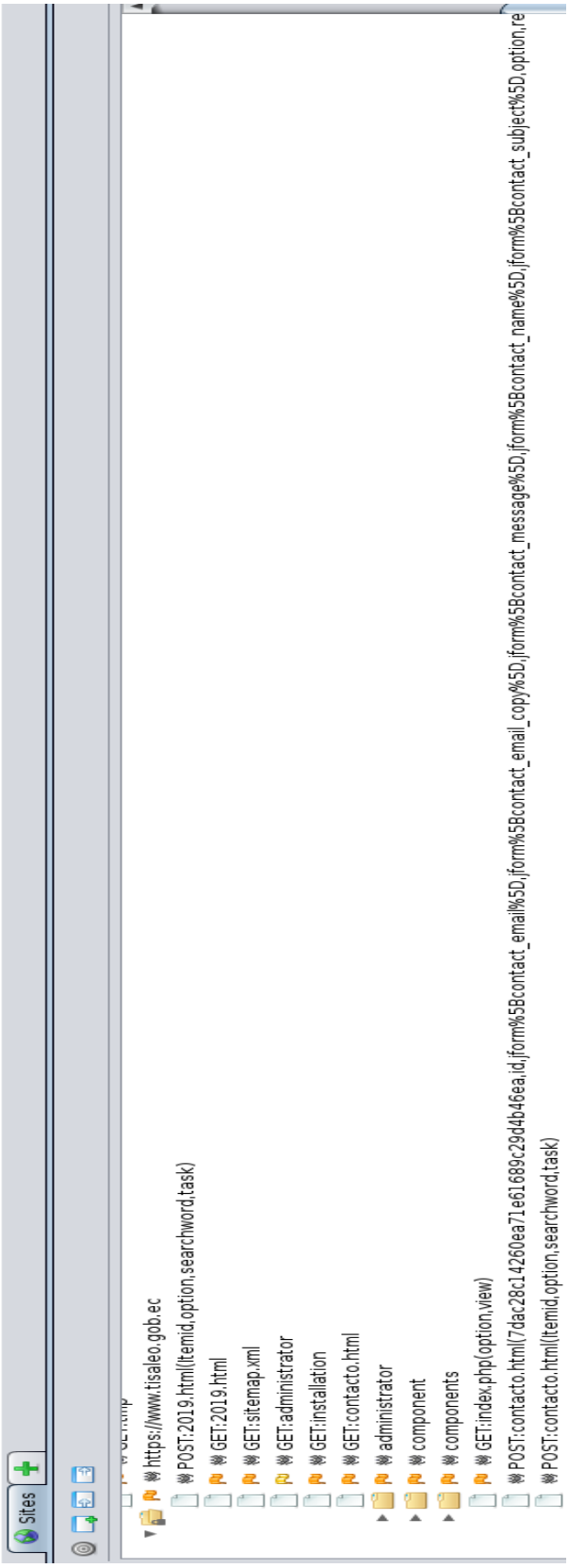
[14] *Whatweb:* el cual devuelve las configuraciones, versiones y tipos de estructura que componen a una determinada dirección *web*.

Figura 33. Estructura del sitio web del GAD Municipal de Tisaleo (1)



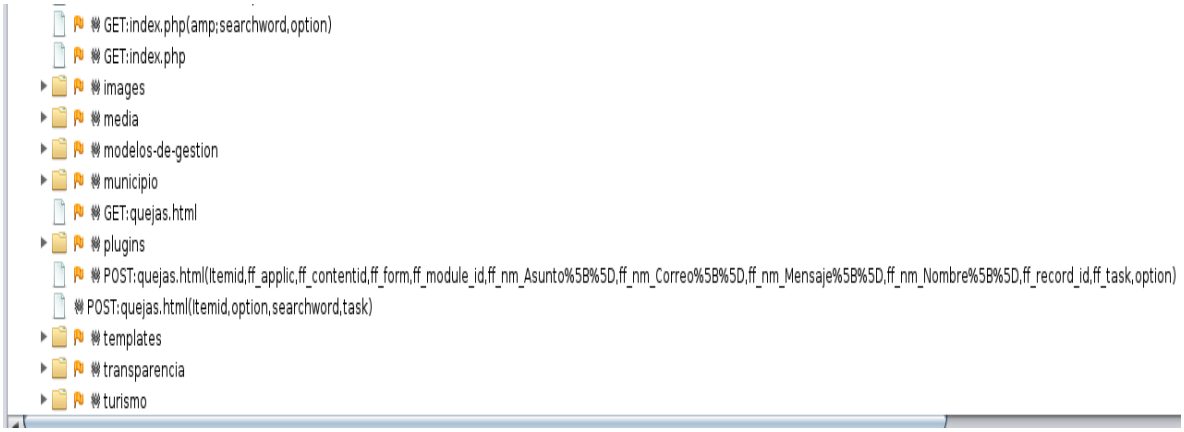
Fuente: elaboración propia

Figura 34. Estructura del sitio web del GAD Municipal de Tisaleo (2)



Fuente: elaboración propia

Figura 35. Estructura del sitio web del GAD Municipal de Tisaleo (3)



Para determinar la infraestructura, se usó la herramienta *OWASP ZAP* la cual permitió realizar un análisis profundo a la estructura de dicho sitio como, se ve en la figura anterior.

3.1.2. Fase II – *Test* de Manejo de Configuración y Desarrollo

Test de configuración e infraestructura de la red

Las herramientas administrativas en estos días son usadas para el manejo de contenidos de los sitios *web*, varias veces, un mínimo error conlleva a un riesgo de dimensiones incalculables.

Por ellos, se analiza las herramientas administrativas que utiliza el sitio *web*, en este caso es *Joomla*.

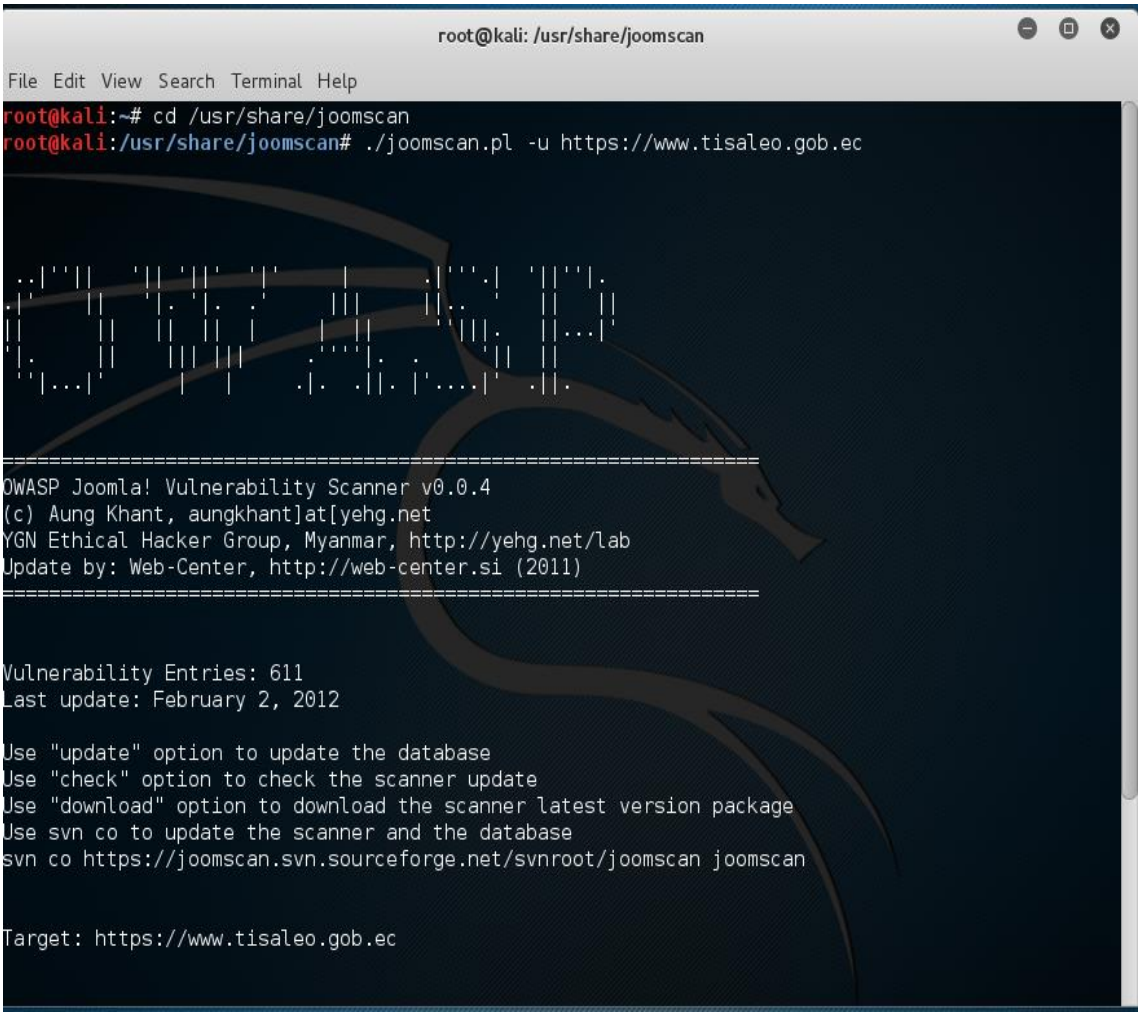
Figura 36. Inicio de la página de acceso de administración

Fuente: elaboración propia

Con el conocimiento adquirido sobre las herramientas para manejo de contenidos, se procede a realizar un análisis profundo de las vulnerabilidades del sitio *web* del presente tema de estudio.

Por el análisis realizado en los puntos anteriores, se pudo determinar la herramienta óptima para dicho uso, la cual fue *Joomscan*[15], la cual analiza vulnerabilidades de la herramienta para manejo de contenidos *Joomla*.

Figura 37. Inicio de la herramienta Joomscan

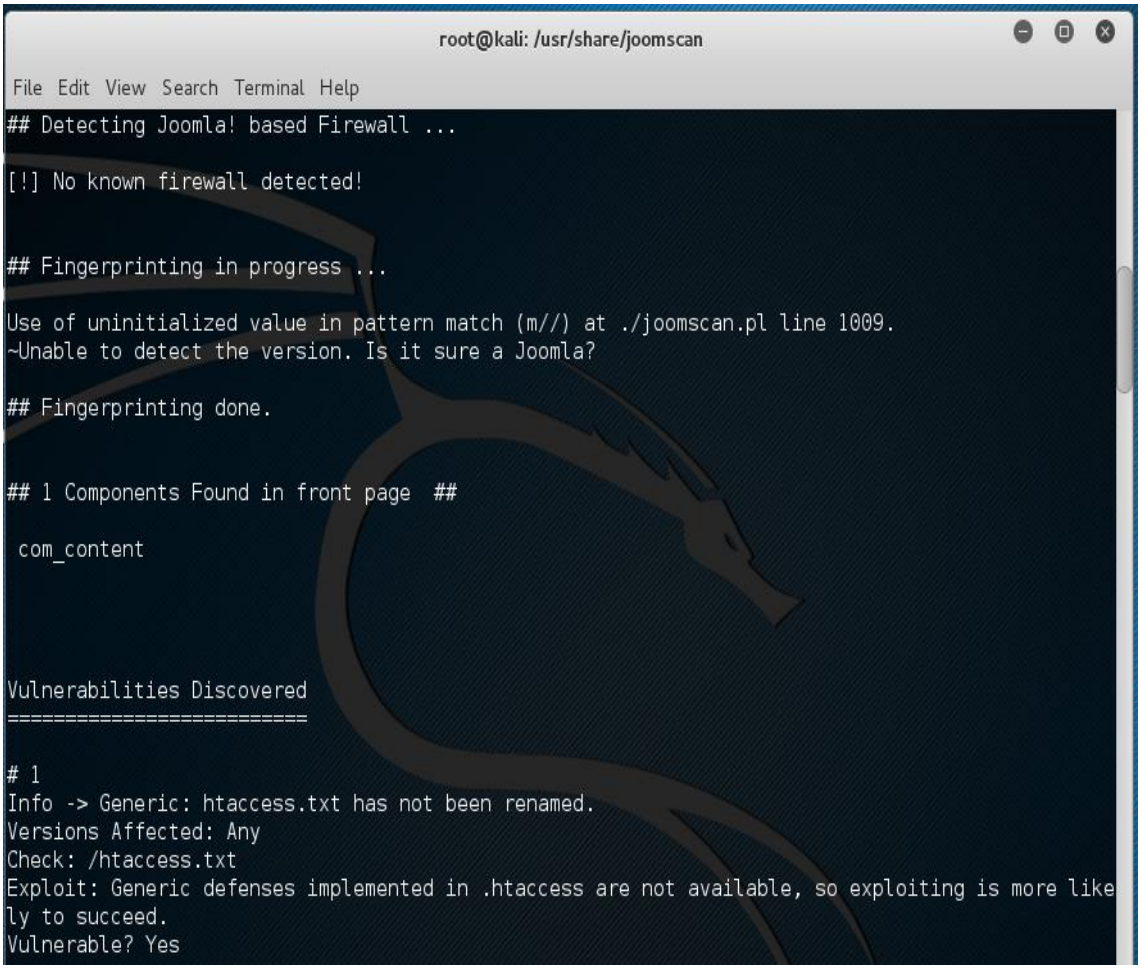


Fuente: elaboración propia

[15] *Joomscan:* Es un paquete de herramientas que está instalado por defecto en *Kali Linux*, el cual realiza un escaneo de aplicaciones *web* basadas en el sistema gestor de contenidos *Joomla* para detectar y reportar vulnerabilidades de seguridad encontradas.

La herramienta *Joomscan,* se enumera las posibles vulnerabilidades de la base de datos y si las mismas fueron encontradas o no dentro de un dominio específico.

Figura 38. Primera vulnerabilidad encontrada



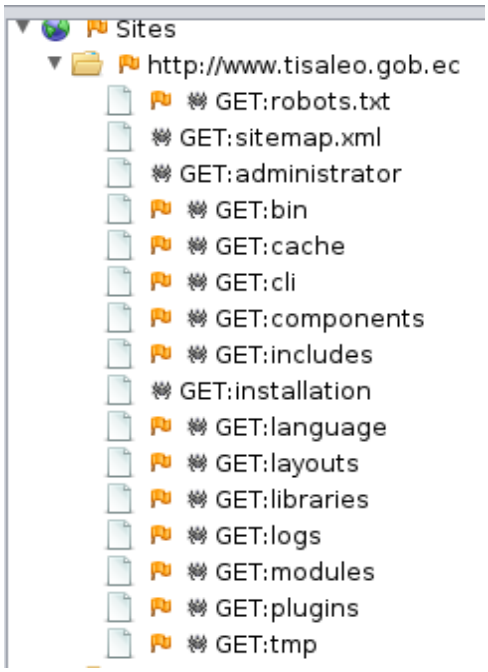
Fuente: elaboración propia

Como, se muestra en la imagen anterior, la primera vulnerabilidad encontrada fue sobre el archivo *htaccess.txt* del cual ya, se habló en la primera fase en la *subsección 3.1.1.*, ahí, se puede ver a donde, se redirige dicho archivo.

Test de las extensiones de los archivos que manejan información sensible

Las extensiones de los archivos manejados en los servidores establecen que lenguajes, *plugin* y tecnologías emplear para complementar los requisitos, el uso de extensiones de archivos estándar consigue otorgar al análisis información pertinente acerca del funcionamiento interno de un sitio *web*.

Figura 39. Archivos encontrados en el sitio web



Fuente: elaboración propia

En este caso hay una configuración básica del sitio web, varios archivos fueron encontrados tal como: el archivo *robots*, *plugin*[16], archivos de lenguaje, archivos de ordenanzas, actas, contactos, entre otros más.

Por otro lado, si el caso fuera encontrar archivos con extensión *.asa* o *.inc* tendrían un grave problema de seguridad debido a que dichos archivos son utilizados para almacenar información de configuraciones de base de datos y otro tipo de información sensible.

Test* de transporte de seguridad estricto *HTTP

La obtención de cabeceras de un sitio *web*, ya son editadas y encontrar más información de dichos, además, de ingresar a dicho sitio sin ninguna dificultad.
Dentro del sitio *web* del GAD Municipal de Tisaleo, se obtiene información de las cabeceras gracias a la herramienta *OWASP ZAP* al realizar un análisis tipo *GET* al sitio ya antes mencionado, se puedo obtener la siguiente información:

[16] *Plugin*: complemento en español, programa informático que añade funcionalidades adicionales o una nueva característica al *software*.

Figura 40. Consulta realizada al sitio web principal del GAD Municipal de Tisaleo

```
GET http://www.tisaleo.gob.ec HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0;)
Pragma: no-cache
Cache-Control: no-cache
Content-Length: 0
Host: www.tisaleo.gob.ec
```

Fuente: elaboración propia

A continuación, se ve el resultado obtenido a través de la consulta realizada a las cabeceras del sitio *web* principal del GAD Municipal de Tisaleo, en el cual, se ve información sensible obtenida a través de la consulta tipo *GET* del ya mencionado.

Figura 41. Respuesta a la consulta tipo GET del sitio web principal del GAD Municipal de Tisaleo

```
HTTP/1.1 301 Moved Permanently
Date: Thu, 25 Apr 2019 01:46:11 GMT
Server: Apache
P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM"
Expires: Wed, 17 Aug 2005 00:00:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: 256cde13fd17d2b39a35ed33f3bc1541=8ffi7cv58pbfblmieu9jv0hks5; path=/; secure; HttpOnly
Location: https://www.tisaleo.gob.ec/administrator/
Last-Modified: Thu, 25 Apr 2019 01:46:12 GMT
Content-Length: 0
Content-Type: text/html; charset=utf-8
```

Fuente: elaboración propia

A continuación, se ve el resultado obtenido a través de la consulta realizada a las cabeceras del sitio *web* principal del GAD Municipal de Tisaleo, en el cual, se observa información sensible obtenida a través de la consulta tipo *POST* del ya mencionado.

Figura 42. Consulta de tipo POST realizada al sitio web del GAD Municipal de Tisaleo

```
POST https://www.tisaleo.gob.ec/administrator/index.php HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0;)
Pragma: no-cache
Cache-Control: no-cache
Content-Type: application/x-www-form-urlencoded
Content-Length: 117
Referer: https://www.tisaleo.gob.ec/administrator/index.php
Host: www.tisaleo.gob.ec
```

Fuente: elaboración propia

Figura 43. Respuesta a la consulta realizada de tipo POST al sitio web del GAD Municipal de Tisaleo

```
HTTP/1.1 303 See other
Date: Thu, 25 Apr 2019 02:05:03 GMT
Server: Apache
P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM"
Expires: Wed, 17 Aug 2005 00:00:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: 256cde13fd17d2b39a35ed33f3bc1541=qb3c82tf5vu73rv6ge1vuq5db3; path=/; secure; HttpOnly
Location: /administrator/index.php
Last-Modified: Thu, 25 Apr 2019 02:05:03 GMT
Content-Length: 0
Connection: close
Content-Type: text/html; charset=utf-8
```

Fuente: elaboración propia

Como, se ve en las imágenes anteriores las cabeceras, se encuentran al descubierto lo cual es un grave peligro, como, se mencionó que son modificadas para diferentes usos maliciosos de los atacantes, como el ser modificaciones de valores, o cambios en los documentos, entre otros más.

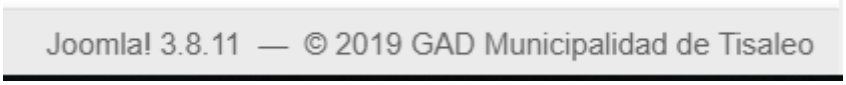
3.1.3. Fase III – *Test* de manejo de identidad

Test de definición de roles

En toda institución, se define los roles del sistema con el fin de determinar las autorizaciones que tiene los administradores y los usuarios que manejan el sitio *web* interno; los mismos son los que permiten el acceso a información sensible que contiene el sitio *web*, con la posibilidad de realizar cambios que afecten a la página principal manejada por *Joomla*.

En primera instancia, se revisó la interfaz del administrador, en lo, que se descubre que existe información que facilita una intromisión, como la versión de *Joomla*, ubicada en el pie inferior derecho de la misma, la cual es antigua, graficada en la sección inferior.

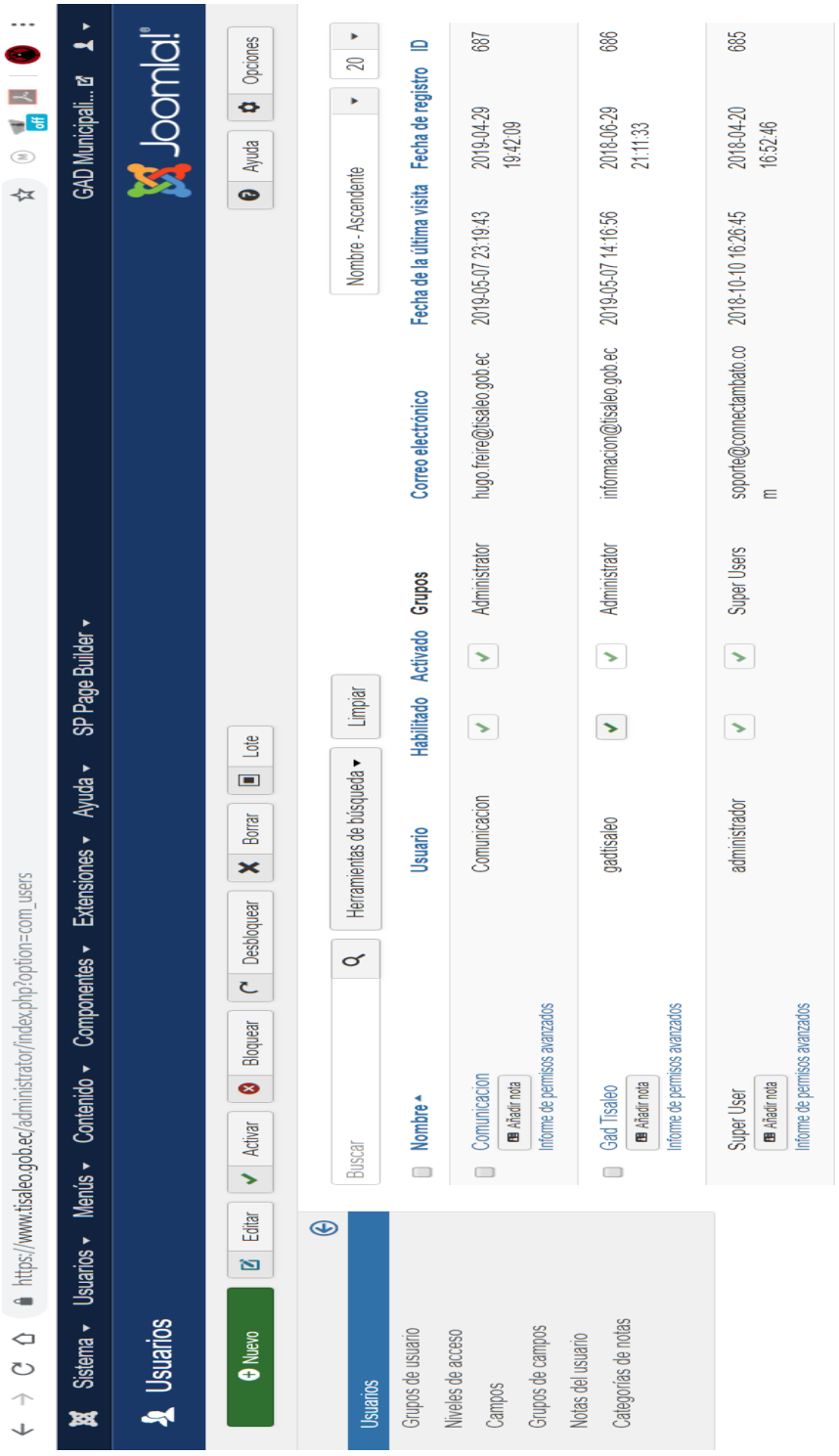
Figura 44. Versión de Joomla en la interfaz de administrador



Fuente: elaboración propia

Es por lo, que se requiere un análisis al flujograma de autorizaciones correspondientes a una entidad, para así poder delimitar las acciones, que son o no realizar dentro de un sitio *web*.

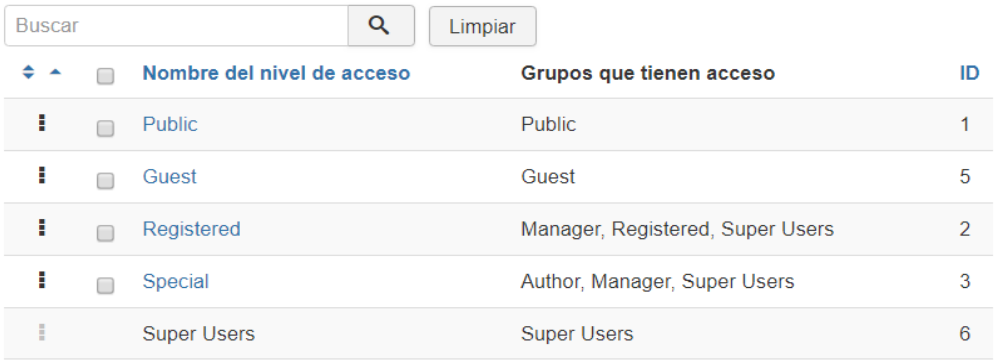
Figura 45. Lista de usuarios y roles de administración del sitio web.



Fuente: elaboración propia

En el sistema de administración *Joomla*, se enlista los usuarios y roles existentes, gracias a la colaboración del GAD Municipal de Tisaleo, el usuario con él, que se obtuvo el ingreso tiene permisos de administrador.

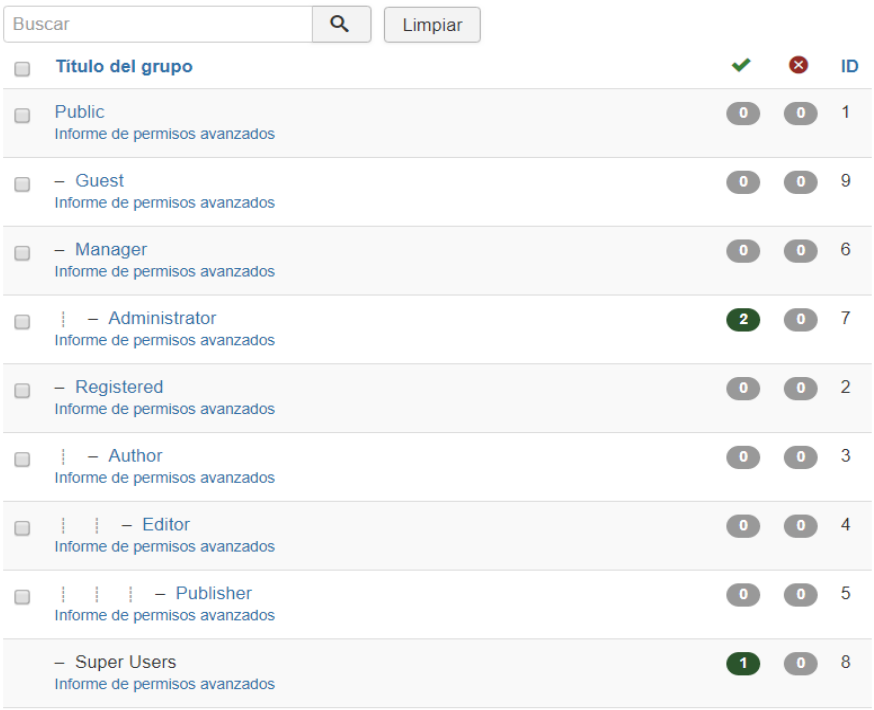
Figura 46. Niveles de acceso y roles del sitio web del GAD Municipal de Tisaleo



Fuente: elaboración propia

En la siguiente imagen, se puede ver los grupos de usuarios que existen en el sitio *web* del GAD Municipal de Tisaleo, y los respectivos privilegios que tiene sobre el ya mencionado.

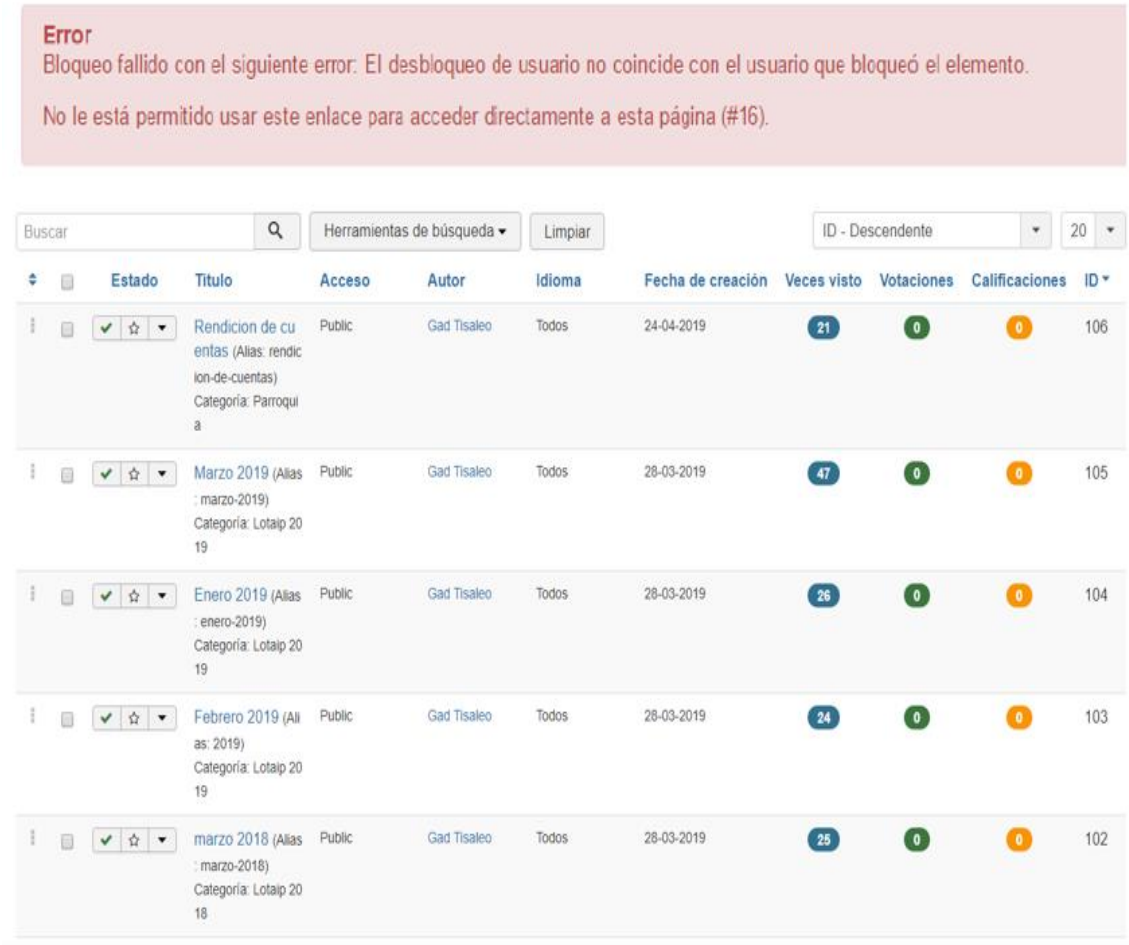
Figura 47. Grupos de usuarios del sitio web



Fuente: elaboración propia

Las principales seguridades que tiene la administración del sistema del GAD Municipal de Tisaleo, se realiza mediante el usuario creador de la página, es el único que contiene dichos permisos para eliminar, es decir, el super usuario tiene acceso total.

Figura 48. Tentativa de eliminación de una publicación del sitio web



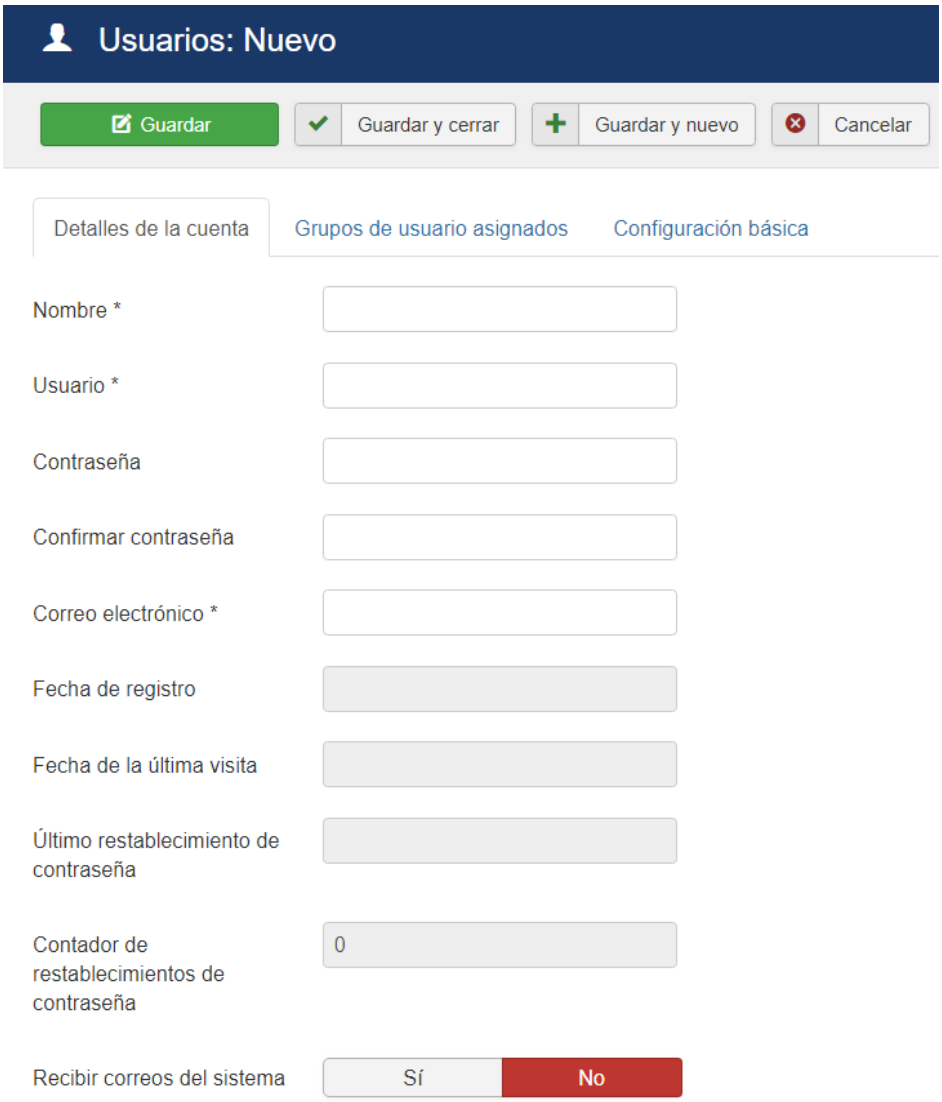
Fuente: elaboración propia

Test de proceso de registro de nuevos usuarios

En el proceso de registro de nuevos usuarios, se tiene privilegios de administrador, solo los usuarios con este rol crean a nuevos usuarios.

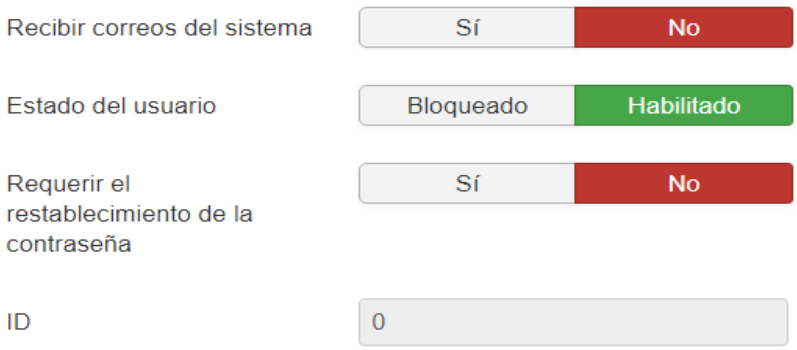
En *Joomla* hay un registro de usuarios con una interfaz gráfica muy sencilla con la cual, se guía paso a paso la definición de un nuevo usuario.

Figura 49. Formulario de registro de nuevo usuario (1)



Fuente: elaboración propia

Figura 50. Formulario de registro de nuevo usuario (2)



Fuente: elaboración propia

Test de procesos de creación de nuevas cuentas

Con la creación de una nueva cuenta, también, se le otorgar el rol y los permisos necesarios para que funcione con toda normalidad, en el punto anterior, se visualizó como es la creación de una nueva cuenta, es por lo que existen las configuraciones de usuarios.

Figura 51. Configuración de nivel de acceso y usuarios

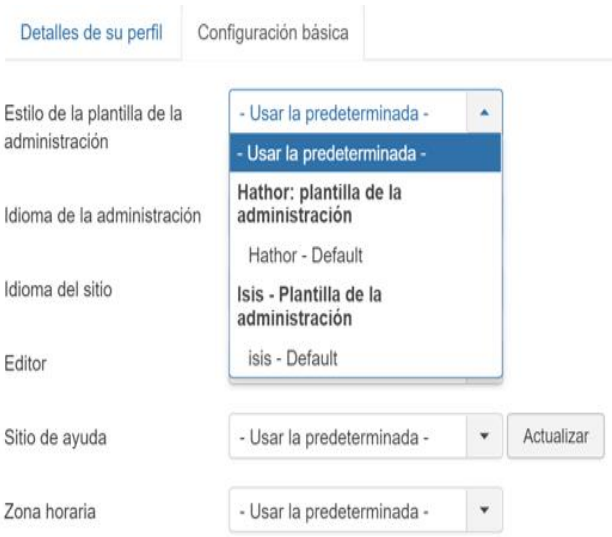
Fuente: elaboración propia

Al configurar al usuario en el grupo pertinente, se le asigna los roles y acciones que realiza el mismo, cada rol posee acciones distintas para lo cual es importante tener el conocimiento de las mismas al momento de la asignación del grupo.

De la misma forma las configuraciones básicas muestran aquellas, que se mostrarán al usuario para el manejo de la aplicación, tal como tipo de estilo y métodos de utilización de pantallas.

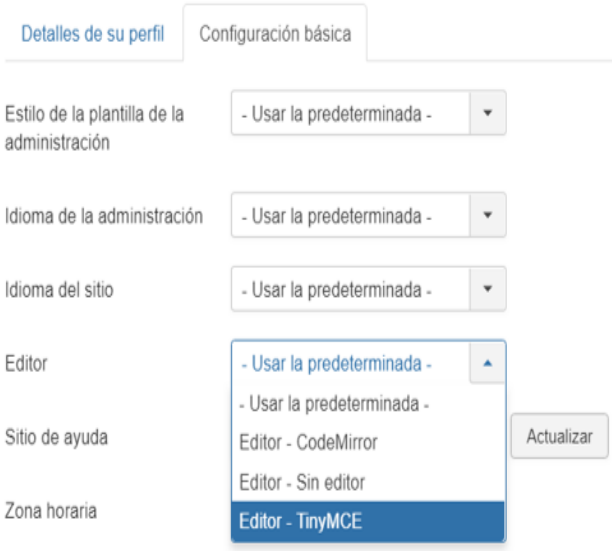
A continuación, se ve la plantilla básica para la configuración de un nuevo usuario, tal así que podemos ver los detalles esenciales, que se necesita para el mismo, y, también, se observa que la configuración no es estricta.

Figura 52. Configuración básica de usuario, plantillas (1)



Fuente: elaboración propia

Figura 53. Configuración básica de usuario, estilos (2)

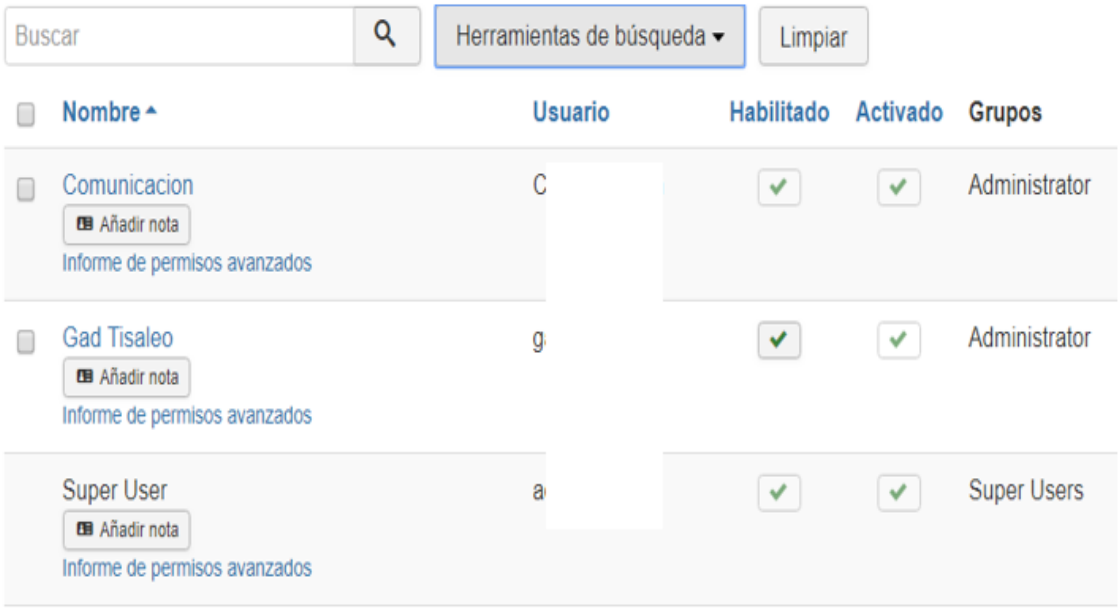


Fuente: elaboración propia

Test para políticas de uso de nombres de usuarios débiles o sin seguridades

Para la creación de cuentas hay que tener en cuenta los nombres de usuario, y tratar de obviar a toda costa que sean fáciles de adivinar; los nombres como: administrador, *admin* usuario, *usr*, entre otros son muy comunes y por defecto, dichos nombres no son recomendables de utilizar.

Figura 54. Listado de usuarios que manejan el sitio web del GAD Municipal de Tisaleo



Fuente: elaboración propia

Lo que demuestra la existencia de procesos por revisar y que son modificados para evitar futuros riesgos de seguridad informática.

3.1.4. Fase IV -*Test* de Autenticación

Test de credenciales transportadas en un canal encriptado

La encriptación de datos es fundamental debido a que, existe la posibilidad en la que un atacante realice un análisis completo de la red e intervenir peticiones que son producidas hacia una aplicación *web*, y si las mismas, no se encuentran cifradas, el atacante tiene una puerta abierta hacia el acceso de información sensible, en el caso del presente proyecto de investigación, se obtiene usuarios y contraseñas del administrador de *Joomla* y de los correos electrónicos municipales, el puerto del *Cpanel*, se encuentra por defecto, esto es un grave riesgo para el GAD Municipal de Tisaleo.

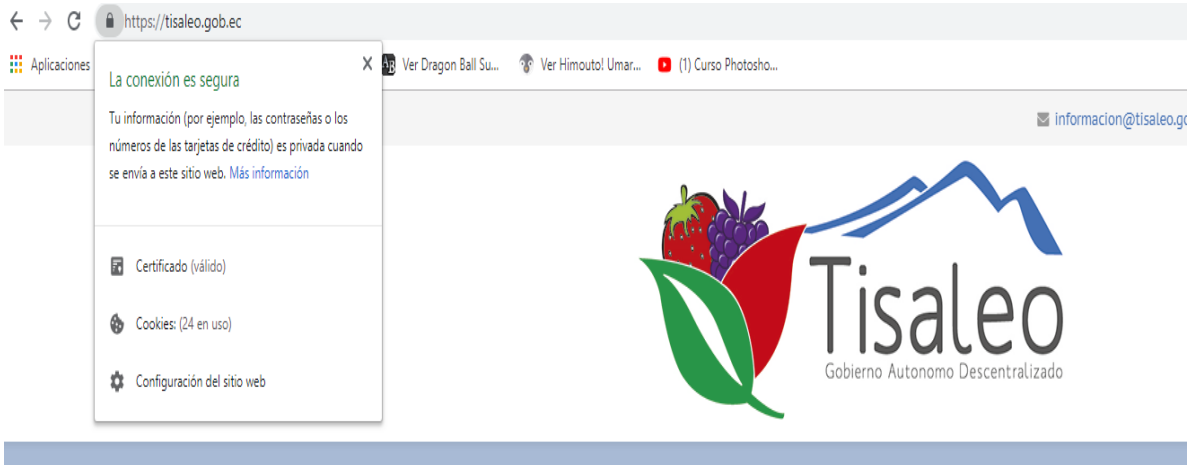
Para la comprobación correspondiente, se realizará una petición tipo *POST* al sitio *web* del GAD Municipal de Tisaleo:

Figura 55. Petición tipo POST realizada al sitio web del GAD Municipal de Tisaleo (1)

```
POST https://www.tisaleo.gob.ec/administrator/index.php HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0;)
Pragma: no-cache
Cache-Control: no-cache
Content-Type: application/x-www-form-urlencoded
Content-Length: 117
Referer: https://www.tisaleo.gob.ec/administrator/index.php
Host: www.tisaleo.gob.ec
```

Fuente: elaboración propia

Figura 56. Petición tipo POST realizada al sitio web del GAD Municipal de Tisaleo (2)



Fuente: elaboración propia

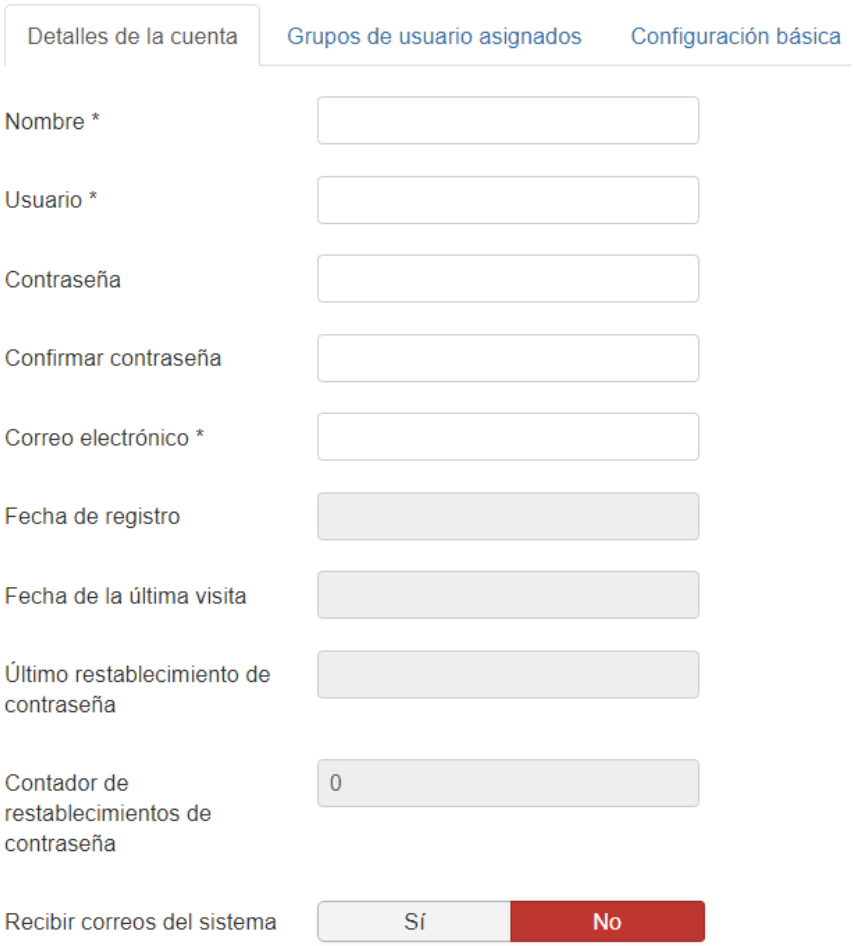
Como, se puede visualizar en las *figuras 55 y 56*, la respuesta viene de un servicio *https* lo cual demuestra que la información, se transporta por un canal encriptado y los mismos están protegidos por un cifrado, claro está que siempre existen vulnerabilidades, pero el protocolo seguro es un poco más difícil de ser vulnerado.

Test de manejo de credenciales y políticas de seguridad de usuarios

En el momento en, que se crea un nuevo usuario, numerosas veces son creados con nombres de usuario y contraseñas que son adivinadas por un intruso y, no se diga nada de las contraseñas que son generadas, cabe recalcar que es un grave error dejar las contraseñas por defecto, existe la posibilidad que el usuario y la contraseña sean la cédula, esto es fácil de consultar, en internet existe varias páginas que obtienen la misma, con un simple *click*.

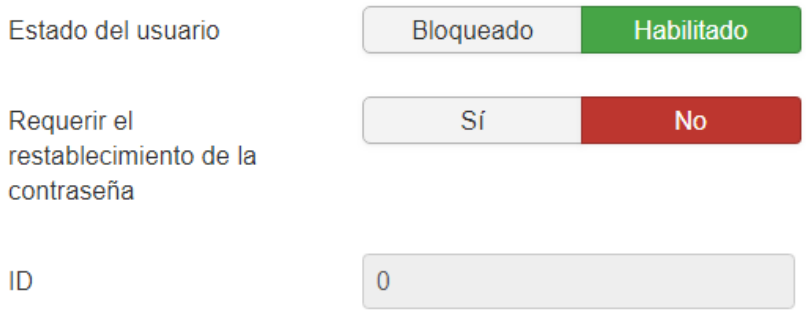
Muchas veces el usuario tiene la facilidad de cambiar la contraseña por una más difícil, pero en su mayoría los usuarios no la cambian, no desean tener muchas contraseñas complicadas en su memoria, luego es difícil de recordar, por lo que dejan las contraseñas que son entregadas por el sistema.

Figura 57. Formulario para creación de usuarios (1)



Fuente: elaboración propia

Figura 58. Formulario para creación de usuarios (2)



Fuente: elaboración propia

El sitio *web* del GAD Municipal de Tisaleo contiene una sola persona encargada de la Unidad de Tecnología, existe un solo usuario administrador que es dicha persona, un super usuario por parte de la empresa creadora del sitio *web* y para finalizar un usuario creado para el presente análisis, el cual utilizó durante el desarrollo de la presente investigación. A pesar de que el sitio *web* tiene la capacidad de generar más usuarios, no, se lo realiza, pero en un futuro con más personal, se crea más usuarios.

Test de debilidades de mecanismos de cierre

Las debilidades de mecanismo de cierre hacen referencia al manejo del sitio *web* para ataques de fuerza bruta, mediante el mismo la cuenta que está vulnerable a bloqueos automáticos después de un número determinado de intentos de ingreso en el cual, se utilizó credenciales erróneas.

La metodología *OWASP* plantea una sucesión de pasos a seguir para la verificación del correcto mecanismo de cierre:

- Intentar ingresar al sistema con datos incorrectos en tres ocasiones.
- Intentar ingresar al sistema con datos incorrectos en cuatro ocasiones.
- Intentar ingresar al sistema con datos incorrectos en cinco ocasiones.
- Ingresar al sistema, demuestra, que no se ha disparado un mecanismo de cierre.
- Si, se dispara un mecanismo de cierre, se habrá bloqueado la cuenta.
- Intentar ingresar de manera correcta después de cinco minutos, si el mecanismo de cierre se desactiva a los cinco minutos de bloqueo.

- Intentar ingresar de forma correcta después de diez minutos, si el mecanismo de cierre se desactiva a los diez minutos de bloqueo.
- Intentar ingresar de manera correcta después de quince minutos, si el mecanismo de cierre se desactiva a los quince minutos de bloqueo.

En el sitio *web* del GAD Municipal de Tisaleo, se intentó realizar los pasos mencionados en el punto anterior más de 20 intentos fallidos, en la que la cuenta, no se bloqueó.

Figura 59. Intento N.º 20 de ingreso con datos erróneos

Fuente: elaboración propia

Seguido, se intentó ingresar con los datos correctos, en la cual, se comprobó que no existe un bloqueo de la cuenta posterior a lo hecho con anterioridad, por lo tanto, se dice, que el sitio es vulnerable a taques de fuerza bruta.

Figura 60. Ingreso correcto al portal de Joomla

Fuente: elaboración propia

Como, se puede ver en la figura anterior el sistema de bloqueo después de varios intentos no funciona, a dicha cuenta, se trató de ingresar más de 20 veces, por último, se ingresó con los datos correctos, funcionó de forma exitosa y por ello, se confirma que la cuenta, no se bloqueó después de los intentos mencionados previo-realizados.

Para ejemplificar lo grave de la presente vulnerabilidad, se realizó un ataque de fuerza bruta en contra del sitio *web*.

Por motivos del presente estudio y por motivos de que un ataque real conllevaría semanas sólo, se ejemplifica la posibilidad de llevar uno a cabo, se tiene como preámbulo las credenciales ya otorgadas por el GAD Municipal de Tisaleo.

Figura 61. Creación del diccionario de datos con la herramienta *Crunch*

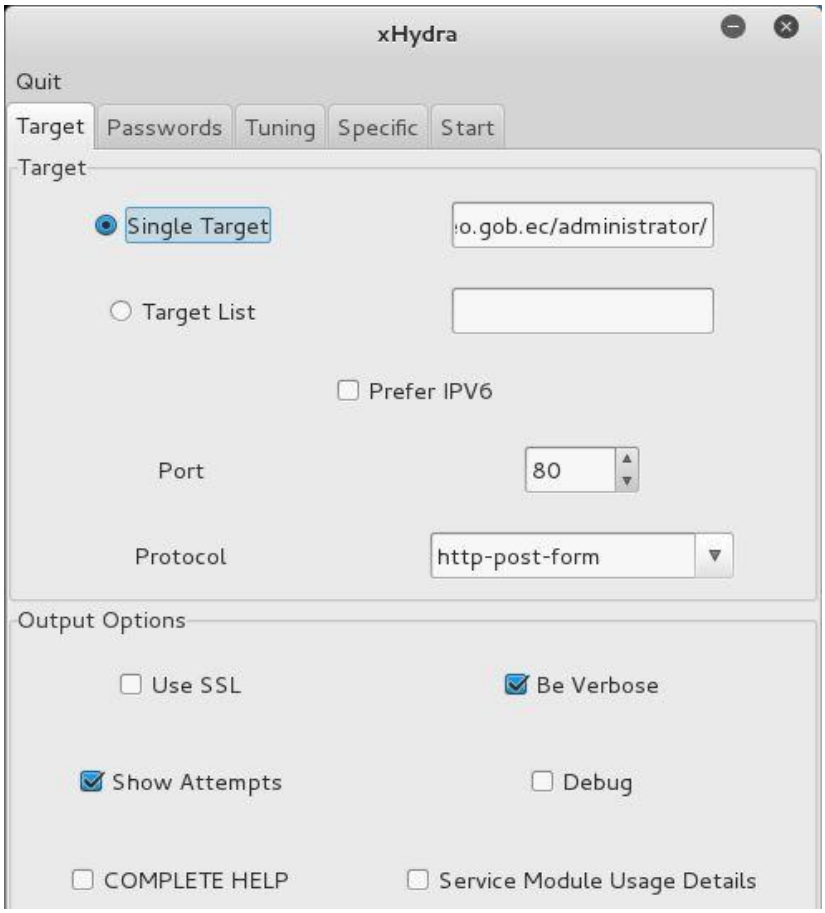
```
root@kali:~/Documents# crunch 12 12 -t Comunic@@@@@ -o dictionary.txt
Crunch will now generate the following amount of data: 154457888 bytes
147 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 11881376
```

Fuente: elaboración propia

En primer lugar, es necesario construir el diccionario de datos, al conocer ya la clave y por motivo de estudio para reducir tiempos de procesamiento para *Crunch,*[17] se lo desarrolla con dicha premisa.

[17] Crunch: Herramienta que genera diccionario de datos, una lista de palabras sujeta a las condiciones que el usuario especifique y que el archivo de salida pueda ser utilizado en cualquier otro programa.

Figura 62. Ataque de fuerza bruta con la herramienta *Hydra (1)*

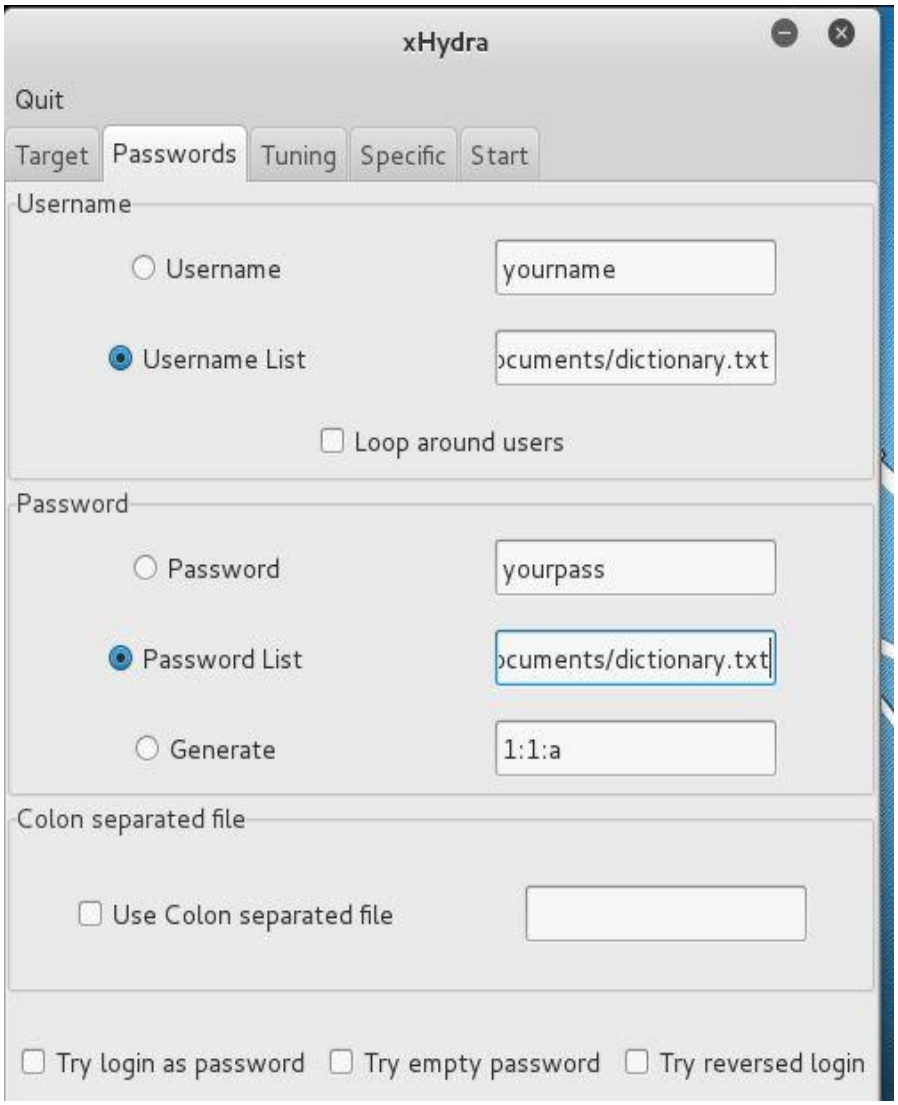


Fuente: elaboración propia

Después de realizar aquello, se utiliza la herramienta *Hydra*[18] con la cual, se selecciona el objetivo víctima, el puerto y el protocolo a utilizar y, por último, se prosigue a la ejecución de la herramienta.

[18] Hydra: Herramienta que permite realizar ataques de fuerza bruta a servicios *online*, tal como, *FTP*, *SSH*, *MySQL*, *POP3*, *Telnet*, *etc.*

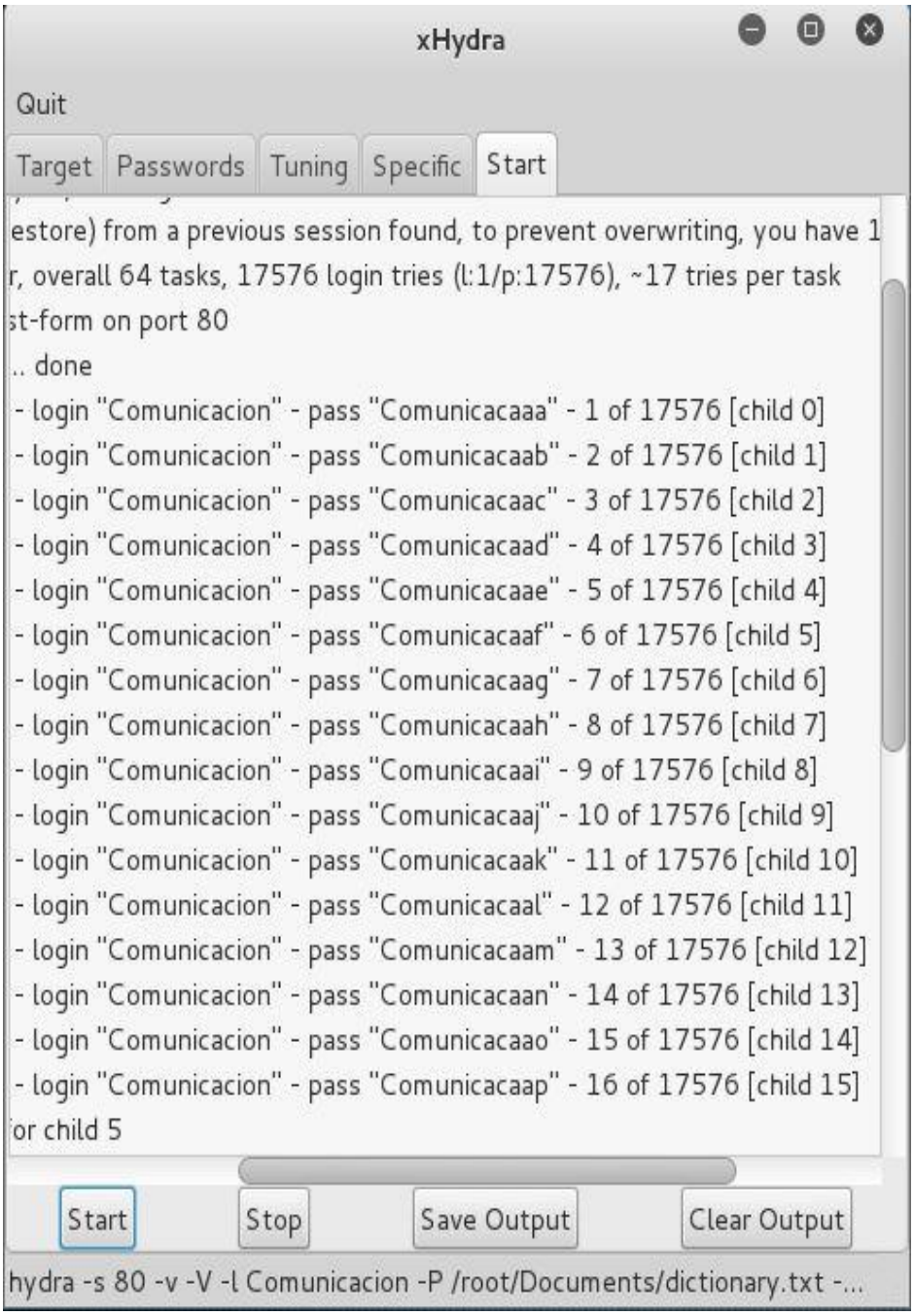
Figura 63. Ataque de fuerza bruta con la herramienta *Hydra (2)*



Fuente: elaboración propia

Seguido de ello, se selecciona el tipo de contraseñas, que se va a utilizar, en este caso, se utiliza el diccionario de datos, que se ha construido.

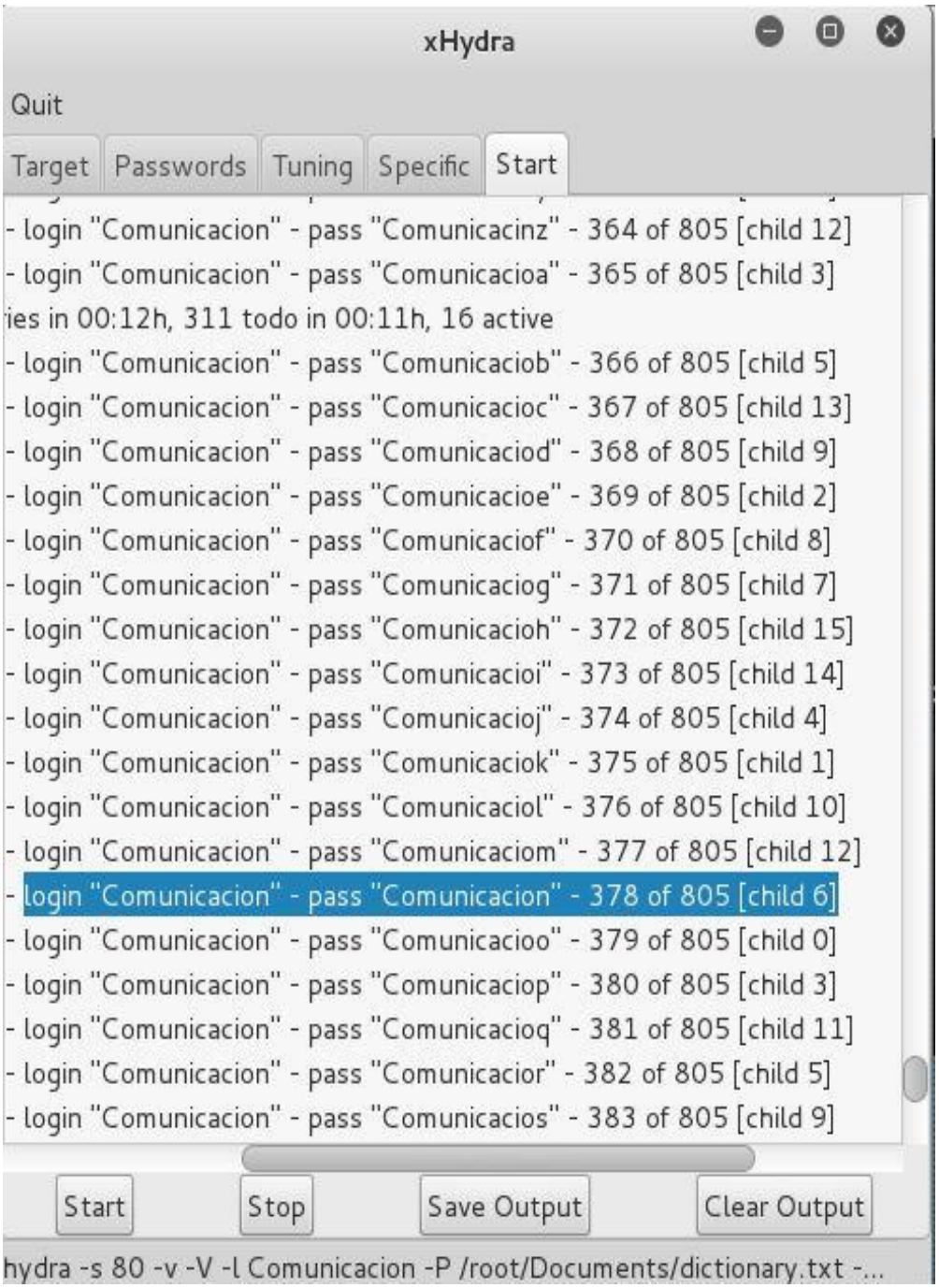
Figura 64. Resultados del ataque de fuerza bruta



Fuente: elaboración propia

Por último, se ejecuta el ataque a la espera de que la clave sea la correcta.

Figura 65. Resultado encontrado del ataque de fuerza bruta



Fuente: elaboración propia

Después de algún tiempo, se obtiene la clave que automático selecciona *Hydra* por lo cual, se demuestra la posibilidad de un ataque de fuerza bruta.

Test para sobrepasar el esquema de autenticación

Hoy en día hay varias formas de sobrepasar los esquemas de autenticación, tales como inyecciones *SQL*, ataques de fuerza bruta, análisis de archivos *hash*[19].

Para el presente caso de estudio, se procedió a realizar una inyección *SQL*, la cual resultó fallida, al intentar proceder con las inyecciones los caracteres, se transforman y, no se procesan por lo que, no se realiza un acceso externo mediante código *SQL*.

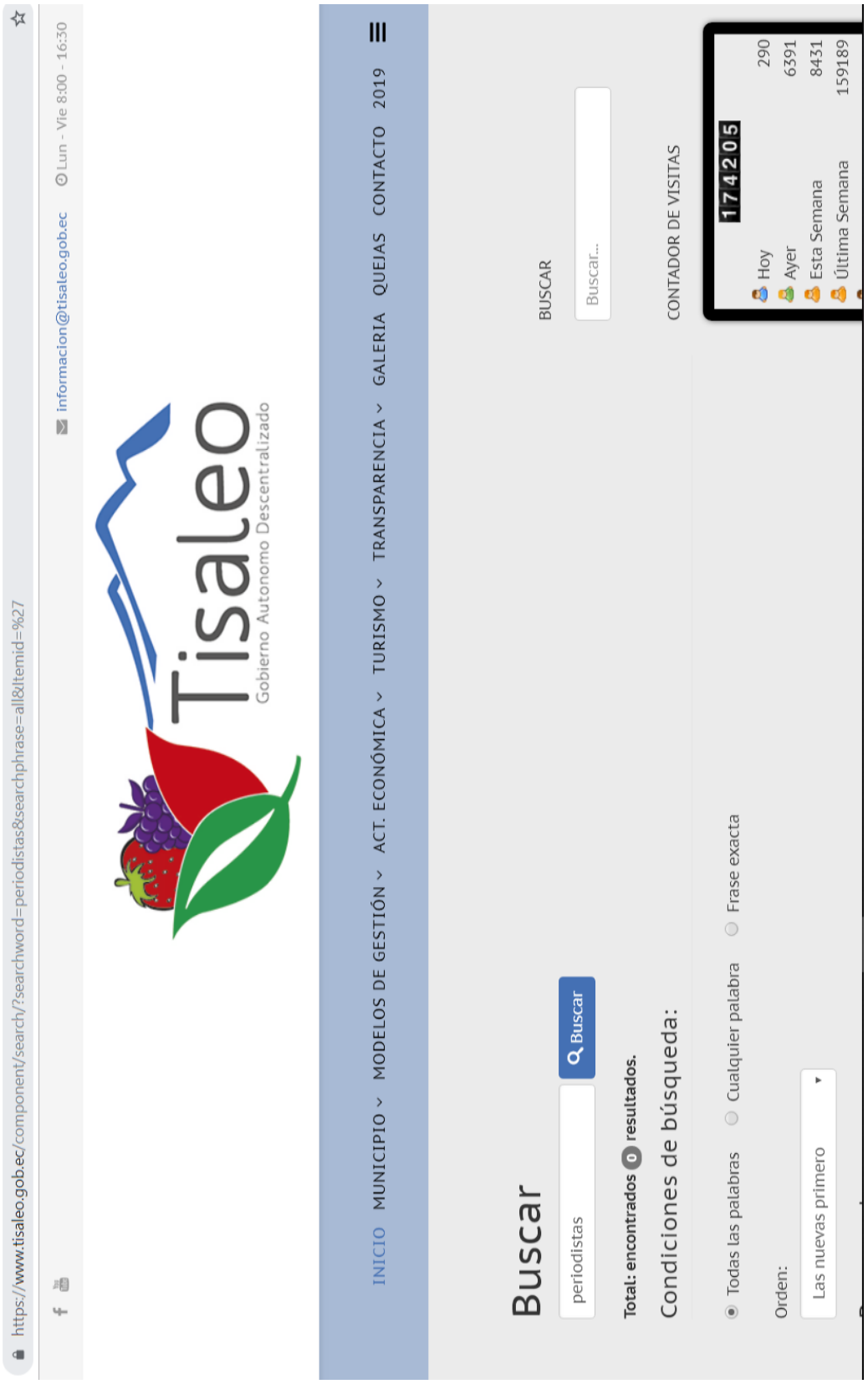
Como, se puede ver en las siguientes figuras, se ingresó en la *URL* las inyecciones *SQL* respectiva, que se aplicó al *textbox* de búsqueda del sitio *web* del GAD Municipal de Tisaleo, seguido, se puede observar en las *figuras 59 y 60*, se procedió a dar *enter* en la *url*, se pudo ver que la misma como, se transformó en una diferente.

Figura 66. Inyección *SQL* simple (‘) en un *textbox* de búsqueda

Fuente: elaboración propia

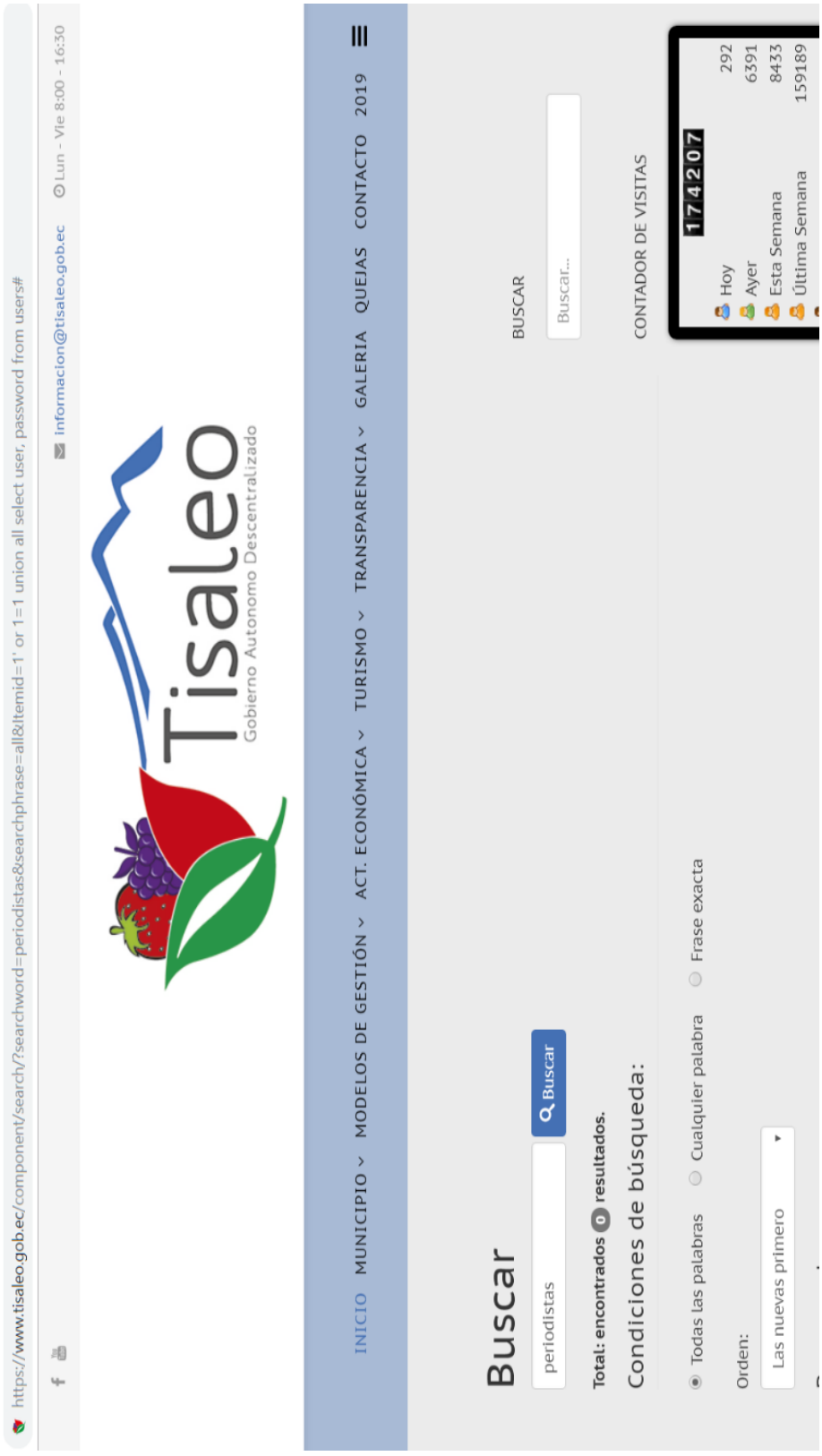
[19] *Hash*: Algoritmo informático que convierte cualquier bloque arbitrario de datos en una nueva cadena de caracteres con una longitud fija.

Figura 67. Resultado de la inyección *SQL* simple (‘)



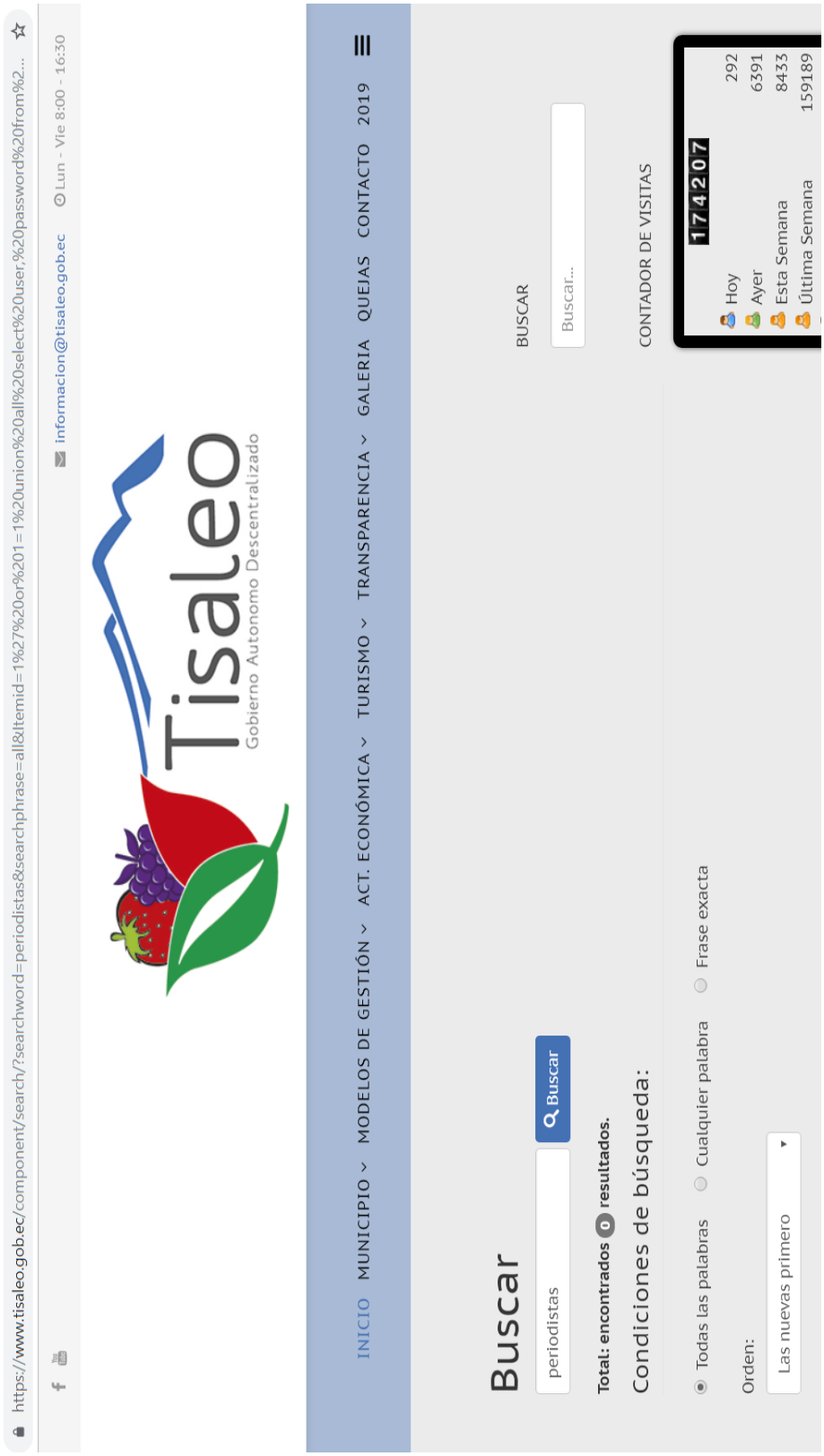
Fuente: elaboración propia

Figura 68. Inyección *SQL (1' or 1=1 union all select user, password from users#)* en un *textbox*



Fuente: elaboración propia

Figura 69. Resultado de la inyección *SQL (1' or 1=1 union all select user, password from users#)*

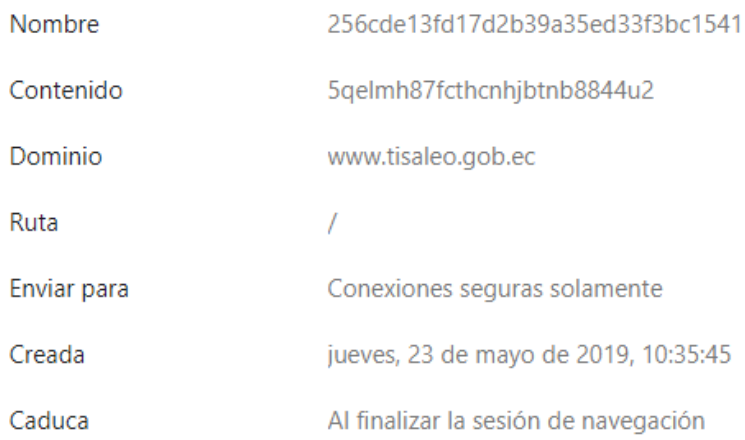


Fuente: elaboración propia

Test de funcionalidad de recordar contraseñas

Las páginas web tienen *cookies*[20], si estas, se quedan activadas, varias veces, se guardan las contraseñas y el estado de la sesión para facilitar el ingreso del usuario, el análisis de las mismas es fundamental para determinar si las *cookies* están cifradas, un atacante identifica esta debilidad, puesto que sí, se encuentran cifradas no existe posibilidad de obtener dichas contraseñas de forma fácil mediante el robo de las *cookies* del navegador en uso.

Figura 70. Análisis de cookies de navegación del sitio web del GAD Municipal de Tisaleo



Fuente: elaboración propia

Test de funcionalidades de reseteo de contraseñas

Existe la posibilidad de guardar la información delicada en la memoria caché del navegador, hay que establecer que el historial de un navegador no es el mismo que la memoria *caché* del mismo, es ahí donde, se nota la diferencia entre la memoria *caché*[21], es temporal, además, donde, se bajan los archivos de un determinado sitio *web* hacia archivos temporales para tener un acceso a ellos mucho más rápido, varios de estos archivos son *tokens* de sesión los cuales mantienen una sesión activa, es decir, que se, deja una puerta abierta para que un atacante logre suplantar la identidad de una víctima.

[20] *Cookies*: Galleta Informática, es una pequeña información enviada por una aplicación *web* y almacenada en el navegador del usuario, de tal manera el sitio consulta la actividad que tiene el cliente.
[21] Memoria *caché*: La *caché* del navegador es una función que los principales navegadores contienen, permite cargar la información de las páginas *web* más rápido, está guardada en la computadora parte de la información que, con anterioridad, se ha solicitado.

Mediante una prueba bastante simple, se analiza la existencia de memoria cache vulnerable dentro del sitio *web*, al cerrar sesión, en este caso la plataforma *Joomla*, retorna a la página principal en el navegador.

Figura 71. Cerrar sesión en el sitio web del GAD Municipal de Tisaleo

Fuente: elaboración propia

Figura 72. Salida exitosa del sitio web

Fuente: elaboración propia

Es entonces el momento en, que se regresa a la página anterior del navegador, para comprobar si existe alguna vulnerabilidad en la memoria cache.

3.1.5. Fase V - *Test* de manejo de sesiones

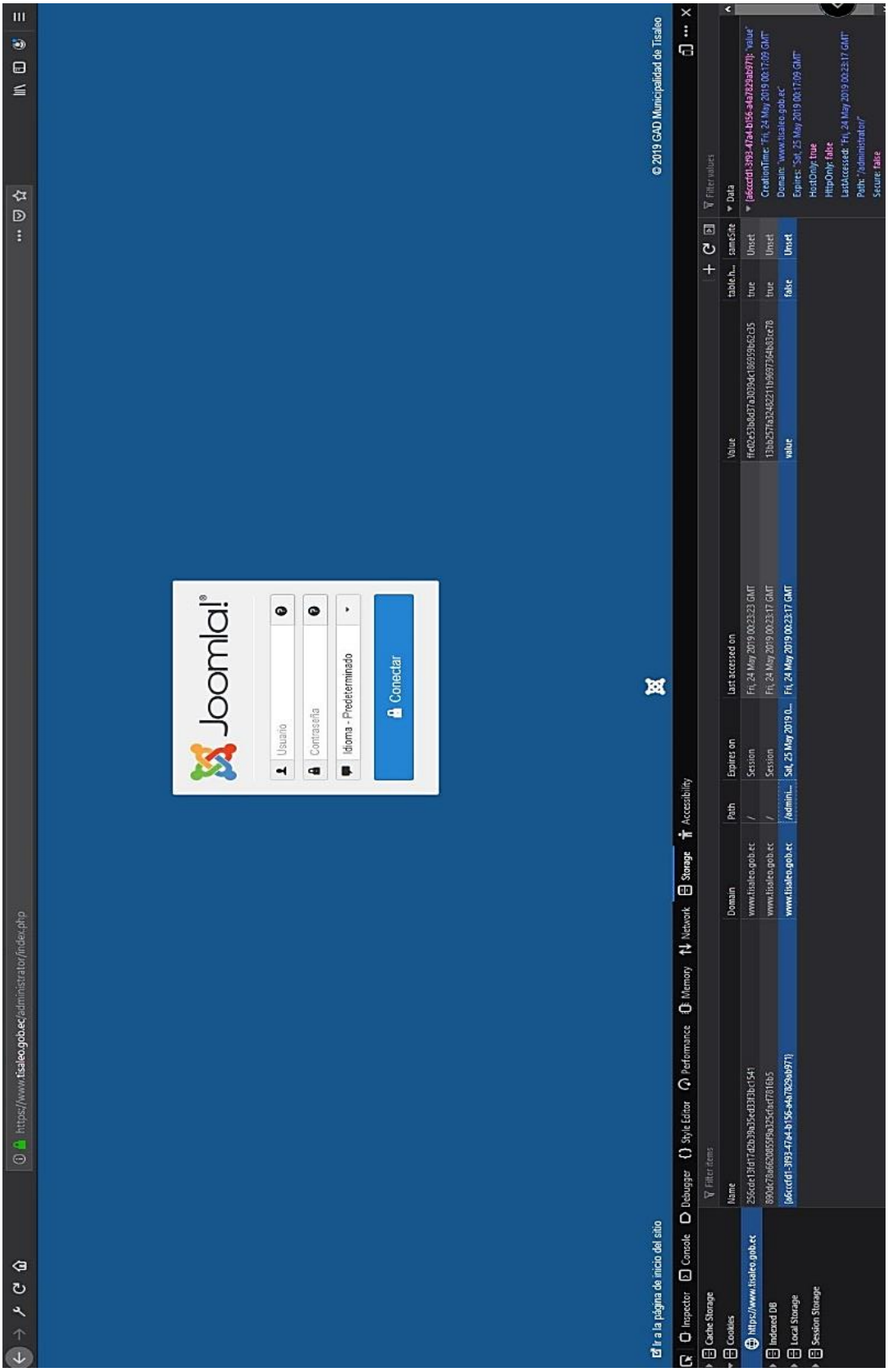
Test para sobrepasar el esquema de manejo de sesiones y atributos de *cookies*

En todo sitio *web*, se encuentran las cookies, las cuales guardan información dentro del navegador para que la misma no tenga que volver a ser consultada en *internet*. Es un mecanismo que ahorra tiempo de procesamiento, pero existe la posibilidad de que sea explotado, varias veces la información guardada es la de sesión.

En el caso del presente estudio, se realiza un ataque de *Session hijacking*[22] que consiste en apoderarse de una *cookie* de sesión no cifrada y utilizarla en otro navegador.

[22] *Session Hijacking* - Secuestro/Robo de sesión: Se trata de que un individuo consigue el identificador de sesión entre una aplicación *web* y un usuario, de esta forma, existe la posibilidad de suplantar la identidad del usuario y acceder a la cuenta.

Figura 73. Análisis en el navegador Firefox for Developers



Fuente: elaboración propia

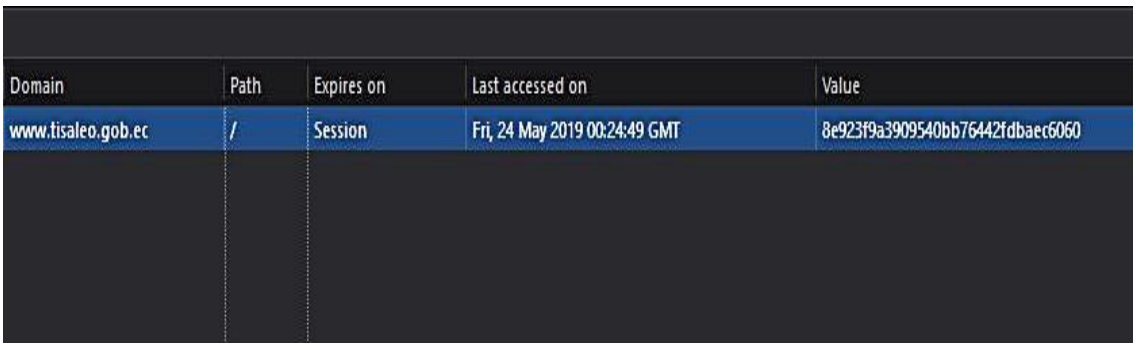
Para el ataque, se utiliza de manera única el navegador *Firefox for Developers*[23] el cual tiene herramientas que permiten analizar y cambiar las cookies de sesión. En la imagen, se aprecia la interfaz del navegador mencionado con anterioridad y las *cookies* presentes dentro del navegador.

Figura 74. Resultado del análisis *Firefox for Developers (1)*

Fuente: elaboración propia

Para la prueba, se inicia sesión con la cuenta que, gracias al apoyo del GAD Municipal de Tisaleo, se otorgó para el análisis de vulnerabilidades. Una vez iniciada la sesión dentro de la interfaz antes descrita, se copia el valor de la *cookie* de sesión.

Figura 75. Resultado del análisis *Firefox for Developers (2)*

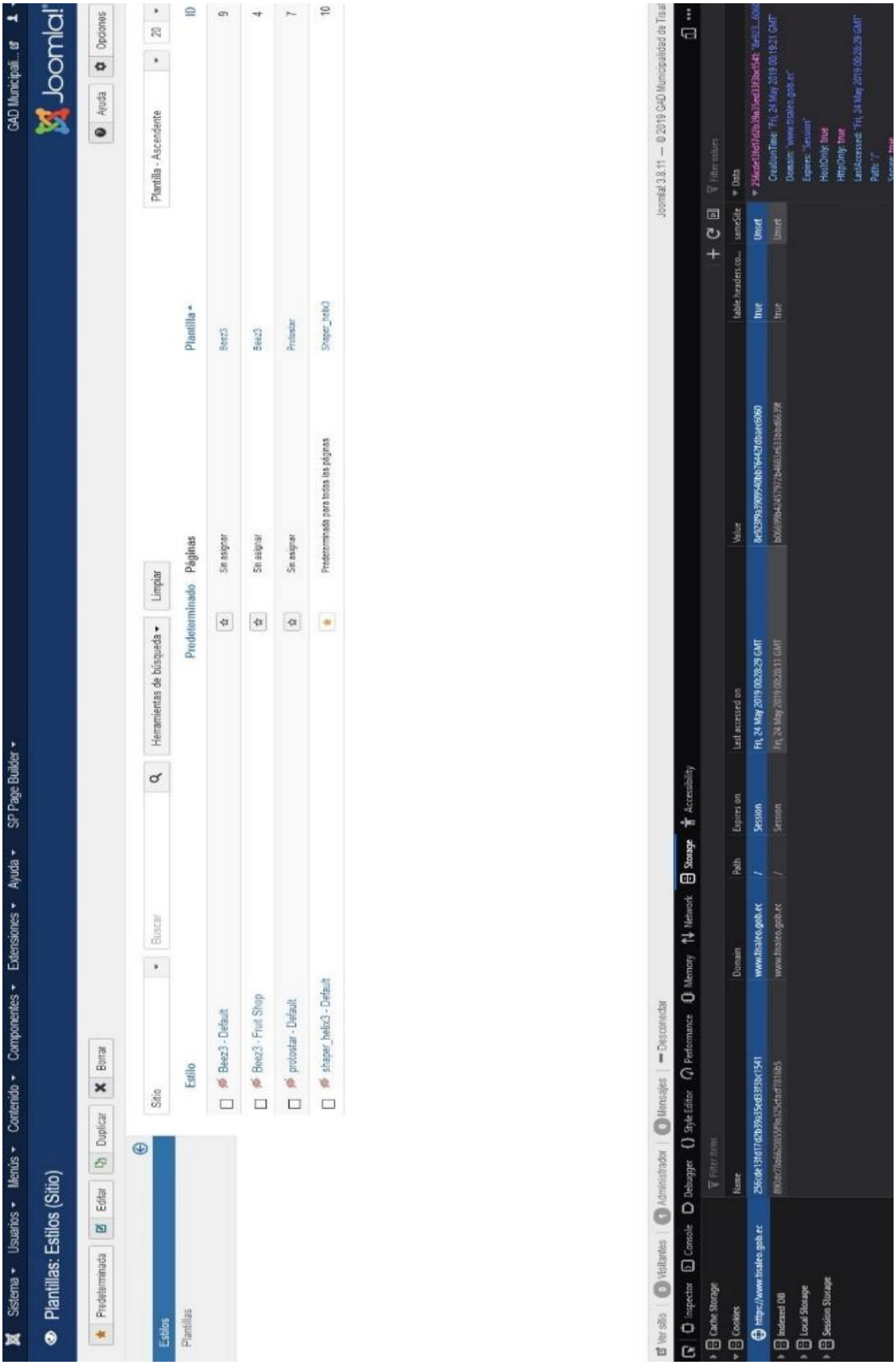


Fuente: elaboración propia

Para motivos del estudio, se usaron dos computadores con *Firefox for Developers*, en el segundo, se pega la *cookie* copiada del primer navegador, se da como resultado el robo de sesión, se logra abrir la interfaz de administrador.

[23] *Firefox for Developers:* es una versión del navegador Firefox creada para los desarrolladores web, la cual contiene herramientas flexibles para hacking.

Figura 76. Resultado del análisis *Firefox for Developers (3)*



Fuente: elaboración propia

Test de arreglo de sesiones

Una prueba de arreglo de sesiones se enfoca más en analizar la vulnerabilidad que existe en el momento en el que una *cookie* de sesión, no se elimina tras cerrar la misma. Esto sucede mientras el propio sitio permite volver a iniciar sesión sin haber cerrado la anterior, de esta manera existe la posibilidad que un atacante robe una cookie de sesión y utilizarla a pesar de que el usuario cerró la sesión.

Dentro de la interfaz del sitio *web* del GAD Municipal de Tisaleo, se encuentra que, para cada sesión, se le otorga una *cookie* distinta, comprobado en el punto anterior, por lo cual, se considera que esta prueba no tuvo éxito y que el sitio *web* es seguro en cuestión al arreglo de sesiones.

Test de funcionalidad de cerrar sesión

En el momento en que un usuario inicia sesión con sus credenciales dentro de cualquier área, es necesario que el mismo pueda finalizar su sesión para que, si alguna otra persona, se acerca a su equipo, no pueda acceder a los parámetros que el usuario maneja.

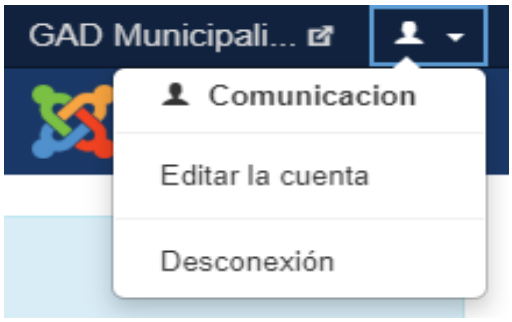
La presente prueba evalúa el aspecto físico del sitio, en el cual, se determina si la disposición de los botones de cerrar sesión existe y son visibles para el usuario.

Figura 77. Plataforma Joomla

Fuente: elaboración propia

Dentro de la interfaz en la parte superior derecha, se observa el símbolo de usuario, dentro del cual al dar *click*, se despliega el menú correspondiente.

Figura 78. Ventana de cierre de sesión



Fuente: elaboración propia

Se consiguió desconectarse de la sesión y, se asegura que si alguien más utiliza la máquina del usuario ésta no pueda tener acceso a los mismos parámetros, por lo cual se, determina que la interfaz de administrador del sitio *web* del GAD Municipal de Tisaleo posee una funcionalidad de cerrar sesión.

***Test* de tiempo de espera de sesión**

Mientras un usuario deja abierta su sesión, pero no está presente en el área de trabajo, la interfaz proporciona la funcionalidad de cerrar de manera automática la sesión para que otra persona no pueda acceder a los parámetros que trabaja el usuario.

En el caso del sitio de administración del GAD Municipal de Tisaleo, se realizó una prueba que consistía en dejar por más de 10 minutos abierta la sesión, pero sin manipularla para verificar la existencia de un cierre de sesión automático, como resultado que la misma no lo posee por lo cual representa una vulnerabilidad grave a la integridad de la información presente dentro del sitio *web*.

3.1.6. Fase VI y VIII - *Test* de Validación de entradas del lado del cliente

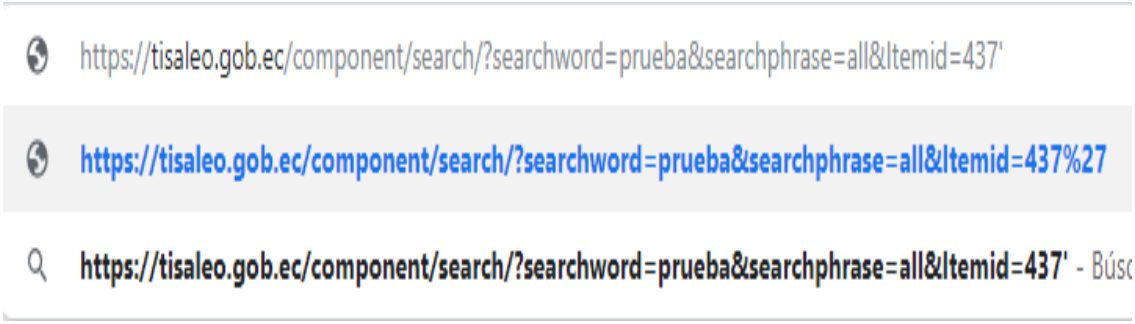
Test* de *Cross-Site Scripting

En la presente prueba, se busca inyectar código dentro del sitio *web* a la espera que el mismo responda con una acción para la cual no estaba programado, esta prueba es utilizada por los atacantes de mayor manera en ataques de *phishing*, mientras el usuario entra a un *link* infectado el atacante es capaz de robar los datos de navegación.

La prueba, que se realiza para la verificación de cumplimiento de la prueba es el añadir un parámetro no esperado por una *url* y verificar cómo reacciona la misma, en este caso,

se utilizará el apóstrofe como objeto de verificación, es un símbolo muy utilizado en programación *javascript*.

Figura 79. Inyección de Código *(')*



Fuente: elaboración propia

Como resultado, se observa que el sitio ignora el apóstrofe, que se transformó por lo cual, se comprueba que el sitio web está protegido contra *XSS*, es decir, que el mismo no es ejecutable desde la *url*.

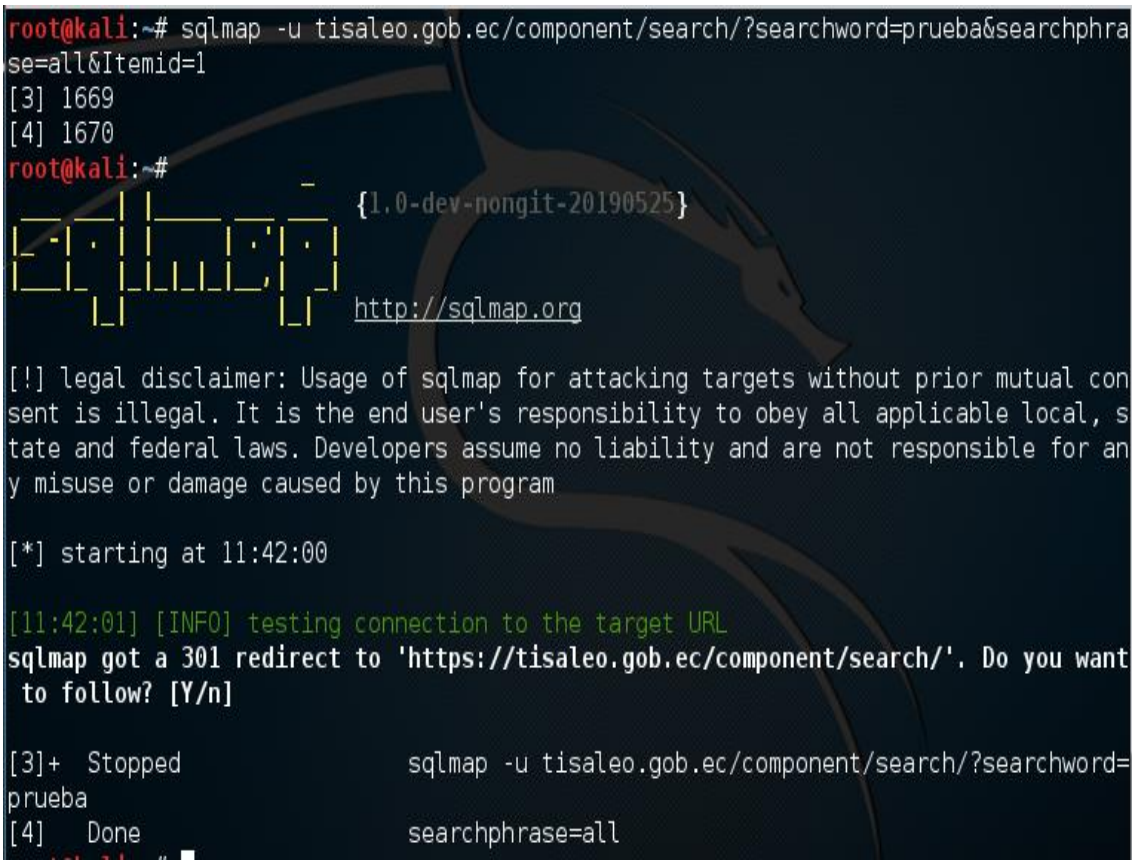
Test* de Inyección *SQL

Una inyección *SQL*[24] consiste en insertar desde el lado del cliente código de consulta para verificar que la página devuelva algún dato, de esa manera capturara información sensible tales como nombres de usuarios o contraseñas cifradas.

Existen varias maneras de verificar la posibilidad de un ataque *SQL*. En primer lugar, se usa la misma prueba para *XSS*[25] el cual no tuvo resultados, después de ello, se utiliza las herramientas de *Kali Linux* para la verificación de la existencia de esta vulnerabilidad.

[24] *Inyección SQL:* Es el ingreso de cogido tipo *SQL* que exponer información de filas o tablas de la base de datos, que se utiliza.
[25] *Cross Site Scripting - XSS:* Utilizado para inyectar código ejecutable en una aplicación *web*, no segura para que realice acciones distintas a las programadas.

Figura 80. Inyección *SQL* con la herramienta *SQLMAP*



Fuente: elaboración propia

Como, se observa, se realizó la prueba, pero sin dar mayores resultados lo cual prueba que el sitio, se encuentra protegido contra inyección *SQL* desde el lado del cliente.

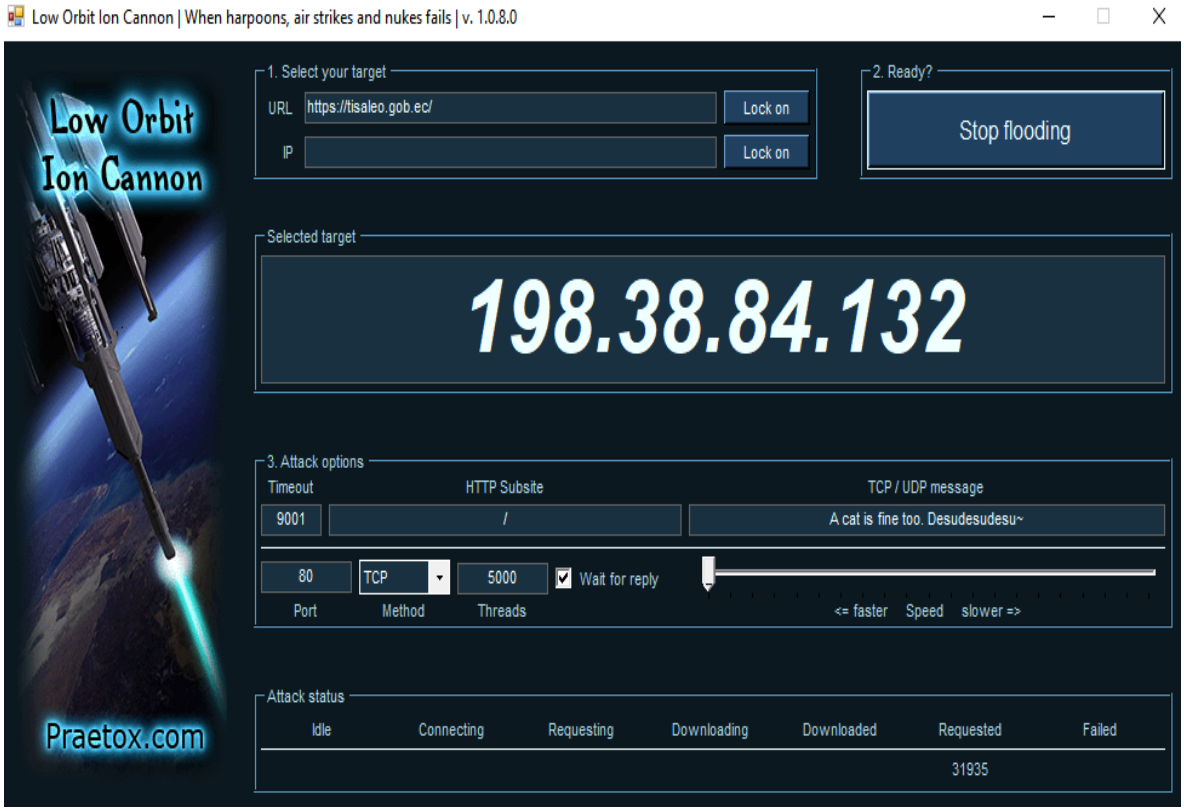
Test de Sobrecarga de *Buffer (DOS)*

El ataque *DOS*[26] (*Denial of Service*) es uno de los mayores problemas para todos los sitios *web* existentes en internet. El mismo consiste en enviar una cantidad inmensa de peticiones hasta que el sitio colapse y no pueda ser accedido. Representa un grave problema que en estos días no exista una manera de detener este tipo de ataques, existe la posibilidad de mitigarlo para que el daño sea mínimo.

Para el presente estudio, se utiliza la herramienta de *Windows Low Orbit Ion Cannon*[27] la cual, se configuró para que ataque con 5000 peticiones cada segundo.

[26] *Ataque DOS* (Denial of Service): Consiste en enviar al objetivo una gran cantidad de peticiones simultaneas, esta sobrecarga evita que la respuesta de los recursos del servidor sea la correcta.
[27] *Windows Low Orbit Ion Cannon - LOIC*: Herramienta utilizada para comprobar que cantidad de tráfico tolerar un objetivo, además, el realizar este tipo de pruebas desde un navegador *web*.

Figura 81. Ataque *DOS* con la herramienta de *Windows LOIC*



Fuente: elaboración propia

De esa manera, se provoca el resultado esperado, el cual es haber iniciado la caída de la página.

Figura 82. Resultado del ataque de *DOS*

Fuente: elaboración propia

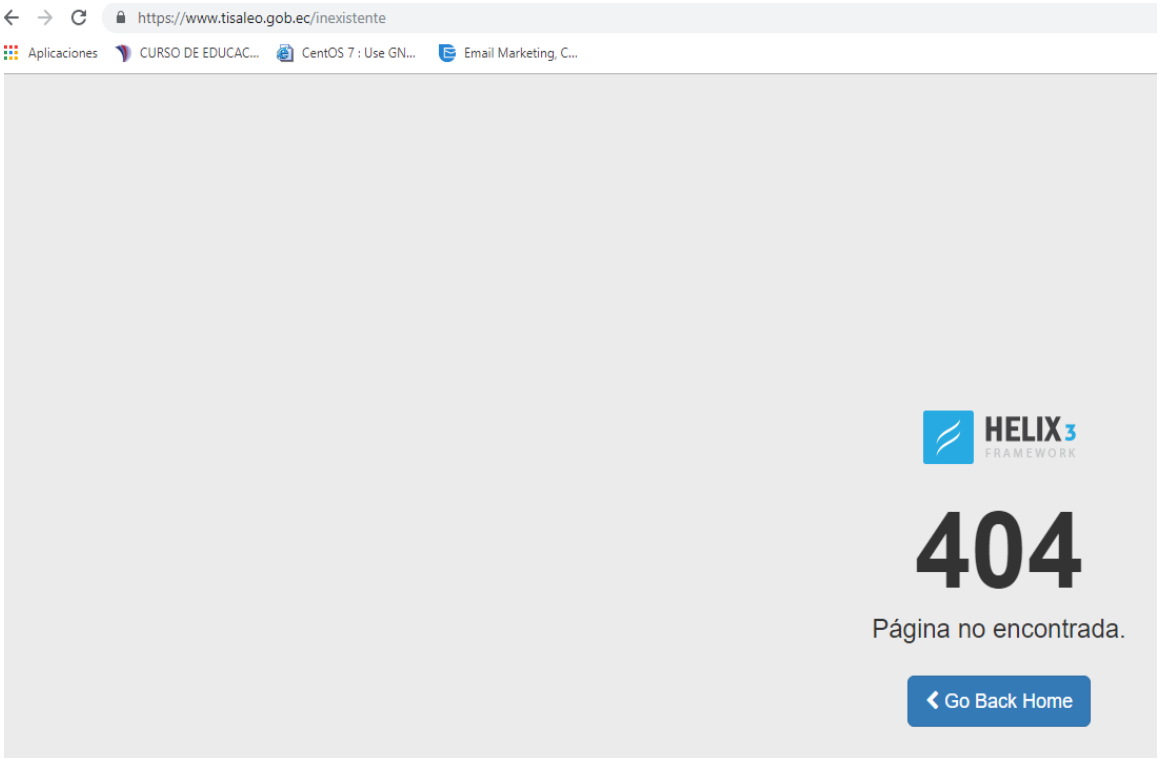
3.1.7. Fase VII - *Test* de Errores

Existencia de un manejo propio de errores

Durante un análisis de vulnerabilidades hacia un sitio *web*, se provocan muchos errores; es posible causar, estos errores mediante solicitudes específicas, dichos errores son muy importantes para un determinado análisis debido a que los mismos revelan mucha información acerca de la base de datos, *bugs* y componentes tecnológicos relacionados con la aplicación y sitio *web*.

Muchas veces los errores son manipulados por el servidor, como, por ejemplo, al realizar una petición que el mismo no reconoce y devuelve datos acerca del sitio *web*, que se utiliza para la presente investigación en cuestión ya sea como el error *404 Not Found*, el mismo, se puso a prueba en el sitio web del GAD Municipal de Tisaleo.

Figura 83. Error 404 Not Found



Fuente: elaboración propia

La figura anterior quiere decir, que se usa la plataforma de *Helix* para el sitio *web*, con esta información, se investiga *exploits* específicos para esta interfaz de desarrollo.

3.2. Diseño de las Estrategias

Después de haber realizado un análisis al sitio *web* del Gobierno Autónomo Descentralizado Municipal de Tisaleo, se utiliza las vulnerabilidades encontradas, se procede a realizar el diseño de procesos correctivos para dichas vulnerabilidades, las cuales serán citadas del punto anterior en orden de impacto hacia el sitio *web* mientras, se sigue la metodología descrita con anterioridad; de la misma manera , se cita el grado de impacto o riesgo existente ante la presciencia de las vulnerabilidades y las estrategias, que se sigue para su respectiva corrección.

Mediante la investigación ejecutada, la metodología *OWASP* plantea diferentes parámetros de solución para varias de las vulnerabilidades encontradas, en el caso de la presente y para los fines oportunos, llevar a cabo soluciones inmediatas; posterior, se enlistará los procesos fundamentales realizados por el administrador del sitio para solucionar de la mejor manera posible las distintas brechas de seguridad existentes.

Dichos procesos fueron diseñados a partir de las soluciones de la metodología *OWASP* que se encuentran en su apartado de análisis de vulnerabilidades en su sitio *web*, se tomó en cuenta el rango de tiempo para el cumplimiento de las mismas y su eficiencia en mitigación de amenazas.

Tabla 9. Vulnerabilidad 1

Vulnerabilidad:	No existe una política para creación de nuevos usuarios, contraseñas y roles	
Apartado:	3.1.	Subsección: 3.1.2. - 3.1.3
Descripción:	Dentro del GAD Municipal de Tisaleo no existe una política para la creación de nuevos usuarios, correos y sus respectivas contraseñas.	
Riesgo:	**Bajo**	
Estrategia:	Crear una política interna para la creación de nuevos usuarios, la definición de roles y sus respectivas contraseñas.	

Fuente: elaboración propia

En la primera vulnerabilidad, se dice que no existe una política para la creación de nuevos usuarios, contraseñas y roles dentro del GAD Municipal de Tisaleo, dicha fragilidad, se encuentra en el apartado 3.3. subsección 3.1.2. y 3.1.3.; la misma, se considera de nivel bajo, no representa mayor riesgo para la seguridad del sitio *web*, porque dentro del GAD Municipal de Tisaleo no existe una política para la creación de nuevos usuarios, correos y sus respectivas contraseñas. La estrategia, que se propone es el crear una política interna para la creación de nuevos usuarios, la definición de roles y sus respectivas contraseñas.

Tabla 10. Vulnerabilidad 2

Vulnerabilidad:	No existe tiempo de espera para el cierre de sesión automático	
Apartado:	3.1.	Subsección: 3.1.4. - 3.1.5.
Descripción:	Al no cerrarse automáticamente una sesión después de un tiempo de inactividad existe la posibilidad de accesos físicos no autorizados.	
Riesgo:	**Bajo**	
Estrategia:	Configurar a la herramienta de manejo de contenidos para que el cierre de sesión del usuario sea automático en un tiempo recomendado de 5 minutos de inactividad.	

Fuente: elaboración propia

Para la segunda vulnerabilidad, se indica que no existe tiempo de espera para el cierre de sesión automático en el GAD Municipal de Tisaleo, dicha fragilidad, se encuentra en el apartado 3.1. subsección 3.1.4. y 3.1.5.; la misma, se considera de nivel bajo, no representa mayor riesgo para el sitio *web* y al no cerrarse automáticamente una sesión después de un tiempo de inactividad existe la posibilidad de accesos físicos no autorizados. La estrategia, que se propone es configurar a la herramienta de manejo de contenidos para que el cierre de sesión del usuario sea automático en un tiempo recomendado de 5 minutos de inactividad.

Tabla 11. Vulnerabilidad 3

Vulnerabilidad:	El acceso a la interfaz de edición y nombres de *plugins* del *CMS Joomla*, se encuentra por defecto	
Apartado:	3.1.	Subsección: 3.1.1 - 3.1.3. - 3.1.4.
Descripción:	Al instalarse la herramienta de manejo de contenidos la misma crea un sitio de *login* el cual, se encuentra por defecto como *administrator* y los *plugins* de manejo de errores crean sus propios mensajes que dejan al descubierto las herramientas utilizadas	
Riesgo:	**Medio**	
Estrategia:	Cambiar el nombre del sitio de *login* de la herramienta *CMS Joomla* Verificar en todas las configuraciones la redirección al nuevo sitio de *login* Cambiar los mensajes de error por defecto a uno propio de la institución	

Fuente: elaboración propia

En la tercera vulnerabilidad, se dice que el acceso a la interfaz de edición y nombres de *plugins* del *CMS Joomla*, se encuentra por defecto dentro del GAD Municipal de Tisaleo, la misma, se encuentra en el apartado 3.1. subsección 3.1.1 - 3.1.3. - 3.1.4. ; la misma, se considera de nivel medio, no representa mayor riesgo para la seguridad del sitio *web*, porque instalarse la herramienta de manejo de contenidos la misma crea un sitio de *login* el cual, se encuentra por defecto como *administrator* y los *plugins* de manejo de errores crean sus propios mensajes que dejan al descubierto las herramientas utilizadas. La estrategia, que se propone es el crear una política interna para la creación de nuevos usuarios, la definición de roles y sus respectivas contraseñas.

Tabla 12. Vulnerabilidad 4

Vulnerabilidad:	Los puertos de acceso a los servicios se encuentran en el estado básico de instalación	
Apartado:	3.1.	Subsección: 3.1.1.
Descripción:	El puerto de acceso a los diferentes servicios del sitio *web*, se encuentran en por defecto, es decir, el estado básico de instalación, esto da oportunidad a una puerta a una intrusión	
Riesgo:	**Medio**	
Estrategia:	Cambiar en la configuración del servidor el número de los puertos para que no coincidan con los dados por defecto en la instalación Verificar todos los archivos de configuración para evitar que los mismos, se encuentren en su estado por defecto	

Fuente: elaboración propia

Para la cuarta vulnerabilidad, se muestra que los puertos de acceso a los servicios se encuentran en el estado básico de instalación en el GAD Municipal de Tisaleo, dicha debilidad, se encuentra en el apartado 3.1. subsección 3.1.1.; la misma, se considera de nivel medio, no representa mayor riesgo para el sitio *web* y el puerto de acceso a los diferentes servicios del sitio *web*, se encuentran en por defecto, es decir, el estado básico de instalación, esto da oportunidad a una puerta a una intrusión. Las estrategias, que se proponen son: primero, cambiar en la configuración del servidor el número de los puertos para que no coincidan con los dados por defecto en la instalación, y segundo, verificar todos los archivos de configuración para evitar que los mismos, se encuentren en su estado por defecto.

Tabla 13. Vulnerabilidad 5

Vulnerabilidad:	En la búsqueda de *Google*, se encontró la interfaz de acceso para el administrador del servidor.	
Apartado:	3.1.	Subsección: 3.1.1.
Descripción:	Se encuentra mediante una búsqueda en la herramienta *Google* el acceso para la administración detallada en el apartado	
Riesgo:	**Alto**	
Estrategia:	Retirar todos los accesos mediante motores de búsqueda Crear accesos únicos a través de direcciones *ip* internas	

Fuente: elaboración propia

En la quinta vulnerabilidad, se enseña que, en la búsqueda de *Google*, se encontró la interfaz de acceso para el administrador del servidor, dicha fragilidad, se encuentra en el apartado 3.1. subsección 3.1.1; la misma, se considera de nivel alto, representa un riesgo para el sitio *web*, porque, se encuentra mediante una búsqueda en la herramienta *Google* el acceso para la administración detallada en el apartado. Las estrategias, que se proponen son: primero, retirar todos los accesos mediante motores de búsqueda, segundo, crear accesos únicos a través de direcciones *ip* internas.

Tabla 14. Vulnerabilidad 6

Vulnerabilidad:	Existe la posibilidad de robo de cookie de sesión y que sea accedida desde otro lugar	
Apartado:	3.1.	Subsección: 3.1.4. – 3.15.
Descripción:	No existe un mecanismo que no permita la conexión simultanea de dos sesiones idénticas	
Riesgo:	**Alto**	
Estrategia:	Al ser robada una *cookie* de sesión y ser accedida desde otro lugar, existe la posibilidad de crear una regla que detecte el uso de la misma cookie y no permita su ingreso, se alerta al usuario del intento de acceso no autorizado (Ejemplo *WhatsApp Web*) Incluir un *token* en la sesión y en el navegador para cada *request*, y así, se verifica que el ingreso fue del mismo servidor y no un atacante	

Fuente: elaboración propia

Para la sexta vulnerabilidad existe la posibilidad de robo de cookie de sesión y que sea accedida desde otro lugar, dicha vulnerabilidad, se encuentra en el apartado 3.1. subsección 3.1.4. y 3.1.5.; la misma, se considera de nivel alto, representa un riesgo para el sitio *web*, a causa de que no existe un mecanismo que no permita la conexión simultanea de dos sesiones idénticas. Las estrategias, que se proponen son: primero, al ser robada una *cookie* de sesión y ser accedida desde otro lugar, se dice que el crear una regla que detecte el uso de la misma cookie y no permita su ingreso, se alerta al usuario del intento de acceso no autorizado (Ejemplo *WhatsApp Web*) y, por último, incluir un *token* en la sesión y en el navegador para cada *request*, y así, se verifica que el ingreso fue del mismo servidor y no un atacante.

Tabla 15. Vulnerabilidad 7

Vulnerabilidad:	El puerto de acceso remoto *SSH*, se encuentra por defecto y abierto externamente.	
Apartado:	3.1.	Subsección: 3.1.1.
Descripción:	Es posible acceder desde un computador externo al servicio *SSH* dado que el puerto de igual manera se encuentra por defecto y abierto pude existir ataques de fuerza bruta	
Riesgo:	**Alto**	
Estrategia:	Modificar en la configuración del servicio el puerto de acceso Crear una regla de proxy para que el acceso a este servicio sea solo por direcciones *ip* confiables En caso de requerir mayor seguridad, se expone que el crear una regla para verificar direcciones *IP* y *MAC* para que solo el equipo del administrador tenga acceso	

Fuente: elaboración propia

En la séptima vulnerabilidad, se muestra que en el puerto de acceso remoto *SSH*, se encuentra por defecto y abierto externamente, dicha debilidad, se encuentra en el apartado 3.1. subsección 3.1.1; la misma, se considera de nivel alto, representa un riesgo para el sitio *web*, porque es posible acceder desde un computador externo al servicio *SSH* dado que el puerto de igual manera se encuentra por defecto y abierto pude existir ataques de fuerza bruta. Las estrategias, que se proponen son: primero, modificar en la configuración del servicio el puerto de acceso, segundo, crear una regla de proxy para que el acceso a este servicio sea solo por direcciones ip confiables, y para finalizar, en caso de requerir mayor seguridad, se explica que el crear una regla para verificar direcciones *IP* y *MAC* para que solo el equipo del administrador tenga acceso.

Tabla 16. Vulnerabilidad 8

Vulnerabilidad:	Versión de *Joomla* desactualizada	
Apartado:	3.1.	Subsección: 3.1.3.
Descripción:	La versión encontrada es 3.8.11 pero la actual 3.9.6 lo cual provocar graves fallos al ser vulnerable a ataques que ya son públicos y han sido parchados en versiones posteriores	
Riesgo:	**Alto**	
Estrategia:	Realizar un programa de actualización a la herramienta de manejo de contenidos Actualizar *plugins* dentro del *CMS*	

Fuente: elaboración propia

Para la octava vulnerabilidad, se dice que la versión de *Joomla* está desactualizada, dicha vulnerabilidad, se encuentra en el apartado 3.1. subsección 3.1.3.; la misma, se considera de nivel alto, representa un riesgo para el sitio *web*, porque, se encontró el sitio en la versión 3.8.11 pero la actual es 3.9.6 lo cual provoca graves fallos al ser vulnerable a ataques que ya son públicos y han sido parchados en versiones posteriores. Las estrategias, que se proponen son: primero, realizar un programa de actualización a la herramienta de manejo de contenidos, y segundo actualizar *plugins* dentro del *CMS.*

Tabla 17. Vulnerabilidad 9

Vulnerabilidad:	No se encuentra configurado un mecanismo de cierre automático adecuado ante ataques de fuerza bruta	
Apartado:	3.1.	Subsección: 3.1.4. – 3.1.5.
Descripción:	El sitio web de *login* para la interfaz de administración permite un número infinito de intentos para poder acceder	
Riesgo:	**Alto**	
Estrategia:	Crear reglas de mecanismo de cierre para evitar ataques de fuerza bruta Como sugerencia que al quinto intento exista un tiempo de espera de 60 segundos y, se refresque la cookie de sesión de esa manera, un atacante vuelve a configurar el programa de ataque	

Fuente: elaboración propia

En la novena vulnerabilidad, se muestra que, no se encuentra configurado un mecanismo de cierre automático adecuado ante ataques de fuerza bruta, dicha vulnerabilidad, se encuentra en el apartado 3.1. subsección 3.1.4. y 3.1.5.; la misma, se considera de nivel alto, representa un riesgo para el sitio *web*, porque el sitio web de *login* para la interfaz de administración permite un número infinito de intentos para poder acceder. Las estrategias, que se proponen son: primero, crear reglas de mecanismo de cierre para evitar ataques de fuerza bruta, para finalizar, como sugerencia, se recomienda que, al quinto intento exista un tiempo de espera de 60 segundos y, se refresque la cookie de sesión de esa manera, un atacante vuelve a configurar el programa de ataque.

Tabla 18. Vulnerabilidad 10

Vulnerabilidad:	El sitio *web* queda inhabilitado al ser atacado mediante sobrecarga de *buffer* (Ataque *DOS*)	
Apartado:	3.1.	Subsección: 3.1.6.
Descripción:	Existe la posibilidad de realizar este tipo de ataque en mayor escala y dar de baja tanto al sitio web como al servidor.	
Riesgo:	**Alto**	
Estrategia:	Al ser un ataque el cual es imposible detener, se recomiendan acciones para mitigar los daños que pueda causar Al ser una página gubernamental el servidor maneja una cantidad muy grande de peticiones lo cual mitiga en gran medida los ataques Se recomienda, en lo posible, utilizar equipos antiguos como servidores de balanceo de carga los cuales serán la primera línea de defensa ante este tipo de ataques	

Fuente: elaboración propia

Para la décima vulnerabilidad, se dice menciona que el sitio *web* queda inhabilitado al ser atacado mediante sobrecarga de *buffer* (Ataque *DOS*), dicha fragilidad, se encuentra en el apartado 3.1. subsección 3.1.6.; la misma, se considera de nivel alto, representa un riesgo para el sitio *web*, porque, se encontró el sitio en la versión 3.8.11 pero la actual es 3.9.6 lo cual provoca graves fallos al ser vulnerable a ataques que ya son públicos y han sido parchados en versiones posteriores. Las estrategias, que se proponen son: primero, al ser un ataque el cual es imposible detener, se recomiendan acciones para mitigar los daños que pueda causar, segundo, al ser una página gubernamental el servidor maneja una cantidad muy grande de peticiones lo cual mitiga en gran medida los ataques, tercero, se recomienda, en lo posible, utilizar equipos antiguos como servidores de balanceo de carga los cuales serán la primera línea de defensa ante este tipo de ataques.

3.3. Validación de Resultados

Para proceder con la validación de los resultados de la presente investigación, se realizó un informe el cual, se presentó al personal de la Unidad de Tecnología del GAD Municipal de Tisaleo, la ya mencionada, se encuentra anexado en Anexos 2, en la cual facilitó la información para proceder con las pruebas que propone la metodología *OWASP*, es necesario mencionar que con el resultado del análisis el equipo podrá corregir las vulnerabilidades que, se encontraron en la presente al sitio *web*; además, se observa que el certificado de culminación del proyecto y la satisfacción por parte de la entidad.

CONCLUSIONES

- Como punto inicial de la presente investigación, se fundamentó teóricamente los epígrafes tal como: Seguridad Informática, Objetivos de la Seguridad Informática, Integridad de la Información, Análisis de Riesgos, la conceptualización de los distintos subtemas de este estudio investigativo, lo cual permitió entender de mejor manera cada uno de los temas ya mencionados para la construcción del producto del estudio.

- Inmediatamente se procedió a realizar un análisis de riesgos que permitió identificar las vulnerabilidades, riesgos, amenazas sobre la información digital en el GAD Municipal de Tisaleo.

- Después del análisis, se realizó al sitio *web,* se identificó un número considerable de vulnerabilidades críticas, por lo, que se evaluaron las mismas ante ataques definidos por la *OWASP Top 10*.

- Por medio de una reunión con el jefe de la Unidad de Tecnología del GAD Municipal de Tisaleo, se validó el estudio mediante el cumplimiento de los diseños correctivos, los cuales fueron entregados en un informe del análisis correspondiente, además, se logró contemplar que las autoridades, se encontraron complacidas con tal.

RECOMENDACIONES

- Se propone al personal de la Unidad de Tecnología del GAD Municipal de Tisaleo profundizar los axiomas, definiciones e ideas de todo lo que abarca la seguridad informática para tener un entendimiento conceptual al momento del análisis del sitio *web*.

- Se recomienda al GAD Municipal de Tisaleo realizar periódicamente análisis de seguridad informática para evitar riesgos y así garantizar el correcto funcionamiento del sitio *web* para los usuarios.

- Se sugiere actualizar los sistemas operativos, de esta manera, se evita posibles intrusiones, las versiones desactualizadas tienen fallas de seguridad que en la mayoría de las veces en la siguiente versión son parcheados.

- Se aconseja realizar un ejercicio de *Hacking Ético* de manera periódica puesto que permitirá verificar si las vulnerabilidades identificadas con anterioridad fueron corregidas y al mismo tiempo examinar si, se encuentra alguna debilidad en las aplicaciones *web* que maneja la municipalidad, para corregirlas lo más pronto posible.

BIBLIOGRAFÍA

Aguilera Gonzalez, D., Guitierrez Perez, M., & Perez Bernal, L. (2016). Deteccion y mitigacion de ataques ARP en la Red Corporativa de la division territorial Holguin, ETECSA. *Revista Digital de las Tecnologias de la Informacion y las Comunicaciones Telem@tica*, 7.

Allsopp, W. (2017). *Advanced Penetration Testing: Hacking the World's Most Secure Networks.* (J. Wiley, & &. Sons, Edits.) Indianápolis, Indiana, Estados Unidos: Wiley. Obtenido de https://books.google.com.ec/books?id=xukgDgAAQBAJ&dq=Advanced+penetration+testing+wil+allsopp&lr=&hl=es&source=gbs_navlinks_s

Auditoria, Consejo, Instalación y Seguridad de Sistemas de Información. (2018). Seguridad informática - Hacking Ético: Conocer el ataque para una mejor defensa (4ª edición). Barcelona, España: ENI.

Baca, G. (2016). Introducción a la seguridad informática. México: Patria.

Baena Paz, G. (2017). En *Metodología de la Investigación* (pág. 156). México D.F: Patria.

Barrio, M. (2017). Ciberdelitos: amenazas criminales del ciberespacio: Adaptado reforma Código Penal 2015 . Madrid: Reus.

Campos, M. (2017). Métodos de Investigación Académica Fundamentos de Investigación Bibliográfica. *ICOMOSCR.ORG*, 84.

Cano, J. (2016). *ISACA.* Obtenido de Journal: https://www.isaca.org/Journal/archives/2016/volume-5/Pages/cyberattacks-the-instability-of-security-and-control-knowledge.aspx

Cañadas Osinski, I., & San Luis Costas, C. (2018). *Análisis de datos en investigación. Primeros pasos.* Elche, España: Universidad Miguel Hernández.

Coronado, S. (Enero de 2017). *Repositorio PUCE.* Obtenido de http://repositorio.puce.edu.ec/bitstream/handle/22000/13157/Tesis%20Steven%20Coronado.pdf?sequence=1&isAllowed=y

Gómez, O. (21 de Marzo de 2017). *CISCO*. Obtenido de Blog Cisco Latinoamérica: https://gblogs.cisco.com/la/sg-oscargomez-la-seguridad-informatica-es-responsabilidad-de-toda-la-empresa/

González, H. R., & Montesino, R. (2018). Capacidades de las metodologías de pruebas de penetración para detectar vulnerabilidades frecuentes en aplicaciones web. *Scielo*.

Guallpa, L. G. (Octubre de 2017). *Dspace*. Obtenido de Uniandes: http://dspace.uniandes.edu.ec/handle/123456789/6762

Guevara, C. B. (Abril de 2017). *Eprints UCM*. Obtenido de Universidad Complutense de Madrid: http://eprints.ucm.es/46037/1/T39510.pdf

Halton, W., Weaver, B., Ahmed, J., Rao, S., & Imran, M. (2017). Major Flaws in Web Applications. En W. Halton, B. Weaver, J. Ahmed, S. Rao, & M. Imran, *Penetration Testing: A Survival Guide* (pág. 1045). Birmingham: Packt.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. d. (2014). *Metodología de la Investigación Sexta Edición.* Ciudad de México: McGraw-Hill/ Interamericana Editores.

Insitituto Vasco de Estadistica . (27 de Septiembre de 2018). *Eustat.* Obtenido de http://www.eustat.eus/document/datos/ct_02_c.pdf

Machaca, A. (22 de Enero de 2018). *OWASP ORG*.

Mastrian, K., & McGonigle, D. (2016). Informatics for Health Professionals. Estados Unidos: Jones & Barlett Learning .

McDonough, B. (2019). *Cyber Smart: Five habits to protect your family, money, ad identity from cyber criminals.* Indianapolis, Indiana: Wiley & Sons.

Modarres, M., Kaminskiy, M., & Krivtsov, V. (2016). Reliability Engineering and Risk Analysis. *Taylor & Francis Group*, CRC Press.

Montenegro, K. S. (Marzo de 2018). *Repositorio Universidad de Guayaquil.* Obtenido de Repositorio Nacional en Ciencia y Tecnologia: http://repositorio.ug.edu.ec/bitstream/redug/27047/1/B-CINT-PTG-N.262%20Montenegro%20Avata%20Karina%20Stefany.pdf

Mora Ortega, A. (22 de Noviembre de 2017). *Repositorio Universidad de Cuenca.* Obtenido de http://dspace.ucuenca.edu.ec/bitstream/123456789/28552/1/Trabajo%20de%20titulaci%C3%B3n.pdf

Najera-Gutierrez, G., & Ahmed Ansari, J. (2018). Chapter 1: Introduction to Penetration Testing and Web Applications Proactive Security Testing. En G. Najera-Gutierrez, & J. Ahmed Ansari, *Web Penetration Testing with Kali Linux: Explore the methods and tools of ethical hacking with Kali Linux, 3rd Edition* (pág. 426). Birmingham: Packt Publishing.

Open Web Application Security Project . (22 de Agosto de 2018). *OWASP*. Obtenido de Membership: https://www.owasp.org/index.php/Membership

Open Web Application Security Project . (14 de Marzo de 2019). *OWASP*. Obtenido de About_The_Open_Web_Application_Security_Project: https://www.owasp.org/index.php/About_The_Open_Web_Application_Security_Project

Open Web Application Security Project. (31 de Agosto de 2008). *OWASP*. Obtenido de Proyecto de Pruebas de OWASP: https://www.owasp.org/index.php/Proyecto_de_Pruebas_de_OWASP

Open Web Application Security Project. (7 de Mayo de 2017). *OWASP*. Obtenido de OWASP Testing Guide v4 Table of Contents: https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents

Open Web Application Security Project. (25 de Enero de 2019). *OWASP*. Obtenido de About The Open Web Application Security Project: https://www.owasp.org/index.php/About_The_Open_Web_Application_Security_Project

Open Web Application Security Project Foundation. (2015). *Guía de Pruebas OWASP.*

Patiño, S., Mosquera, C., Suárez, F., & Nevarez, R. (Diciembre de 2017). *Universidad, Ciencia y Tecnología.* Obtenido de Revista de la Universidad Nacional Experimental Politecnica "Antonio José de Sucre": http://www.uct.unexpo.edu.ve/index.php/uct/article/view/805/648

Quiroz , S., & Macías, D. (2017). Seguridad en Informática: Consideracione. *Dominio de las Ciencias*, 13.

Quiroz Zambrano, S., & Macías Valencia, D. (2017). Seguridad en Informática. *Dialnet*, 13.

Red Hat, Inc. (2005). *Red Hat Enterprise Linux 4: Manual de seguridad*. Obtenido de Massachusetts Institute of Technology: http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/s1-sgs-ov-controls.html

Rocha, Á., Correia, A. M., Reis, L., Mnosça, M., & Adeli, H. (2016). New Advances in Information Systems and Technologies. Portugal: Springer.

Rodriguez, A., & Pérez, A. (1 de Marzo de 2017). Metodos científicos de indagación y de construcción del conocimiento. *Revista EAN*, 22. Obtenido de http://www.scielo.org.co/pdf/ean/n82/0120-8160-ean-82-00179.pdf

Romero Castro, M., Figueroa Morán, G., Vera Navarrete, D., Álava Cruzatty, J., Parrales Anzúles, G., Álava Mero, C., . . . Castillo Merino, M. (2018). *Introducción a la Seguridad Informática y el Análisis de Vulnerabilidades.* 3Ciencias.

Stefinko, Y., & Piskuzub, A. (2017). Theory of Modern Penetration Testing Expert System. *Biblioteca Nacional de Ucrania VI Vernadsky*, 2.

Superintendencia Nacional de Salud de Colombia. (Junio de 2018). *Guía de Metodología de Análisis de Riegos de Seguridad y Privacidad de la Información Superintendencia Nacional de Salud.* Obtenido de https://docs.supersalud.gov.co/PortalWeb/planeacion/AdministracionSIG/ASGU05.docx

ANEXOS

Anexo 1: Entrevista al Gobierno Autónomo Descentralizado Municipal de Tisaleo y encuestas a los municipios de Ambato, Cevallos, Quero y el Honorable Gobierno Provincial de Tungurahua

ENTREVISTA AL PERSONAL DE LA UNIDAD DE TECNOLOGIA DEL GOBIERNO AUTONOMO DESCENTRALIZADO MUNICIPAL DE TISALEO

INDICACIONES GENERALES:

Esta entrevista tiene como fin recopilar datos sensibles que se manejan en las aplicaciones *web*; posteriormente será de utilidad para el desarrollo de las estrategias para la protección de las mismas.

CUESTIONARIO:

1. ¿Qué medidas tiene para asegurar la información y el acceso de la aplicación web que maneja el municipio? y que protocolos utiliza?

2. ¿Cuántas personas existen con acceso de administrador de la aplicación? y cuáles son las razones?

3. ¿Cuál es el proceso de creación de nuevos usuarios?

¿Qué tipo de credenciales usa para la creación de los usuarios?

¿Existe exigencias por parte de la aplicación para el tipo de contraseñas que se ingresan?

4. Se basa en alguna norma/estándar para garantizar la seguridad informática?

5. ¿Cree usted que necesitaría de consultoría externa para garantizar mejores procesos de seguridad informática?

6. Se ha capacitado en éstos últimos 2 años en protocolos de respuesta a incidentes informáticos?

7. Tiene usted respaldos de la información sensible del municipio? Y ¿En dónde la almacena?

8. ¿Cómo gestiona los respaldos en caso de existir un incidente informático?

9. Considera adecuado el grado de seguridad general que ofrece la aplicación?

10. Ha sufrido la aplicación algún ataque o un acceso indebido?

11. Si hubo un ataque a la aplicación, ¿qué información y que cantidad se perdió?

12. ¿Si la información se perdió, cuanto tiempo se tardó en recuperarla? Y del 100% de información perdida cuanto recupero?

_____

ING. HUGO LEONIDAS FREIRE

ANALISTA PROGRAMADOR

ENTREVISTA AL DIRECTOR DE TECNOLOGIAS DE LA INFORMACION DEL GOBIERNO AUTONOMO DESCENTRALIZADO MUNICIPAL DE -

INDICACIONES GENERALES:

Esta entrevista tiene como fin recopilar datos sensibles que se manejan en las aplicaciones *web*; posteriormente será de utilidad para el desarrollo de las estrategias para la protección de las mismas.

CLAUSULAS DE CONFIDENCIALIDAD:

Yo, Pamela Jazmín Parra Zamora con cedula 1804041885 me comprometo a que el contenido de esta entrevista no va a ser compartido y me obligo en forma irrevocable ante el GADM del Cantón - a no revelar, divulgar o facilitar bajo cualquier forma a persona alguna sea natural o jurídica, pública o privada, o de cualquier otra naturaleza, y a no utilizar para su propio beneficio o para beneficio de un tercero, toda la información generada durante la vigencia de la presente investigación.

CUESTIONARIO:

1. ¿Qué mecanismos tiene para asegurar la información y el acceso de las aplicaciones *web* que maneja el municipio? y que protocolos utiliza?

2. ¿Cuántas personas existen con acceso de administrador de las aplicaciones *web*? y cuáles son las razones?

3. Se basa en alguna norma/estándar para garantizar la seguridad informática?

4. ¿Cree usted que necesitaría de consultoría externa para garantizar mejores procesos de seguridad informática?

5. Se ha capacitado en éstos últimos 2 años en protocolos de respuesta a incidentes informáticos?

6. Ha sufrido la aplicación algún ataque o un acceso indebido?

7. Si hubo un ataque a la aplicación, ¿qué información y que cantidad se perdió?

8. ¿Si la información se perdió, cuanto tiempo se tardó en recuperarla? Y del 100% de información perdida cuanto recupero?

_____

ING.

DIRECTOR DE TI-

ENTREVISTA AL DIRECTOR GENERAL DE SISTEMAS DEL HONORABLE GOBIERNO PROVINCIAL DE TUNGURAHUA

INDICACIONES GENERALES:

Esta entrevista tiene como fin recopilar datos sensibles que se manejan en las aplicaciones *web*; posteriormente será de utilidad para el desarrollo de las estrategias para la protección de las mismas.

CLAUSULAS DE CONFIDENCIALIDAD:

Yo, Pamela Jazmín Parra Zamora con cedula 1804041885 me comprometo a que el contenido de esta entrevista no va a ser compartido y me obligo en forma irrevocable ante el Honorable Gobierno Provincial de Tungurahua a no revelar, divulgar o facilitar bajo cualquier forma a persona alguna sea natural o jurídica, pública o privada, o de cualquier otra naturaleza, y a no utilizar para su propio beneficio o para beneficio de un tercero, toda la información generada durante la vigencia de la presente investigación.

CUESTIONARIO:

1. ¿Qué mecanismos tiene para asegurar la información y el acceso de las aplicaciones *web* que maneja el Gobierno Provincial? y que protocolos utiliza?
2. ¿Cuántas personas existen con acceso de administrador de las aplicaciones *web*? y cuáles son las razones?
3. Se basa en alguna norma/estándar para garantizar la seguridad informática?
4. ¿Cree usted que necesitaría de consultoría externa para garantizar mejores procesos de seguridad informática?
5. ¿Se ha capacitado en éstos últimos 2 años en protocolos de respuesta a incidentes informáticos?
6. ¿Ha sufrido la aplicación algún ataque o un acceso indebido?

7. Si hubo un ataque a la aplicación, ¿qué información y que cantidad se perdió?

8. ¿Si la información se perdió, cuanto tiempo se tardó en recuperarla? Y del 100% de información perdida cuanto recupero?

_____

ING. XAVIER FRANCISCO LOPEZ

DIRECTOR GENERAL DE SISTEMAS

Anexo 2: Informe final presentado al GAD Municipal de Tisaleo

Informe de Estrategias para GAD Municipal de Tisaleo

Introducción

La presente investigación es de suma importancia para la comunidad tisaleña, en el sitio web, se encuentra información sensible sobre Consulta de Impuestos, Facturación Electrónica, pagos a la Empresa Pública Mancomunada de Tránsito de Tungurahua, pagos de Impuestos, Servicios Básicos, información sobre Planificación y Catastros, Obras Sociales, Turismo, Líneas de Fábrica, Permisos de cerramiento, Permisos de Trabajos Varios, aprobación de Planos Arquitectónicos y Estructurales, permiso de Construcción, aprobación de Fraccionamiento Urbano, aprobación de Fraccionamiento Rural, aprobación de Lotizaciones y urbanizaciones, edificaciones especiales, aprobación de Propiedad Horizontal, excedente de Área, titularización de Predios urbanos, certificado de uso de suelo, resellado de trámites municipales aprobados, informes técnicos, patentes, exoneración de impuestos-tercera edad, exoneración de impuestos-discapacidad, exoneración del servicio de agua potable.

Actualmente no, se ha explorado a profundidad el campo de la seguridad informática dentro de los sitios *web* propias del GAD Municipal de Tisaleo, por lo cual el presente proyecto de investigación representa una innovación adecuada para la comunidad universitaria.

Para la investigación, se contó con la asesoría del administrador del sitio *web* del GAD Municipal de Tisaleo, en el cual, se realizó pruebas de los diferentes tipos de ataques que hoy en día son los más comprometedores para las entidades que tienen funciones virtuales.

Los primordiales beneficiarios del presente proyecto será la comunidad tisaleña en general, las empresas que se encuentran ubicadas en el Cantón Tisaleo y el personal del GAD Municipal de Tisaleo, la colectividad disfrutará de la seguridad de sus datos personales tales como número de cédula, áreas de terreno, cuentas de agua potable, cuenta de luz eléctrica, predios urbanos y rural, líneas de fábrica, permisos de cerramientos, permisos de construcción, patentes y algo muy importante los enlaces a otras sitios *web* del Gobierno del Ecuador que aloja el sitio *web* del GAD Municipal de Tisaleo tal como *Quipux-Gestión Documental, SERCOP,* a más de dar confianza de que, se mantendrá siempre confiable y que los datos enviados no serán vulnerados, los archivos recibidos estarán correctamente procesados, no obstante, el administrador del sitio *web* podrá estar seguro de que no existan

ataques que sean un riesgo para los servidores, también, de existirlos contarán con metodologías que permitan reducir dichos ataques de manera sencilla sin alterar el funcionamiento principal del mismo.

El presente proyecto de investigación, se realizó en base a la metodología *OWASP* para la cual, se usó las siguientes herramientas que serán descritas brevemente: navegadores como *Google hacking* y *Firefox for Developers*, máquinas virtuales como *Oracle VM Virtual Box* y *VMware Workstation*, sistemas operativos como *Kali Linux* y *Microsoft Windows XP,7, 10*, complementos de *Kali Linux*, varios comandos, y ciertas herramientas externas, además, mediante el uso de un *checklist* para verificar cada uno de los puntos correspondientes a la misma.

Objetivo

Desarrollar estrategias para la protección de la Integridad de la Información digital del Gobierno Autónomo Descentralizado Municipal de Tisaleo.

Checklist: Fase I Recolección de Información		
Identificación de la Auditoria		
Institución Auditada: Gobierno Autónomo Descentralizado Municipal de Tisaleo		
Proyecto: Análisis de vulnerabilidades y diseño de procesos correctivos del sitio web del Gobierno Autónomo Descentralizado Municipal de Tisaleo **Tipo de Auditoria:** ○ Interna ○ Externa		
Auditor		
Nombre: Pamela Jazmín Parra Zamora		
Correo Electrónico: pamela.j.parra.z@pucesa.edu.ec / pamelaparra19@yahoo.com		
Teléfono: 0987896039 / 0984639237		
Checklist		
¿Existe vulnerabilidad?	**Si**	**No**
a) Uso de un motor de búsqueda para verificación de existencia de información vulnerable	X	
b) Análisis general de las aplicaciones web	X	
c) Recolección de metadatos del sistema para la comprobación de existencia de información vulnerable	X	
d) Identificación de puntos de entrada a la aplicación		X
e) Análisis al entorno de la aplicación web	X	
f) Análisis y mapa de arquitectura de la aplicación		X

Checklist: Fase II Test de Manejo de Configuración y Desarrollo
Identificación de la Auditoria
Institución Auditada: Gobierno Autónomo Descentralizado Municipal de Tisaleo

Proyecto: Análisis de vulnerabilidades y diseño de procesos correctivos del sitio web del Gobierno Autónomo Descentralizado Municipal de Tisaleo **Tipo de Auditoria:** o Interna o Externa
Auditor
Nombre: Pamela Jazmín Parra Zamora
Correo Electrónico: pamela.j.parra.z@pucesa.edu.ec / pamelaparra19@yahoo.com
Teléfono: 0987896039 / 0984639237
Checklist

¿Existe vulnerabilidad?	**Si**	**No**
a) Test de configuración e infraestructura de la red	X	
b) Test de las extensiones de los archivos que manejan información sensible		X
c) Test de transporte de seguridad estricto HTTP	X	

Checklist: Fase III Test de manejo de identidad
Identificación de la Auditoria
Institución Auditada: Gobierno Autónomo Descentralizado Municipal de Tisaleo
Proyecto: Análisis de vulnerabilidades y diseño de procesos correctivos del sitio web del Gobierno Autónomo Descentralizado Municipal de Tisaleo **Tipo de Auditoria:**

○ Interna ○ Externa
Auditor
Nombre: Pamela Jazmín Parra Zamora
Correo Electrónico: pamela.j.parra.z@pucesa.edu.ec / pamelaparra19@yahoo.com
Teléfono: 0987896039 / 0984639237
Checklist

¿Existe vulnerabilidad?	**Si**	**No**
a) Test de definición de roles	X	
b) Test de proceso de registro de nuevos usuarios	X	
c) Test de procesos de creación de nuevas cuentas	X	
d) Test para políticas de uso de nombres de usuarios débiles o sin seguridades	X	

Checklist: Fase IV Test de Autenticación
Identificación de la Auditoria
Institución Auditada: Gobierno Autónomo Descentralizado Municipal de Tisaleo
Proyecto: Análisis de vulnerabilidades y diseño de procesos correctivos del sitio web del Gobierno Autónomo Descentralizado Municipal de Tisaleo **Tipo de Auditoria:** ○ Interna ○ Externa

Auditor		
Nombre: Pamela Jazmín Parra Zamora		
Correo Electrónico: pamela.j.parra.z@pucesa.edu.ec / pamelaparra19@yahoo.com		
Teléfono: 0987896039 / 0984639237		
Checklist		
¿Existe vulnerabilidad?	**Si**	**No**
a) Test de credenciales transportadas en un canal encriptado		X
b) Test de manejo de credenciales y políticas de seguridad de usuarios	X	
c) Test de debilidades de mecanismos de cierre	X	
d) Test para sobrepasar el esquema de autenticación		X
e) Test de funcionalidad de recordar contraseñas		X
f) Test de funcionalidades de reseteo de contraseñas		X

Checklist: Fase V Test de Manejo de Sesiones
Identificación de la Auditoria
Institución Auditada: Gobierno Autónomo Descentralizado Municipal de Tisaleo
Proyecto: Análisis de vulnerabilidades y diseño de procesos correctivos del sitio web del Gobierno Autónomo Descentralizado Municipal de Tisaleo **Tipo de Auditoria:** o Interna o Externa
Auditor
Nombre: Pamela Jazmín Parra Zamora

Correo Electrónico: pamela.j.parra.z@pucesa.edu.ec / pamelaparra19@yahoo.com		
Teléfono: 0987896039 / 0984639237		
Checklist		
¿Existe vulnerabilidad?	**Si**	**No**
a) Test para sobrepasar el esquema de manejo de sesiones y atributos de cookies	X	
b) Test de arreglo de sesiones		X
c) Test de funcionalidad de cerrar sesión		X
d) Test de tiempo de espera de sesión	X	

Checklist: Fase VI y VIII Test de Validación de Entradas del Lado del Cliente
Identificación de la Auditoria
Institución Auditada: Gobierno Autónomo Descentralizado Municipal de Tisaleo
Proyecto: Análisis de vulnerabilidades y diseño de procesos correctivos del sitio web del Gobierno Autónomo Descentralizado Municipal de Tisaleo **Tipo de Auditoria:** ○ Interna ○ Externa
Auditor
Nombre: Pamela Jazmín Parra Zamora
Correo Electrónico: pamela.j.parra.z@pucesa.edu.ec / pamelaparra19@yahoo.com
Teléfono: 0987896039 / 0984639237

Checklist		
¿Existe vulnerabilidad?	**Si**	**No**
a) Test de Cross-Site Scripting		X
b) Test de Inyección SQL		X
c) Sobrecarga de Buffer (DOS)	X	

Checklist: Fase VII Test de Errores		
Identificación de la Auditoria		
Institución Auditada: Gobierno Autónomo Descentralizado Municipal de Tisaleo		
Proyecto: Análisis de vulnerabilidades y diseño de procesos correctivos del sitio web del Gobierno Autónomo Descentralizado Municipal de Tisaleo **Tipo de Auditoria:** o Interna o Externa		
Auditor		
Nombre: Pamela Jazmín Parra Zamora		
Correo Electrónico: pamela.j.parra.z@pucesa.edu.ec / pamelaparra19@yahoo.com		
Teléfono: 0987896039 / 0984639237		
Checklist		
¿Existe vulnerabilidad?	**Si**	**No**
a) Existencia de un manejo propio de errores	X	

Anexo 3: Certificado de culminación del proyecto de investigación

Tisaleo
...tierra de tesoros escondidos!

CERTIFICACIÓN

Yo, Hugo Leonidas Freire Analista Programador del Gobierno Autónomo Descentralizado Municipal de Tisaleo, certifico que la Srta. Parra Zamora Pamela Jazmín, con cedula de ciudadanía N°1804041885 realizó el trabajo de investigación: Estrategias para Protección de la Integridad de la Información Digital del Gobierno Autónomo Descentralizado Municipal de Tisaleo, de conformidad a los intereses de esta institución gubernamental.

Por la atención que se sirva dar al presente, me suscribo de usted.

Atentamente,

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE TISALEO
TECNOLÓGICO
TISALEO - TUNGURAHUA

Ing. Hugo Leonidas Freire
ANALISTA PROGRAMADOR