UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

TEMA:

DISEÑO DE UN MODELO DE ANÁLISIS FORENSE INFORMÁTICO EN EL HONORABLE GOBIERNO PROVINCIAL DE TUNGURAHUA.

Proyecto de Trabajo de Graduación. Modalidad: Proyecto de Investigación, presentado previo la obtención del título de Ingeniero en Sistemas Computacionales e Informáticos

SUB LÍNEA DE INVESTIGACIÓN:

Seguridad Computacional

AUTORA: Alexandra Elizabeth Pineda Vaca
PROFESOR REVISOR: Ing. Franklin Oswaldo Mayorga Mayorga

Ambato - Ecuador
Julio, 2016

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del Trabajo de Investigación sobre el Tema:

"DISEÑO DE UN MODELO DE ANÁLISIS FORENSE INFORMÁTICO EN EL HONORABLE GOBIERNO PROVINCIAL DE TUNGURAHUA", de la señorita Alexandra Elizabeth Pineda Vaca, estudiante de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, considero que el informe investigativo reúne los requisitos suficientes para que continúe con los trámites y consiguiente aprobación de conformidad con el numeral 7.2 de los Lineamientos Generales para la aplicación de Instructivos de las Modalidades de Titulación de las Facultades de la Universidad Técnica de Ambato.

Ambato, julio de 2016

Ing. Franklin Oswaldo Mayorga Mayorga

AUTORÍA

El presente trabajo de investigación titulado: DISEÑO DE UN MODELO DE ANÁLISIS FORENSE INFORMÁTICO EN EL HONORABLE GOBIERNO PROVINCIAL DE TUNGURAHUA. Es absolutamente original, auténtico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, julio de 2016

Alexandra Elizabeth Pineda Vaca

CC: 1804288726

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga uso de este Trabajo de Titulación como un documento disponible para la lectura, consulta y procesos de investigación.

Cedo los derechos de mi Trabajo de Titulación, con fines de difusión pública, además autorizo su reproducción dentro de las regulaciones de la Universidad.

Ambato, julio de 2016

Alexandra Elizabeth Pineda Vaca

CC: 1804288726

APROBACIÓN COMISIÓN CALIFICADORES

La Comisión Calificadora del presente trabajo conformada por los señores docentes Ing. David Guevara e Ing. Hernando Buenaño, revisó y aprobó el Informe Final del trabajo de graduación titulado DISEÑO DE UN MODELO DE ANÁLISIS FORENSE INFORMÁTICO EN EL HONORABLE GOBIERNO PROVINCIAL DE TUNGURAHUA, presentado por la señorita Alexandra Elizabeth Pineda Vaca de acuerdo al numeral 9.1 de los Lineamientos Generales para la aplicación de Instructivos de las Modalidades de Titulación de las Facultades de la Universidad Técnica de Ambato.

Ing. José Vicente Morales Lozada, Mg

PRESIDENTE DEL TRIBUNAL

Ing. David Omar Guevara Aulestia, Mg
DOCENTE CALIFICADOR

Ing. Edwin Hernando Buenaño Valencia, Mg
DOCENTE CALIFICADOR

DEDICATORIA

Dedicado con mucho amor a mis padres Mariana y Peregrino que con su infinito amor, sus enseñanzas y la confianza me han impulsado a luchar por mis sueños y no descansar hasta verlos hecho realidad.
A mis hermanas Vanessa y Gissela que siempre han estado a mi lado pesar de las diferencias.
A mi esposo Roberto por confiar en mi y apoyarme en las decisiones tomadas a lo largo de nuestra vida juntos.
Especialmente está dedicado a mis abuelitos Luis y Mercedes que han sido un ejemplo de lucha constante y me han enseñado a nunca darse por vencido, que a pesar de que digan que no hay un mañana, nunca perder la fé y seguir adelante porque ese mañana si vendrá.

Alexandra Pineda

AGRADECIMIENTO

A Dios por darme sabiduría, paciencia y fuerza para salir adelante a pesar de las dificultades para poder concluir con exito mi tesis.

Agradezco a los docentes de la Facultad, que a más de impartir sus conocimientos relacionados a la carrera, comparten sus experiencias y nos guian tanto en el ambito profesional como en lo personal. Guiandonos a ser profesionales más humanos.

A mi tutor el Ing. Franklin Mayorga por su guia y colaboración durante la elaboración de la tesis.

Al personal del área de Sistemas del Honorable Gobierno Provincial de Tungurahua por abrirme las puertas de la institución y brindarme la ayuda necesaria para la realización de este proyecto.

Alexandra Pineda

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

Resumen Ejecutivo

Este proyecto esta orientado al análisis forense informático en el Honorable Gobierno Provincial de Ambato mediante el diseño de un modelo de análisis forense basado en el estudio de los modelos más utilizados en la actualidad. El modelo diseñado consta de tres fases: Análisis Forense Proactivo, Activo y Reactivo, cada uno de estos tienen subfases.

El análisis Forense Proactivo es el más importante del diseño creado, para lo cual se verificó la documentación de la institución, creando políticas y procedimientos de seguridad que hacían falta en la institución. Utilizando la metodología OSSTMM se realizó un análisis de la seguridad de la institución con la finalidad de corregir vulnerabilidades, mejorando la seguridad de la misma.

El análisis Forense Activo se basa en determinar si existe una intrusión o no, y si es afirmativo recolectar la mayor cantidad de evidencia en tiempo real y contener la intrusión para minimizar los equipos o sistemas infectados. Para la aplicación de éste análisis se explotó algunas vulnerabilidades encontradas durante el análisis forense Proactivo y se siguió los procedimientos definidos para la identificación del incidente. Éste análisis se realiza sin la necesidad de apagar los equipos o sistemas por lo que es beneficioso en el caso de los servidores, pues dependiendo del tipo de ataque puede no ser necesario que dejen de funcionar.

Mientras que el análisis Forense Reactivo se lo realizaría en casos extremos, es decir si la intrusión a dañado equipos o borrado información de los mismos. Para este tipo de análisis se cuenta con una serie de herramientas especialmente diseñadas con estos propósitos, de las cuales se realizó un cuadro con sus principales características, tomando en cuenta que al ser aplicado en una institución pública, se debe utilizar software libre. Es necesario tener mucha precaución en varios aspectos, como en la cadena de custodia con el fin de asegurar que la evidencia no ha sido comprometida. De la misma manera al sacar respaldos por ejemplo de los discos duros, se deben asegurar que sean copias exactas de los originales para de esta manera al momento del análisis de la evidencia obtener resultados reales.

Para la documentación de los incidentes de seguridad se crearon formularios de incidentes.

Abstract

This project is oriented to forensic analysis in the Honorable Provincial Government of Ambato by designing a model of forensic analysis based on the study of the models used today. The model designed consists of three phases: Proactive and Reactive Active Forensics, each of these has sub-phases.

Proactive Forensic analysis is the most important design created, for which documentation was verified institution, creating security policies and procedures that were needed in the institution. Using the methodology OSSTMM an analysis of the security of the institution in order to correct vulnerabilities was conducted, improving the safety of it.

Active Forensic analysis is based on determining whether an intrusion or not, and if so collect as much evidence in real time and to minimize the intrusion contain equipment or infected systems. For the application of this analysis some vulnerabilities found during the Proactive forensic analysis and followed procedures defined for the identification of the incident. This analysis is done without the need to shut down the equipment or systems which is beneficial in the case of servers, because depending on the type of attack can not be required to stop working.

While Reagent Forensic analysis would take place in extreme cases, if the intrusion equipment damaged or deleted information from them. For this type of analysis it has a number of specially designed for these purposes, of which a table with its main characteristics was made, taking into account that when applied in a public institution, use free software tools. It is necessary to be very cautious in several aspects, such as the chain of custody in order to ensure that the evidence has not been committed. In the same way to get backups for example hard drives, they must ensure that they are exact copies of the originals in this way at the time of analyzing evidence to obtain real results.

For documenting security incidents were created incident forms.

Introducción

El objetivo del presente proyecto es diseñar un modelo de análisis forense y aplicarlo en el Honorable Gobierno Provincial de Tungurahua, fortaleciendo de esta manera la seguridad tecnológica de la institución y preparándola, para que en caso de incidentes informáticos se tenga parámetros bajo los cuales actuar. Minimizando asi las posibles intrusiones y en caso de que éstas ocurran se pueda controlar a tiempo disminuyendo el impacto que pueda causar en la institución. Este modelo es diseñado de acuerdo a las necesidades y procedimientos de la institución, teniendo en cuenta principalmente que es una entidad pública. Para lograr los objetivos del proyecto de investigación se ha dividido en los siguientes capitulos:

Capítulo 1, "El Problema".- Se describe el problema, la contextualización desde una óptica global hasta los problemas que poseen instituciones de la ciudad y la necesidad de ser corregidos, se plantea la justificación y los objetivos que se alcanzarán con la presente investigación.

Capítulo 2, "Marco Teórico".- Se presenta los antecedentes investigativos sobre los cuales se desarrolla la propuesta, se presenta la fundamentación teórica, guía en la búsqueda de una solución al problema planteado.

Capítulo 3, "Metodología".- Se describe la modalidad de la investigación a utilizar, como se realiza la recolección y procesamiento de la información para su análisis y, las actividades a seguir para el desarrollo de los objetivos del proyecto.

Capítulo 4, "Desarrollo de la Propuesta".- Se describe el desarrollo del proyecto mediante las actividades realizadas para el cumplimiento de cada uno de los objetivos específicos.

Capítulo 5, "Conclusiones y Recomendaciones".- Se describe las conclusiones y recomendaciones finales en base a los resultados obtenidos del desarrollo del proyecto de investigación.

CAPÍTULO 1

El problema

1.1. Tema

Diseño de un modelo de análisis forense informático en el Honorable Gobierno Provincial de Tungurahua

1.2. Planteamiento del problema

La informática en el mundo actual es indispensable y sus aplicaciones están prácticamente en todas las actividades que realiza el ser humano, permitiendo la agilidad de procesos que manualmente llevaría mucho más tiempo e incluso que realizarlos sería imposible si no fuera por la ayuda de la tecnología, esto ha hecho que la manera de trabajar, comunicarse, realizar trámites, e inclusive la forma en que operan los delincuentes haya cambiado.

Los gobiernos de varios países han estado aprovechando al máximo las posibilidades que ofrecen las tecnologías de la información y las comunicaciones, para ofrecer a la ciudadanía los servicios de manera eficaz y eficiente, superando las enormes barreras de infraestructura, recursos y capacidad de uso que persisten en países en vías de desarrollo como el nuestro. Al ofrecer estos servicios están más vulnerables a los delitos informáticos.

Diariamente son generados miles de datos y almacenados en dispositivos físicos o virtuales, haciendo de estos elementos tecnológicos los escenarios perfectos para personas que lucran de la información obtenida ilegalmente. Dado que la información es un activo muy importante y que merece extrema precaución, pues la pérdida o divulgación de esta información puede causar pérdidas económicas, de imagen y pueden afectar a la productividad de las empresas o personas[1].

Ambato es una ciudad en crecimiento empresarial, por esta razón los ciberdelincuentes también ponen más atención a las instituciones y empresas de la zona, atacando principalmente a las páginas web, un ejemplo de ello es el reciente ataque a

la página web de Diario la Hora, lo que ocasiona que no puedan visualizar su contenido a nivel externo e internamente ocasiona la caída de los servidores, provocando que no se pueda administrar el sitio[2].

Toda institución es vulnerable a los ataques informáticos y más aún las entidades públicas que poseen información de todos los ciudadanos y este es el principal objetivo de los ciberdelincuentes, además de hacer daño a la reputación de las entidades.

El Municipio de Guayaquil, El Honorable Gobierno Provincial de Tungurahua, el GAD Municipalidad de Ambato, etc. han sido víctimas de ataques a sus páginas web en varias ocasiones, y los atacantes únicamente han sido identificados porque en la gráfica que muestran está sus alias, pero en realidad no se toman medidas para identificar a los verdaderos autores de tales ataques.

El Honorable Gobierno Provincial de Tungurahua ha sido atacado por ciberdelincuentes en varias ocasiones, al no contar con un modelo de análisis forense informático las acciones tomadas para corregir el problema de seguridad solo han resuelto el problema momentáneamente, sin haber identificado a los atacantes, sin saber que información sustrajeron durante el ataque y lógicamente sin asegurar la evidencia digital para utilizarla en caso de un proceso jurídico.

La ciberdelincuencia es un tipo de delito que afecta a la sociedad debido a los avances tecnológicos y la poca seguridad informática que tienen las organizaciones. La delincuencia informática mundial causa un perjuicio de 114 mil millones de dólares anuales, según estudios se determinó que más de dos tercios de los adultos en línea (69 %) han sido víctimas de la ciberdelincuencia alguna vez en la vida[3].

Estándares internacionales como la norma ISO/IEC 27037 - 2012, hace referencia a Tecnología de la información, técnicas de seguridad, guías para la identificación, recolección, adquisición y preservación de la evidencia digital. Mientras que en Ecuador la ley que regula los delitos informáticos es la Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas publicada en la Ley N°. 67. Registro Oficial[4].

1.2.1. Delimitación

Área Académica: Hardware y Redes.

Línea de Investigación: Tecnologías de la Información.

Sub Línea de Investigación: Seguridad Computacional.

Delimitación Espacial: La presente investigación se desarrollará en el Honorable Gobierno Provincial de Tungurahua.

Delimitación Temporal: La presente investigación se desarrollará en 6 meses posteriores a la aprobación del proyecto por parte del H. Consejo Directivo de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

1.3. Justificación

Los avances tecnológicos han revolucionado el mundo, las empresas y organizaciones deben estar al día con las mismas. Esto ha hecho que los delincuentes también evolucionen en la forma de operar, lo más importante de una organización es su información y es a esto a lo que apuntan los ciberdelincuentes, es por ello que toda organización debe disponer de medidas preventivas, defensivas y correctivas en caso de ser atacado. Por lo cual es indispensable para las instituciones tener un modelo de análisis forense informático adecuado y herramientas jurídicas para el proceso de investigación y posterior condena de un delito informático.

El modelo de análisis forense debe estar listo a aplicarse de acuerdo a los requerimientos de la institución. De tal forma que si hay una ataque tengan la guía adecuada de los procedimientos a seguir para detectar al atacante y actuar de acuerdo a las leyes, que en el país están reguladas por la Ley de comercio Electrónico, firmas electrónicas y mensajes de datos (Ley N° 2002-67). Sin embargo hay que tener claro que los ciberdelincuentes pueden atacar desde cualquier parte del mundo, solo basta que el dispositivo tenga acceso a internet. Por este motivo no basta con tener conocimiento de las leyes del país, sino que es necesario conocer los convenios que existen entre varios países o regiones de cooperación para la resolución de este tipo de delitos.

La aplicación adecuada del modelo en el Honorable Gobierno Provincial de Tungurahua va a contribuir en la calidad del material extraído y de manera directa en la aceptación del mismo durante un peritaje informático, pues aportará diferentes guías para la recolección de evidencia digital.

Con el desarrollo del presente proyecto se beneficiarán principalmente los funcionarios del Honorable Gobierno Provincial de Tungurahua a través de la aplicación del modelo de análisis forense informático, luego de analizar los problemas causados por un delito informático y la forma de actuar ante esta situación, se ha observado la necesidad de elaborar un modelo de análisis forense se indica que el proyecto es totalmente factible de realizar y aplicar.

1.4. Objetivos

1.4.1. General

Diseñar un modelo de análisis forense informático para aplicarlo en el Honorable Gobierno Provincial de Tungurahua.

1.4.2. Específicos

- Revisar los niveles de ataques en el Honorable Gobierno Provincial de Tungurahua.
- Estudiar los modelos de análisis forense más aceptados en la actualidad.
- Analizar los parámetros bajo los cuales se debe crear el modelo de análisis forense informático.
- Crear procesos que permitan la preparación forense informática de la institución.
- Desarrollar procedimientos de análisis de evidencia digital siguiendo estándares y técnicas establecidas en la institución y que estén contemplados en el marco legal.
- Diseñar el modelo de análisis forense informático para el Honorable Gobierno Provincial de Tungurahua.
- Aplicar el modelo de análisis forense informático diseñado para el Honorable Gobierno Provincial de Tungurahua.

CAPÍTULO 2

Marco Teórico

2.1. Antecedentes Investigativos

Para investigar toda la compleja actividad que tiene lugar en el uso de las nuevas tecnologías de la información ha surgido la informática forense. Realizando una investigación por los principales repositorios de las universidades y portales web en la región latinoamericana que ofertan la Carrera de Ingeniería en Sistemas y tratan sobre la tecnología actual se encontró algunos documentos que pueden ser de utilidad en ésta investigación.

En la Escuela Superior Politécnica de Chimborazo, Juntamay Tenezaca Ana Lucía y Macas Carrasco Nancy Patricia, en el 2011 en su proyecto "Estudio y Aplicación de procedimientos de análisis forense en servidores de bases de datos SQL SERVER y MYSQL, caso práctico DESITEL-ESPOCH" obtiene como idea principal el aplicar la informática forense, como medio que ayude a esclarecer hechos delictivos informáticos, basándose en una guía de procedimientos de análisis forense, la misma que está conformada por seis fases que se complementan entre si para realizar un correcto análisis forense, esto está basado en estándares y procedimientos aceptados en procesos legales[4].

En la Universitat Oberta de Catalunya, Rifá Pous Helena, Serra Ruiz Jordi y Rivas López José Luis, en el 2009 en su proyecto "Análisis forense de sistemas informáticos", estudian el análisis forense en el área de informática, los incidentes de seguridad que han ocurrido en España, principales conceptos y algunas leyes dentro de este tema, así como la explicación de cómo afrontar la adquisición de los datos, análisis e investigación, la base jurídica de la infracción y como obtener pruebas incriminatorias sin violar los derechos de los usuarios e infractores. Exponen las diferentes formas de contactar con la policía judicial y el modo de actuar una vez que reciben la denuncia, explican la forma correcta de realizar el informe del incidente y por ultimo un ejemplo de análisis forense [1].

En la Escuela Politécnica Nacional, Almeida Avilés Andrés Sebastián, en el 2014 en su proyecto "Modelo de Análisis Forense para una entidad bancaria", propone un modelo de análisis forense digital para una entidad bancaria, basado en una estrategia de seguridad de defensa en profundidad, además de fundamento teórico utilizado en la investigación. El modelo que proponen está basado en el propuesto por Grobler el cual menciona que el análisis forense digital consta de tres componentes, el pro activo, el reactivo y el activo. El modelo que proponen está orientado a entidades bancarias con el fin de complementar la estrategia de seguridad que poseen [5].

En la Fundación Universitaria Juan de Castellanos, Avella Pinzón Rocío del Pilar, Gil Gamboa Manuel Salvador y Bohada John A., en el 2013 en su investigación "Realidades de un delito informático en Boyaca", concluyen que la informática forense es un campo con mucha oportunidad de formación profesional y de negocio, enfocándose en la seguridad, investigación forense, expertos en manejo y recuperación de la información. Tomando en cuenta que falta mucho conocimiento en el área de informática forense por parte de los profesionales en Derecho. En esta investigación identifican los estándares RFC 3227 y la norma ISO/IEC 27037:2012, reconocidos y aceptados internacionalmente, los cuales orientan a lo que se debe hacer ante un incidente de seguridad [6].

2.2. Fundamentación teórica

Informática forense

La informática forense como aplicación de las ciencias de la computación a la investigación criminal, ofrece la posibilidad de, metodológicamente identificar, recuperar, preservar, reconstruir, validar, analizar, interpretar, documentar y presentar evidencia digital como parte de la investigación de un incidente informático[7].

Análisis forense

El análisis forense en un sistema informático es una ciencia moderna que permite reconstruir lo que ha sucedido en un sistema tras un incidente de seguridad. Este análisis puede determinar quién, desde dónde, cómo, cuándo y qué acciones ha llevado a cabo un intruso en los sistemas afectados por un incidente de seguridad [1].

Incidentes de seguridad

Un incidente de seguridad es cualquier acción fuera de la ley o no autorizada: ataques de denegación de servicio, extorsión, posesión de pornografía infantil, envío de correos electrónicos ofensivos, fuga de información confidencial dentro de la organización [1].

Siniestro Informático

Según Miguel Antonio Cano "El siniestro informático implica actividades criminales como robos, hurtos, falsificaciones, estafa, sabotaje, etc. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de computadoras lo que a propiciado ha su vez la necesidad de regulación por parte del derecho [8].

Evidencia Digital

La evidencia digital está definido como cualquier dato almacenado o transmitido por medios digitales que sustentan o refutan una hipótesis de como ocurrió un incidente. Es muy importante, ya que un mal manejo de la misma puede ocasionar su pérdida o destrucción [9].

Piratas informáticos o hackers

El acceso se efectúa a menudo desde un lugar exterior, recurriendo a uno de los diversos medios como son: Aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. Los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema [8].

Categorías para hacer una necesaria distinción entre el elemento material de un sistema informático o hardware (evidencia electrónica) y la información contenida en este (evidencia digital). Esta distinción es necesaria al momento de realizar los procedimientos adecuados para cada tipo de evidencia y crear un paralelo entre una escena física del crimen y una digital. El hardware se refiere a todos los componentes físicos de un sistema informático, mientras que la información, se refiere a todos los datos, mensajes de datos y programas almacenados y trasmitidos usando el sistema informático[10].

El hardware:

- Puede ser una mercancía ilegal cuando su posesión no está autorizada por la ley. Ejemplo: Decodificadores de la señal de televisión por cable, su posesión es una violación a los derechos de propiedad intelectual y también un delito.
- Como fruto del delito cuando este es obtenido mediante robo, hurto, fraude u otra clase de infracción.
- Instrumento cuando el hardware cumple un papel importante al cometer un delito, se puede decir que es usada como un arma o herramienta, tal como

una pistola o un cuchillo. Ejemplo los snifers y otros aparatos especialmente diseñados para capturar el tráfico en la red o interceptar comunicaciones.

- Como evidencia es un elemento físico que se constituye como prueba de la comisión de un delito. Por ejemplo el scanner que se usó para digitalizar una imagen de pornografía infantil, cuyas características únicas son usadas como elementos de convicción.

La información:

- Es considerada como mercancía ilegal cuando su posesión no está permitida por la ley, por ejemplo en el caso de la pornografía infantil.
- Será fruto del delito cuando sea el resultado de la comisión de una infracción, como por ejemplo las copias pirateadas de programas de ordenador, secretos industriales robados.
- Es un instrumento o herramienta cuando es usada como medio para cometer una infracción penal. Son por ejemplo los programas de ordenador que se utilizan para romper las seguridades de un sistema informático, sirven para romper contraseñas o para brindar acceso no autorizado. En definitiva juegan un importante papel en el cometimiento del delito.
- Es evidencia: ésta es la categoría más grande y nutrida de las anteriores, muchas de nuestras acciones diarias dejan un rastro digital. Uno puede conseguir mucha información como evidencia, por ejemplo la información de los ISP's, de los bancos, y de las proveedoras de servicios las cuales pueden revelar actividades particulares de los sospechosos.

LEY EN VIGENCIA EN TORNO A DELITOS INFORMÁTICOS. La ley en vigencia para delitos informáticos con las que el Ecuador cuenta están dentro de la Ley de Comercio Electrónico, firmas electrónicas y mensajes de datos (Ley No. 2002-67), entre los artículos se tiene:

Art. 1.- Objeto de la Ley.- Esta Ley regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas.

Reformas al Código Penal Art. 58.- A continuación del Art. 202, inclúyanse los siguientes artículos innumerados:

Art.58. .- El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida,

contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica. Si la información obtenida se refiere a seguridad nacional, o a secretos comerciales o industriales, la pena será de uno a tres años de prisión y multa de mil a mil quinientos dólares de los Estados Unidos de Norteamérica. La divulgación o la utilización fraudulenta de la información protegida, así como de los secretos comerciales o industriales, será sancionada con pena de reclusión menor ordinaria de tres a seis años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica. Si la divulgación o la utilización fraudulenta se realiza por parte de la persona o personas encargadas de la custodia o utilización legítima de la información, éstas serán sancionadas con pena de reclusión menor de seis a nueve años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica[11].

Normas ISO/IEC 27037 La norma ISO/IEC 27037 se publicó en el 2012, bajo el nombre de "Information technology — Security techniques — Guidelines for identification, collection, adquisition and preservation of digital evidence". ISO 27037 Es una directriz que proporciona pautas en actividades específicas como identificación, recopilación, consolidación y preservación de potencial evidencia digital que pueda tener un valor probatorio [12].

RFC 3227 Guía Para Recolectar y Archivar Evidencia" (Guidelines for Evidence Collection and Archiving). Escrito en febrero de 2002 por Dominique Brezinski y Tom Killalea, ingenieros del Network Working Group. Es un documento que provee una guía de alto nivel para recolectar y archivar datos relacionados con intrusiones. Muestra las mejores prácticas para determinar la volatilidad de los datos, decidir que recolectar, desarrollar la recolección y determinar cómo almacenar y documentar los datos. También explica algunos conceptos relacionados a la parte legal [13]

Su estructura es:

a) Principios durante la recolección de evidencia: orden de volatilidad de los datos, cosas para evitar, consideraciones de privacidad y legales.

b) El proceso de recolección: transparencia y pasos de recolección.

c) El proceso de archivo: la cadena de custodia y donde y como archivar

2.3. Propuesta de Solución

Diseñar un modelo de análisis forense acorde a las necesidades y exigencias del Honorable Gobierno Provincial de Tungurahua, con los procedimientos adecuados

para no comprometer la evidencia digital y actuar de acuerdo a la ley en casos de ataques informáticos. Detallando todo el fundamento teórico posible, es decir conceptos detallados y estado del arte de: análisis forense digital, investigación forense digital, además las regulaciones y normativas vigentes para estas instituciones, relacionadas con la seguridad de la información y análisis forense digital.

CAPÍTULO 3

Metodología

3.1. Modalidad de la investigación

El presente trabajo tiene las siguientes modalidades:

Modalidad Bibliográfica o Documental Se considera esta modalidad ya que se utilizará diferentes fuentes como libros, artículos, tesis desarrolladas en Universidades para profundizar enfoques con respecto al tema de la investigación.

Además será necesario recolectar información de las leyes que rigen en el país con respecto al tema investigado y las normativas internacionales relacionadas al tema.

Modalidad aplicada Por la utilización de los conocimientos adquiridos a lo largo de la carrera universitaria en módulos como Seguridad Informática, Gerencia Informática.

Modalidad de Campo Se considera esta modalidad ya que el investigador acudirá al Honorable Gobierno Provincial de Tungurahua para obtener la información necesaria y así lograr alcanzar los objetivos planteados.

3.2. Recolección de información

Se recolectará la información utilizando entrevistas al personal de la institución, así también se buscará en Internet información virtual utilizando documentos técnicos, tesis, libros, todo esto para alcanzar los objetivos planteados.

Pata la recolección de información dentro de la institución se realizó una entrevista al Director del departamento de sistemas del Honorable Gobierno Provincial de Tungurahua, Ing. Ricardo Domínguez y el Ing. Darío Morales que son parte del área mencionada.

3.3. Procesamiento de la información

Para el procesamiento de la información se realizará las siguientes actividades:

- Recolección de requisitos mediante entrevistas.
- Revisión y análisis de la información recogida.
- Lectura de artículos relacionados con la investigación presentada.

3.4. Desarrollo del proyecto

1. Revisar los niveles de ataques en el Honorable Gobierno Provincial de Tungurahua.

   1.1. Análisis de la situación actual de los delitos informáticos

   1.2. Diseño del instrumento de entrevistas.

   1.3. Realización de entrevistas a los funcionarios del área de Sistemas que laboren en la institución identificando los requerimientos de la misma, los niveles de ataques en la institución y análisis de los resultados de las entrevistas.

2. Estudiar los modelos de análisis forense más aceptados en la actualidad.

   2.1. Investigación de los modelos de análisis forense informático más aceptados en la actualidad.

3. Analizar los parámetros bajo los cuales se debe crear el modelo de análisis forense informático.

   3.1. Establecimiento de los parámetros para el desarrollo de los posibles procedimientos del modelo de acuerdo a los resultados de las entrevistas.

4. Crear procesos que permitan la preparación forense informática de la institución.

   4.1Elaboración de los pasos del modelo de análisis forense acorde a los parámetros establecidos.

5. Desarrollar procedimientos de análisis de evidencia digital siguiendo estándares y técnicas establecidas en la institución y que estén contemplados en el marco legal.

   5.1. Análisis de la ley vigente sobre delitos informáticos.

   5.2. Crear procedimientos de análisis de evidencia digital.

6. Diseñar el modelo de análisis forense informático para el Honorable Gobierno Provincial de Tungurahua.

   6.1. Diseño del modelo a aplicarse en el Honorable Gobierno Provincial de Tungurahua.

7. Aplicar el modelo en el Honorable Gobierno Provincial de Tungurahua

   7.1. Aplicación del modelo en el Honorable Gobierno Provincial de Tungurahua.

   7.2. Realización de reportes que muestre los resultados.

   7.3. Revisión de las actividades documentadas.

CAPÍTULO 4

Desarrollo de la Propuesta

4.1. Datos informativos

Título

Diseño de un modelo de análisis forense informático en el Honorable Gobierno Provincial de Tungurahua

Institucionales

- Honorable Gobierno Provincial de Tungurahua

Beneficiarios

Honorable Gobierno Provincial de Tungurahua

Ubicación

Provincia: Tungurahua
Cantón: Ambato
Dirección: Calles Simón Bolívar y Mariano Castillo esquina
Teléfonos: 033730220 ext 120

Equipo Responsable

Tutor: Ing. Franklin Oswaldo Mayorga
Investigador: Alexandra Elizabeth Pineda Vaca

4.2. Antecedentes de la propuesta

En la actualidad la tecnología es parte importante en el desarrollo y productividad de cualquier empresa o institución, pues ayudan en la eficiencia de la misma. Hacer uso de estos recursos tecnológicos permite mejor comunicación tanto dentro como fuera de la empresa. Al mismo tiempo que la tecnología es el mejor aliado de las instituciones o empresas, también pueden ser el mayor peligro si no se cuenta con las seguridad necesarias para proteger lo más importante que tiene una institución, que es la información. Es por ello que es necesario contar con una modelo de análisis

forense adaptada a las necesidades de cada institución, una que no solamente se active en caso de intrusión, sino también que ayude a estar preparados para evitarlas o minimizar el impacto.

4.3. Justificación

El Honorable Gobierno Provincial de Tungurahua ha sido víctima de múltiples ataques informáticos y aunque aparentemente no ha sido robada información de la institución, ha habido otros daños entre ellos la suplantación de la página web de la institución, lo que afecta su imagen y la confianza en la institución.

De acuerdo a lo investigado el Honorable Consejo Provincial de Tungurahua no cuenta con una metodología y plan de contingencias que ayude en caso de incidentes informáticos, ni un modelo que se asegure de evitar o minimizar al máximo las consecuencias, por lo que es más difícil cuando ocurre un incidente de seguridad informático.

La institución no cuenta con políticas de seguridad definidas en cuanto a seguridad tecnológica, las capacitaciones a los empleados en temas de seguridad de la información son muy escasas y en caso de haber alguna capacitación, es dirigida únicamente al personal del área de tecnologías.

La aplicación de un modelo de análisis forense informático en el Honorable Gobierno Provincial de Tungurahua, no solamente ayudará a minimizar riesgos, sino que en caso de ataques dará una guía de: que, cuando y como hacer los procedimientos que sean adecuados dependiendo de la situación.

4.4. Objetivos

4.4.1. Objetivo General

Aplicar un modelo de análisis forense informático en el Honorable Gobierno Provincial de Tungurahua.

4.4.2. Objetivos Específicos

- Revisar los niveles de ataques en el Honorable Gobierno Provincial de Tungurahua.
- Estudiar los modelos de análisis forense más aceptados en la actualidad.
- Analizar los parámetros bajo los cuales se debe crear el modelo de análisis forense informático.

- Crear procesos que permitan la preparación forense informática de la institución.
- Desarrollar procedimientos de análisis de evidencia digital siguiendo estándares y técnicas establecidas en la institución y que estén contemplados en el marco legal.
- Diseñar el modelo de análisis forense informático para el Honorable Gobierno Provincial de Tungurahua.
- Aplicar el modelo en el Honorable Gobierno Provincial de Tungurahua.

4.5. Análisis de factibilidad

4.5.1. Factibilidad operativa

El presente proyecto en la parte operativa cuenta con el aval del Honorable Gobierno Provincial de Tungurahua para hacer uso de la infraestructura física y equipos existentes, además se dispone de los recursos humanos y tecnológicos para la investigación. Cabe añadir que las autoridades del Honorable Gobierno Provincial de Tungurahua muestran interés hacia la presente investigación.

4.5.2. Factibilidad económica

El costo de la investigación estará a cargo del investigador, además que la institución cuenta con todo lo necesario para la aplicación del modelo de análisis forense.

4.5.3. Factibilidad Técnica

Factibilidad en Software

El software que se requiere es de distribución libre por lo que no hace falta pagar licencias, en el caso de Windows la herramienta a utilizarse será la versión de prueba. El software a utilizarse es:

- Kali linux
  - Tor
  - Maltego
  - Zenmap
  - OpenVas

- Whatweb
- Sqlmap
- Metasploit
- Vega

- Windows
  - Nessus

Factibilidad en Hardware

Para el presente proyecto se hará uso del hardware que posee la institución.

4.6. Fundamentación

4.6.1. Fundamentación Teórica

Análisis Forense

El Análisis Forense Informático, también llamado informática forense, computación forense, análisis forense digital, cómputo forense o examen forense digital es la aplicación de técnicas científicas y analíticas especializadas a la infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal y se aplica tanto para la investigación de delitos "tradicionales", (homicidios, fraude financiero, narcotráfico, terrorismo, etc.), como para los propiamente relacionados con las tecnologías de la información y las comunicaciones entre los que podemos mencionar a la piratería de software y comunicaciones, distribución de pornografía infantil, intrusiones y hacking en organizaciones, etc.[13].

El análisis forense en un sistema informático es una ciencia moderna que permite reconstruir lo que ha sucedido en un sistema tras un incidente de seguridad. Este análisis puede determinar quién, desde dónde, cómo, cuándo y qué acciones ha llevado a cabo un intruso en los sistemas afectados por un incidente de seguridad [1].

Denegación de Servicio ("Denial of Service" DoS)

Se trata de un método que tiene como objetivo poner fuera de servicio todo o parte de un sistema informático.

A diferencia de un acto de piratería clásico, el autor del DoS no tiene acceso directo al ordenador, no puede leer o modificar documento confidenciales [14].

Hay dos tipos de denegación de servicios:

- Generar un mal funcionamiento de la aplicación utilizando un fallo del programa.
- Saturación del Servicio(flooding)

Firewall

Es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de red privada y el internet.

Un firewall es software o hardware que comprueba la información procedente de Internet o de una red y, a continuación, bloquea o permite el paso de ésta al equipo, en función de la configuración del firewall.

Como muestra la figura 4.1 el firewall funciona como filtro para controlar los datos que entran y salen de las redes. Dependiendo del servicio el firewall decide si lo permite o no, además examina si la comunicación es entrante o saliente y dependiendo de su dirección puede permitirla o no [15].

Figura 4.1: Firewall

Ingeniería Social

Son estrategias basadas en el engaño y están netamente orientadas a explotar las debilidades del factor humano. Consiste en obtener información confidencial de un usuario acerca la institución o el sistema, explotando características propias del ser humano [16].

Normativas y Estándares Algunos de los estándares y normativas internacionales más relevantes son:

- **ISO 27037**

ISO / IEC 27037: 2012 proporciona directrices para las actividades específicas en el tratamiento de la evidencia digital, que son la identificación, recolección, consolidación y preservación de evidencia digital potencial que puede ser de valor probatorio.

Esta Norma Internacional se asegura de que las personas responsables gestionar las pruebas digitales potencial en formas prácticas que son aceptables en todo el mundo, con el objetivo de facilitar la investigación que involucra a los dispositivos digitales y pruebas digitales de una manera sistemática e imparcial, preservando su integridad y autenticidad.

Esta norma internacional también tiene la intención de informar a los tomadores de decisiones que necesitan para determinar la fiabilidad de las pruebas digitales que se les presentan. Es aplicable a las organizaciones que tienen que proteger, analizar y presentar la evidencia digital potencial [17].

Esta norma ofrece orientación para tratar situaciones frecuentes durante todo el proceso de tratamiento de las pruebas digitales. Además define dos roles especialistas:

- DEFR (Digital Evidence First Responders): Expertos en primera intervención de evidencias electrónicas.
- DES (Digital Evidence Specialists): Experto en gestión de evidencias electrónicas.

ISO 27037 proporciona orientación para los siguientes dispositivos y circunstancias:

- Medios de almacenamiento digitales utilizados en equipos varios como por ejemplo discos duros, disquetes, discos magneto-ópticos y ópticos y otros similares.
- Teléfonos móviles, PDAs, tarjetas de memoria.
- Sistemas de navegación móvil (GPS).
- Cámaras de video y cámaras digitales (incluyendo circuitos cerrados de televisión).
- Ordenadores estándares con conexiones a redes.
- Redes basadas en protocolos TCP/IP y otros protocolos digitales.
- Otros dispositivos con funcionalidades similares a las descritas anteriormente

Lo más importante de esta norma es que ofrece orientación sobre el manejo de las pruebas digitales. Siguiendo las directrices de esta norma se asegura que la evidencia digital potencial se recoge de manera válida a efectos legales para facilitar su aportación en juicios y procesos legales. Además cabe destacar que cubre una amplia gama de tipos de dispositivos y situaciones, por lo que la orientación dentro de la norma es ampliamente aplicable.

- **RFC3227 ("Guidelines for Evidence Collection and Archiving")**

  Define aspectos como:

  - Orden para recabar información a partir de su orden de volatilidad.
  - Ofrece instrucciones de que no se debe hacer cuando se tiene que obtener la información de un sistema.
  - Expone normas éticas que deberían cumplirse.

  Documento publicado por la Internet Engineering Task Force (IETF). Los RFC «Request For Comments» son documentos que recogen propuestas de expertos en una materia concreta, con el fin de establecer por ejemplo una serie de pautas para llevar a cabo un proceso, la creación de estándares o la implantación de algún protocolo.

  El RFC 3227 es un documento que recoge las directrices para la recopilación de evidencias y su almacenamiento sin ponerlas en riesgo.

  En los principios para la recolección de evidencias destacan básicamente tres, el orden de volatilidad de los datos, las acciones que deben evitarse y las consideraciones sobre la privacidad.

  En cuanto al procedimiento de recolección destaca que debe ser detallado, procurando que no sea ambiguo y reduciendo al mínimo la toma de decisiones.

  Sobre el procedimiento de almacenamiento tiene en cuenta la cadena de custodia de las pruebas recogidas anteriormente y dónde y cómo se deben almacenar estas para que estén a buen recaudo.

  Detalla qué tipo de herramientas son las más útiles y qué características deben tener para evitar conflictos, haciendo hincapié en que las herramientas deben alterar lo menos posible el escenario. Según este documento el kit de análisis debe incluir las siguientes herramientas:

  - Programas para listar y examinar procesos.
  - Programas para examinar el estado del sistema.
  - Programas para realizar copias bit a bit.

La base de estas recomendaciones en el principio de intercambio de Locard [18].

- **UNE 71505 y UNE 71506**

  Normas publicadas por la Asociación Española de Normalización y Certificación, tienen como finalidad dar una metodología para la preservación, adquisición, documentación, análisis y presentación de pruebas digitales.

  Estas normas contribuyen a homogeneizar la gestión de las evidencias electrónicas y establecen un marco de referencia de buenas prácticas que contribuye a mejorar la admisibilidad de las pruebas electrónicas en procesos jurisdiccionales siempre que los peritos adopten sus postulados.

  Esta norma debe dar respuesta a las infracciones legales e incidentes informáticos en las distintas empresas y entidades. Con la obtención de dichas pruebas digitales, que serán más robustas y fiables siguiendo la normativa, se podrá discernir si su causa tiene como origen un carácter intencional o negligente.

  Estas normativas son de aplicación a cualquier organización con independencia de su actividad o tamaño, así como a cualquier profesional competente en este ámbito. Se dirige especialmente a incidentes y seguridad, así como al personal técnico que trabaje en laboratorios o entornos de análisis forense de evidencias electrónicas [18].

Defensa en Profundidad

La defensa en profundidad del sistema de información es una defensa global y dinámica, que coordina varias líneas de defensa que cubren toda la profundidad del sistema. Se trata de coordinar las acciones que contengan los atentados contra la seguridad, al menor costo, mediante la gestión de riesgos, un sistema de informes, la planificación de las reacciones y la mejora continua gracias a la experiencia adquirida [19].

La defensa en profundidad como estrategia de la seguridad de la información contempla: las actividades cotidianas, la tecnología y las personas como muestra en la figura 4.2[20].

Figura 4.2: Defensa en Profundidad

Evidencia digital

Es cualquier información, que sujeta a una intervención humana u otra semejante, ha sido extraída de un medio informático [4].

Se entiende por evidencia digital al conjunto de datos en formato binario, estos pueden ser ficheros, su contenido o referencias a estos (metadatos) que se encuentran en los soportes físicos o lógicos del sistema atacado [13].

Como fuentes de metadatos tenemos:

- El proceso de almacenamiento y borrado
- El acceso a Internet
- La ejecución de impresiones
- El sistema operativo de la computadora.

La diferencia entre la evidencia digital informática y la evidencia tradicional es:

- La volatilidad
- La capacidad de duplicación
- La facilidad de alterarla
- La cantidad de metadatos que posee
- Es anónima
- Es eliminable

Características que hacen el proceso de obtención de evidencia sea una labor más exigente poniendo en práctica procedimientos, técnicas y herramientas tecnológicas

para la obtención de las mismas. Teniendo presente siempre las normas y regulaciones legales asociadas con las pruebas y el derecho procesal [13].

Incidentes de seguridad

Un incidente de seguridad es cualquier acción fuera de la ley o no autorizada: ataques de denegación de servicio, extorsión, posesión de pornografía infantil, envío de correos electrónicos ofensivos, fuga de información confidencial dentro de la organización..., en el cual está involucrado algún sistema telemático de nuestra organización [1].

Principio de Locard

"Siempre que dos objetos entran en contacto transfieren parte del material que incorporan al otro objeto". Cada contacto deja un rastro. Conexión SSH: claves públicas en cliente y servidor. Exploits compilados: MD5 único de un "único" atacante [18].

Políticas de Seguridad

Es un conjunto de leyes, reglas y prácticas que regulan la manera de dirigir, proteger y distribuir recursos en una organización para llevar a cabo los objetivos de seguridad informática dentro de la misma.

Las políticas de seguridad definen lo que está permitido y lo que está prohibido, permiten definir los procedimientos y herramientas necesarias, expresan el consenso de los "dueños" y permiten adoptar una buena actitud dentro de la organización [21].

Kali Linux

Kali Linux es una distribución Linux basada en Debian dirigida a pruebas de penetración y de auditoría de seguridad. Contiene varias herramientas destinadas a diversas tareas de seguridad de la información, tales como pruebas de penetración, Forense y de ingeniería inversa [22].

Maltego

Es una herramienta de código abierto creado por Paterva para el análisis y la visualización de las conexiones de datos, utiliza un sistema de entidades sobre las cuales se pueden realizar transformaciones y así obtener mayor información de la misma (dispositivos, DNS, servidores de correo, ips, tecnologías aplicadas, documentos, números telefónicos, correos, etc), la cual es mostrada en forma gráfica mediante una estructura de tipo árbol[22].

Cadena de Custodia

Es el conjunto de pasos o procedimientos seguidos para preservar la evidencia digital, de modo que permita convertirla y usarla como prueba en un proceso judicial.

La cadena de custodia debe:

1. Reducir la cantidad de agentes implicados en el manejo o tratamiento de evidencias.

2. Mantener la identidad de las personas implicadas desde la obtención hasta la presentación de las evidencias.

3. Asegurar la inmutabilidad de las evidencias en los traspasos de éstas entre agentes.

4. Contar con registros de tiempos, firmados por los agentes, en los intercambios de evidencia entre estos. Cada uno de ellos se hará responsable de las evidencias en cada momento.

5. Asegurar la inmutabilidad de las evidencias cuando las evidencias estén almacenadas asegurando su protección.

La cadena de custodia de la evidencia muestra quien, donde y cuando fue obtenida la evidencia y quien tuvo acceso a la misma [23].

4.7. Revisar los niveles de ataques en el Honorable Gobierno Provincial de Tungurahua

4.7.1. Análisis de la situación actual de los delitos informáticos

La situación actual de los delitos informáticos se obtendrá al realizar las entrevistas al personal del área de sistemas del Honorable Gobierno Provincial de Tungurahua.

4.7.2. Diseño de la Entrevista

Personal a entrevistar:

- Ing. Francisco López
- Ing. Ricardo Domínguez
- Ing. Darío Morales

Preguntas

1. ¿Ha sufrido la institución ataques informáticos?

2. ¿Tipo de ataques de los que han sido víctimas?

3. ¿Cuáles son los puntos frecuentes de ataques?

4. ¿Cuáles son las pérdidas causadas por estos incidentes de seguridad?

5. ¿Qué medidas que se ha tomado frente a los ataques?

6. ¿Conoce las medidas adecuadas que se debe tomar frente a un ataque informático?

7. ¿Posee la institución lineamientos a fin de obtener un informe pericial sobre determinados equipos informáticos?

8. ¿Se aplica los procedimientos formales para la gestión de la tecnología dentro de la empresa?

9. ¿Cuál de los procedimientos formales para la gestión de la tecnología dentro de la institución se usa más?

    - Uso de correo electrónico
    - Uso del internet
    - Administración de recursos tecnológicos
    - Uso de red inalámbrica
    - Otros...

4.7.3. Realización de entrevistas a los funcionarios del área de Sistemas que laboren en la institución identificando los requerimientos de la misma, los niveles de ataques en la institución y análisis de los resultados de las entrevistas.

Entrevista realizada al Director del Departamento de Sistemas Ing. Francisco López, Ing. Ricardo Domínguez y el Ing. Darío Morales

1.- ¿Ha sufrido la institución ataques informáticos?

Respuestas:

- Si hemos sufrido ataques en el Honorable Gobierno Provincial de Tungurahua
- Si según yo conozco
- Desde agosto del año anterior si hemos tenido un par de ataques.

  Análisis de los resultados

  De las respuestas obtenidas al formular esta pregunta se puede determinar que la institución ha sufrido varios ataques informáticos.

2.- ¿Tipo de ataques de los que han sido víctimas?

Respuestas:

- Principalmente han sido dos. Uno dirigido a la página web y el segundo dirigido al correo electrónico
- Intrusión a los servidores, se desconoce los métodos utilizados para acceder pero si entraron y modificaron los servidores.
- Principalmente con los servicios de correo electrónico y caídas en el internet.

  Análisis de los resultados:

  La mayor parte de los ataques que ha sufrido la institución han sido dirigidos a los servicios de correo electrónico y a la página web de la institución.

3.- ¿Cuáles son los puntos frecuentes de ataques?

Respuestas:

- Como se decía en la respuesta anterior, los servidores web y los servidores de correo electrónico.
- Los servidores porque el firewall no daba la protección adecuada, spam por los correos electrónicos que activaban las famosas back doors.

- El firewall que se tenía anteriormente era muy deficiente por lo que fue cambiado.

  Análisis de los resultados:

  La mayoría de los ataques son dirigidos al firewall, presumiblemente con el objetivo de dañarlo y tener acceso a los servicios de la institución.

4.- ¿Cuáles son las pérdidas causadas por estos incidentes de seguridad?
Respuestas:

- No ha habido pérdidas de información, pero sí que los servicios no estuvieron disponibles por un tiempo, debido a que la información no esté disponible a los usuarios, por lo tanta la pérdida se podría hablar de tiempo.
- La página web de la institución se cayó y seguramente se perdió información.
- Se dañó un sistema documental que se llamaba lotus, se perdió toda la información que tenía almacenada ese servidor. Entendemos que no se pudo haber sacado información.

  Análisis de los resultados:

  La imagen de la institución ha resultado afectada por los ataques sufridos, pues en su mayoría han sido dirigidos a la página web que es la cara al público.

5.- ¿Qué medidas que se ha tomado frente a los ataques?
Respuestas:

- Lo primero que hicimos fue parchar y actualizar a las últimas versiones de los sistemas operativos, del sistema de correo electrónico y el sistema de página web. Se incrementó las seguridades, se cambió el firewall de la institución y se revisaron las políticas de seguridad con respecto a los usuarios.
- Se ha puesto un nuevo firewall tratando de solventar estas fallas.
- Adquirimos un nuevo firewall, se han aplicado políticas de seguridad a nivel de la red LAN y se han aumentado antivirus a las máquinas que no contaban con este, para que estén protegidas y no estén vulnerables a los ataques.

  Análisis de los resultados:

  La acción que ha tomado la institución para solucionar el problema ha sido el cambiar el firewall.

6.- ¿Conoce las medidas adecuadas que se debe tomar frente a un ataque informático?

Respuestas:

- Por supuesto,

  1. Se debe insolar el problema
  2. Se debe analizarlos y analizar las formas en que fuimos atacados
  3. Dar una solución
  4. Aplicar la solución y todos los parches o lo que se necesite
  5. Restablecer el servicio

- Si

- Creo que debe tenerse implementado un IPS, tener un servidor para que haga IPS.

  Análisis de los resultados:

  El personal del área de tecnología del Honorable Gobierno Provincial de Tungurahua dice conocer las medidas que se debe tomar frente a un ataque, aunque estas no están creadas formalmente.

7.- ¿Posee la institución lineamientos a fin de obtener un informe pericial sobre determinados equipos informáticos?

Respuestas:

- No, no tenemos. Pero si tenemos protocolos que se deben seguir en estos casos. Los protocolos son solo para arreglar el problema porque detectar el culpable es muy difícil.

- Si posee.

- No tenemos.

  Análisis de los resultados:

  La mayor parte de los entrevistados coinciden que no hay lineamientos en la institución para pedir un informe pericial de equipos informáticos, por lo cual en caso de ser necesario habría confusión de si hay o no lineamientos para la obtención de un informe pericial.

8.- ¿Se aplica los procedimientos formales para la gestión de la tecnología dentro de la empresa?

Respuestas:

- Si, tenemos procedimientos aprobados por prefectura, en donde tenemos lineamientos para nuestras actividades.
- Si, actualmente si.
- Si de hecho por ser una institución pública tenemos que hacerlo formalmente ante el señor prefecto y ante la institución como tal.

  Análisis de los resultados

  De acuerdo a los entrevistados en la institución si se aplican procedimientos formales para la gestión de la tecnología.

9.- ¿Cuál de los procedimientos formales para la gestión de la tecnología dentro de la institución se usa más?

- Uso de correo electrónico
  - Uso del internet
  - Administración de recursos tecnológicos
  - Uso de red inalámbrica
  - Otros...

  Respuestas:

  - Si

    1. Procesos de soporte al usuario
    2. Acceso a internet y acceso a los sistemas
    3. el uso de sistemas y recursos tecnológicos.
  - Si la parte que se está utilizando actualmente para adquirir la tecnología, catalogo electrónico que se adquiere con estándares, también basados en la ley la parte del software tratamos de que sea libre y que sea de mejor calidad. Se trata de actualizar toda la parte de los servidores, a las nuevas versiones, tener al día las seguridades.
  - Bajo solicitud. Cuando un usuario necesita el servicio de correo electrónico, de internet, cualquier servicio que tengamos nos tiene que solicitar mediante pedido directo al director o mediante un ticket de trabajo.

  Análisis de los resultados:

Al ser una institución pública está obligada a tener procedimientos formales para el uso de recursos tecnológicos, los mismos que son conocidos por todo el personal en especial por el personal del área de sistemas.

De la entrevista realizada al personal del área de sistemas del Honorable Gobierno Provincial de Tungurahua se puede concluir que:

La institución no posee las seguridades necesarias para evitar o minimizar daños en caso de intrusiones.

El área de sistemas en la institución es relativamente nueva, es por este motivo que hace falta implementar políticas y procedimientos que contribuyan en la seguridad tecnológica. Más aún cuando la institución ha sido víctima de varios ataques informáticos, y la solución se ha limitado a cambiar el firewall. A pesar de los incidentes de seguridad que ha sufrido el Honorable Gobierno Provincial de Tungurahua no existen procedimientos definidos de lo que se debe hacer en caso de una intrusión de seguridad.

4.8. Estudiar los modelos de Análisis Forense más aceptados

4.8.1. Investigación de los modelos de análisis forense informático más aceptados en la actualidad.

Metodología del departamento de Justicia de Estados Unidos de América (DOJ)

El departamento de Justicia de los Estados Unidos desarrolló un diagrama de flujo en el que describe una metodología para el Análisis Forense Digital. No hace distinción entre computadores u otro dispositivo electrónico [24].

Como muestra la figura 4.11 ésta metodología consta de tres etapas:

- Preparación/ Extracción
- Identificación
- Análisis

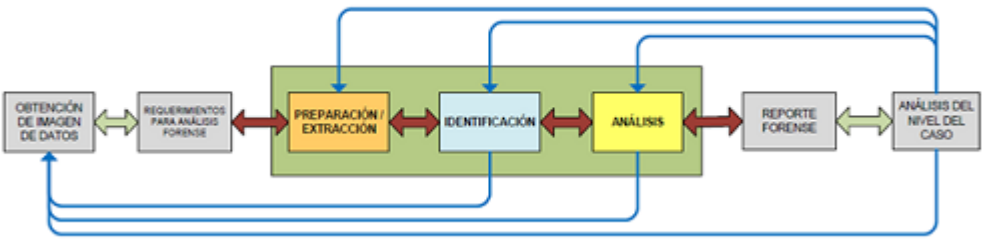

Figura 4.3: Proceso de Análisis Forense DOJ

Modelo de Reith, Carr y Gunsch

Es similar al modelo DFRWS. Los pasos en su modelo son:

- La identificación
- La preparación
- La estrategia de acercamiento
- La preservación
- La colección
- El examen
- El análisis

- La presentación
- Devolviendo la evidencia

Adicional a esto agrega soporte para la preparación de herramientas y la formulación dinámica de acercamientos de investigación. Este modelo también soporta iteraciones libres de clases de actividades individuales.

Este modelo pretende ser abstracto aplicable para cualquier tecnología o cualquier tipo de ciberdelito y que pueda ser utilizado como base otros métodos más detallados para cada tipo específico de investigación [23].

Modelo de Casey

Eoghan Casey presenta un modelo para procesar y examinar evidencias digitales. Tiene los siguientes pasos principales [23]:

1. La Identificación
2. La conservación, la Adquisición y la documentación
3. La Clasificación, la comparación y la individualización
4. La reconstrucción

Modelo DFRWS (Digital Forensics Research Workshop)

Este modelo introduce "Clases de acción en la Investigación digital", las que sirven para clasificar las actividades de una investigación en grupos. Provee una lista de los lugares más comunes en los que se puede encontrar información oculta. Está enfocada a conservar la integridad y mantener la cadena de custodia, además que considera el análisis para grandes volúmenes de información [25].

Las fases de esta metodología son:

- Identificación
- Preservación
- Recolección
- Examinación
- Análisis
- Presentación

Figura 4.4: Fases del modelo DFRWS

Modelo integrado de Brian Carrier y Eugene Spafford

Brian Carrier y Eugene Spafford han propuesto otro modelo que organiza el proceso en cinco grupos, cada uno contiene subfases [23].

- Fases de Preparación
- Fases de Despliegue
- Fases de Investigación Física de la escena del crimen
- Fases de Investigación de la Escena Digital del Delito
- Fase de revisión

Modelo de Lee

Propone la investigación como un proceso. Este modelo se ocupa sólo de investigación de la escena del delito, y no del proceso investigador completo. Identifica cuatro pasos dentro del proceso [23]:

- Reconocimiento
- Identificación
- Individualización
- Reconstrucción

4.9. Analizar los parámetros bajo los cuales se debe crear el modelo de análisis forense informático

4.9.1. Establecimiento de los parámetros para el desarrollo de los posibles procedimientos del modelo de acuerdo a los resultados de las entrevistas.

Para el diseño del modelo de análisis forense se debe tener en cuenta varios parámetros bajo los cuales debe realizarse el modelo, los más importantes son:

Las herramientas a usarse deben ser software libre.

Al ser una institución pública el Honorable Gobierno Provincial está obligado a que la información sea accesible para cualquier ciudadano por la ley de transparencia y acceso a la información.

4.10. Crear procesos que permitan la preparación forense informática de la institución

4.10.1. Elaboración de los pasos del modelo de análisis forense acorde a los parámetros establecidos

Los pasos del modelo de análisis forense se crean dependiendo de la fase y los requerimientos de cada una de ellas, es por eso que se van detallando en el desarrollo del modelo de análisis forense.

4.11. Desarrollar procedimientos de análisis de evidencia digital siguiendo estándares y técnicas establecidas en la institución y que estén contemplados en el marco legal.

4.11.1. Análisis de la ley vigente sobre delitos informáticos.

Regulaciones relacionadas con la seguridad informática y análisis forense digital
Aspectos legales

CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR

Sección tercera

Comunicación e Información

Art. 16. - Todas las personas, en forma individual o colectiva, tienen derecho a:

1. Una comunicación libre, intercultural, incluyente, diversa y participativa, en todos los ámbitos de la interacción social, por cualquier medio y forma, en su propia lengua y con sus propios símbolos.

2. El acceso universal a las tecnologías de información y comunicación.

3. La creación de medios de comunicación social, y al acceso en igualdad de condiciones al uso de las frecuencias del espectro radioeléctrico para la gestión de estaciones de radio y televisión públicas, privadas y comunitarias, y a bandas libres para la explotación de redes inalámbricas.

4. El acceso y uso de todas las formas de comunicación visual, auditiva, sensorial y a otras que permitan la inclusión de personas con discapacidad.

5. Integrar los espacios de participación previstos en la Constitución en el campo de la comunicación.

LEY ORGÁNICA DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA

Art. 1.- Principio de Publicidad de la Información Pública.- El acceso a la información pública es un derecho de las personas que garantiza el Estado. Toda la información que emane o que esté en poder de las instituciones, organismos y entidades, personas jurídicas de derecho público o privado que, para el tema materia de la información tengan participación del Estado o sean concesionarios de éste, en cualquiera de sus modalidades, conforme lo dispone la Ley Orgánica de la Contraloría General del Estado; las organizaciones de trabajadores y servidores de las instituciones del Estado, instituciones de educación superior que perciban rentas del Estado, las denominadas organizaciones no gubernamentales (ONGs), están sometidas al principio de publicidad; por lo tanto, toda información que posean es pública, salvo las excepciones establecidas en esta Ley

Código Orgánico Integral Penal (COIP)

SECCIÓN NOVENA

Delitos contra el derecho a la propiedad Artículo 190.- Apropiación fraudulenta por medios electrónicos.- La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de

otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años.

La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes.

Artículo 191.- Reprogramación o modificación de información de equipos terminales móviles.- La persona que reprograme o modifique la información de identificación de los equipos terminales móviles, será sancionada con pena privativa de libertad de uno a tres años.

Artículo 192.- Intercambio, comercialización o compra de información de equipos terminales móviles.- La persona que intercambie, comercialice o compre bases de datos que contenga.

SECCIÓN TERCERA

Delitos contra la seguridad de los activos de los sistemas de información y comunicación

Artículo 229.- Revelación ilegal de base de datos.- La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años.

Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años.

Artículo 230.- Interceptación ilegal de datos.- Será sancionada con pena privativa de libertad de tres a cinco años:

1. La persona que sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible.

2. La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder.

3. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.

4. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior.

Artículo 231.- Transferencia electrónica de activo patrimonial.- La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años.

Con igual pena, será sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona.

Artículo 232.- Ataque a la integridad de sistemas informáticos.- La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años.

Con igual pena será sancionada la persona que:

1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo.

2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general.

Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a

siete años de privación de libertad.

CÓDIGO ORGÁNICO DE ORGANIZACIÓN TERRITORIAL, AUTONOMÍA Y DESCENTRALIZACIÓN

Artículo 363.- Los gobiernos autónomos descentralizados realizarán procesos para asegurar progresivamente a la comunidad la prestación de servicios electrónicos acordes con el desarrollo de las tecnologías. Los servicios electrónicos que podrán prestar los gobiernos autónomos descentralizados son: información, correspondencia, consultas, trámites, transacciones, gestión de servicios públicos, teleeducación, telemedicina, actividades económicas, actividades sociales y actividades culturales, entre otras. Los gobiernos autónomos descentralizados dotarán servicios de banda libre para el uso de redes inalámbricas en espacios públicos.

4.11.2. Crear procedimientos de análisis de evidencia digital

Los procedimientos a seguir para el análisis de la evidencia digital se detallan en las fases del modelo diseñado para el análisis forense en el Honorable Gobierno Provincial de Tungurahua.

4.12. Diseño y aplicación del Modelo de Análisis Forense para el Honorable Gobierno Provincial de Tungurahua

Un Análisis Forense dependerá tanto del modelo aplicado como de la habilidad y conocimiento del profesional encargado de la realización del mismo.

El presente proyecto se basará en un modelo de tres etapas:

- Análisis Forense Informático Proactivo
- Análisis Forense informático Activo
- Análisis Forense Informático Reactivo

Análisis Forense Informático Pro activo

El conjunto de personas y tecnología debe tener la capacidad de disuadir, retrasar y detectar amenazas e intrusiones, para minimizar el impacto de las mismas y que éstas puedan ser mitigadas en el menor tiempo posible. La seguridad tiene tres elementos fundamentales que son los principales objetivos de los atacantes, estos son la confidencialidad, la integridad y la disponibilidad de recursos.

Esta etapa se refiere a tener una solución antes que se presente el problema. En cualquier institución o empresa lo más importante en cuanto a la seguridad es ser "proactivo".

Para el mejor desarrollo de éste análisis se puede dividir en subfases, guiándose en la estrategia en profundidad.

Defensa en Profundidad

La aplicación de la Seguridad en Profundidad es la mejor opción para una defensa proactiva. Dentro de esta defensa se tiene tres áreas que son:

- Operaciones
- Personas
- Tecnología

Operaciones

En esta área incluye procesos administrativos que respaldan las actividades y la postura de seguridad adoptada por la institución. Para ello lo primero es analizar la institución, es decir: objetivos de la institución, documentos administrativos.

Los documentos administrativos necesarios en esta área son:

- Políticas y procedimientos de Seguridad
- Políticas y procedimientos de gestión de TI
- Procedimientos de respuesta de incidentes
- Políticas y procedimientos de Gestión de la Institución

El área de Sistemas del Honorable Gobierno Provincial de Tungurahua no cuenta con todas las políticas necesarias para un análisis Forense proactivo por lo cual es necesario redactarlas y que las mismas sean aprobadas por las autoridades de la institución. (Anexo A)

Personas

En cualquier empresa o institución el factor humano desempeña un papel muy importante en la estrategia de seguridad, pues son los más vulnerables ya que son los que manejan la información.

Las actividades en ésta área son:

- Estructura Organizacional
- Roles y Responsabilidades
- Seguridad Física
- Capacitación, formación y entrenamiento

Estructura Organizacional

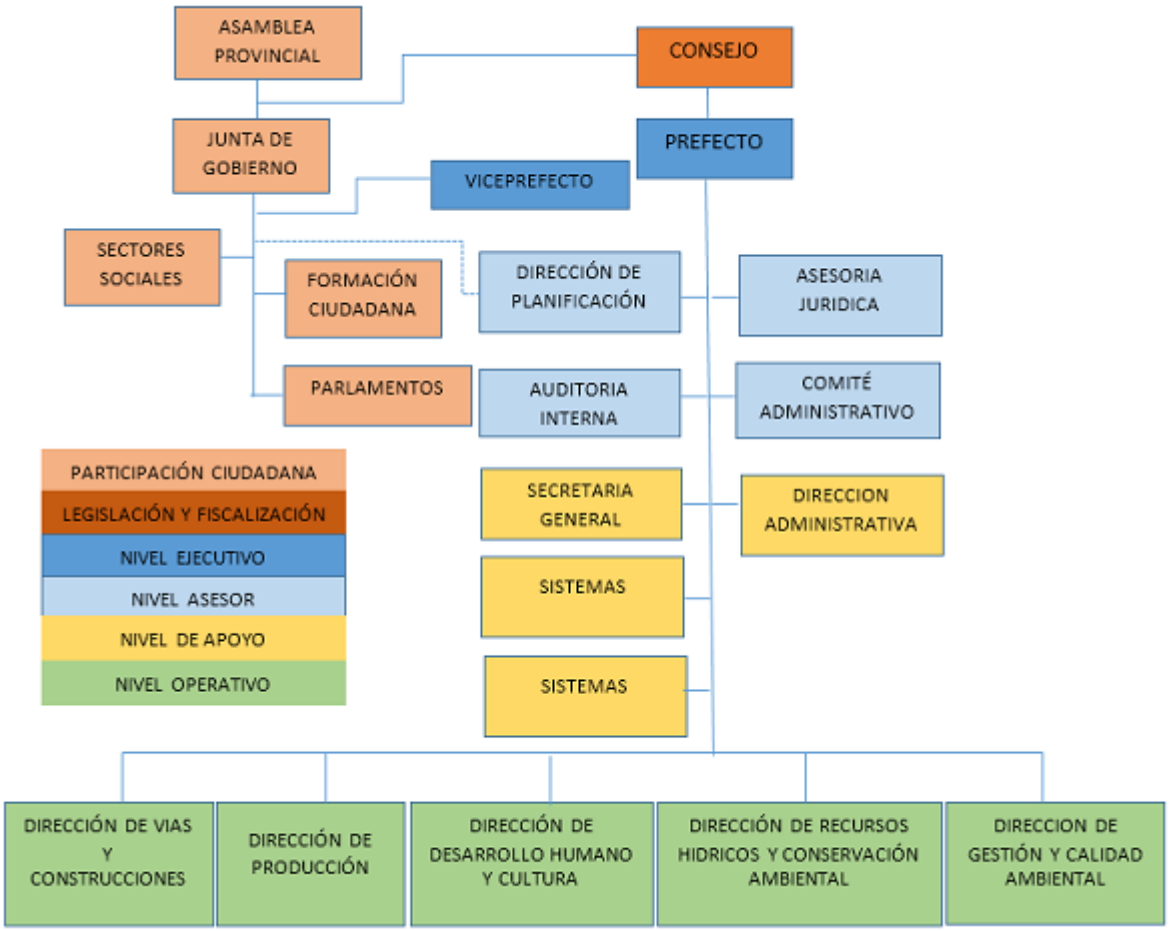

Figura 4.5: Organigrama del Honorable Gobierno Provincial de Tungurahua

En la figura 4.13 está detallado el organigrama del Honorable Gobierno Provincial de Tungurahua.

Roles y Responsabilidades

Los roles y responsabilidades serán de acuerdo al organigrama de la institución.

Seguridad del Personal

Dentro de esta política está los lineamientos del Honorable Gobierno Provincial de Tungurahua en cuanto a: Uso de recursos tecnológicos, responsabilidades y sanciones para todo el personal.

Capacitación y formación del personal

La capacitación y formación del personal en cuanto a seguridad debe ser parte de la institución, pues un personal capacitado es la mejor defensa de cualquier empresa o institución.

La capacitación del personal es el área de seguridad debe estar a cargo del área de Sistemas de la institución.

Plan y equipo de respuesta a incidentes

El plan de respuesta a incidentes debe estar lista para entrar en acción ante cualquier eventualidad.

Seguridad Física

Protección de las áreas de procesamiento de datos, así como el acceso al lugar donde se encuentran los servidores debe tener lineamientos definidos.

Código de conducta

Toda institución o empresa requiere tener código de conducta para todo el personal de la institución. Este debe ser de conocimiento de todos los empleados con el objetivo de crear una cultura de seguridad en la institución. Las instituciones públicas tienen la obligación de cumplir la Norma de control Interno denominada "200-01 - Integridad y Valores Éticos"

Tecnología

- Defensa por capas
- Análisis de riesgos
- Infraestructura tecnológica

  Defensa por capas

  La seguridad por capas es parte de la defensa en profundidad.

  - Seguridad de Usuario
  - Seguridad Física
  - Seguridad de Red
  - Seguridad de Aplicaciones
  - Seguridad de Servidores
  - Seguridad de Sistemas Operativos
  - Seguridad de Información

  Cada una de estas capas se irá definiendo de acuerdo a las necesidades del modelo de análisis forense en desarrollo.

  Seguridad de Usuarios

  Esta capa está formada por las políticas y procedimientos del área de "Personas", contemplada en la defensa en profundidad. El personal es llamado usuario cuando tiene acceso a la infraestructura tecnológica de la institución.

  La gestión de usuarios está definida en las políticas del área de Personas y gestión de perfil (Anexo A).

El desarrollo del análisis Forense Informático Pro activo se realizará en varias etapas:

- Preparación
- Despliegue
- Investigación
- Revisión

Preparación

La institución debe estar preparada en todos los sentidos y áreas, entre los puntos a preparar tenemos:

- El punto de inicio para una estrategia de seguridad es hacer una evaluación y gestión de riesgos tecnológicos.
- El objetivo de ésta es que las operaciones y la infraestructura tecnológica puedan dar soporte al llevar a cabo un procedimiento de análisis forense digital.
- La validación del software y hardware a utilizarse, con la finalidad de que éste funcione correctamente debe estar delineada dentro de las políticas de la institución, como medida de precaución.
- Educación es la parte más importante en la seguridad, dado que un personal bien educado en materia de seguridad es la mejor defensa de cualquier institución o empresa.
- Mejorar la capacidad de adquirir evidencia digital en una organización, incluirá la creación de políticas y procedimientos de análisis forense con el fin de ponerlos en práctica en su momento. Las políticas y procedimientos que se deben tener en cuanto a la preparación de la institución están definidas en la defensa en profundidad.

Dentro de la preparación también se usará la estrategia de defensa en profundidad, dividiendo en tres fases la preparación:

- Operaciones
- Personas
- Tecnología

  Operaciones

  Crear requerimientos y procesos forenses

- Identificar y definir las fuentes de evidencia digital a partir evaluación y gestión de riesgos tecnológicos de la institución.

  El objetivo de ésta medida en definir formalmente a la evidencia como una herramienta de control gerencial para la transparencia de operaciones, uso apropiado de activos, etc.

- Determinar requerimientos de recolección de evidencia

  Detallar los requisitos para el proceso de recolección de la evidencia digital, estos pueden ser técnicos, legales, administrativos, entre otros.

- Las auditorias deben estar enfocadas a la detección de amenazas e impedir amenazas mayores.

  Complementar los procesos de auditoria para utilizar la evidencia digital.

Definir políticas y procedimientos de análisis forense

- Políticas y procedimientos para el tratamiento de la evidencia digital

  Estas deben incluir las premisas necesarias para la preservación, recolección, manejo, manipulación, almacenamiento cadena de custodia, análisis y disposición de la evidencia digital.

- Políticas y Procedimientos para las investigaciones forenses informáticas

  Debe contener los lineamientos necesarios de una investigación forense.

Verificar que los planes de respuesta de incidentes y continuidad del negocio abarquen los procesos forenses.

El objetivo de este punto es incluir procesos que permitan la preparación forense de la institución. Entre lo que podemos destacar:

- Disponibilidad de herramientas forenses listas para ser utilizadas en caso de incidentes.
- Procedimientos de contención y aislamiento de incidentes
- Procedimientos de monitoreo y extracción de evidencia en tiempo real.
- Procedimientos de continuidad y restablecimiento de los recursos afectados, tomando en cuenta la preservación de la evidencia digital.

Personas

Establecer un equipo de respuesta a incidentes

La Institución debe tener un equipo preparado en caso de incidentes que sea capaz de realizar la investigación forense, dicho equipo debe poseer los conocimientos necesarios sobre el tema para no cometer errores durante la investigación.

El área de sistemas del Honorable Gobierno Provincial de Tungurahua es relativamente pequeña, por lo cual dependiendo de la situación podría hacer falta que todo el personal del área colabore en la solución de incidentes por éste motivo todos deben estar capacitados para hacer frente a una investigación forense.

Tecnología

La preparación tecnológica se refiere al despliegue de barreras para evitar o retrasar al máximo las intrusiones informáticas, las mismas que están detalladas más adelante.

Despliegue

Como en el área militar es necesario proteger todos los medios de acceso a la institución. Esto consiste en poner frenos contra amenazas potenciales, ya que ninguna protección es impenetrable, es necesario multiplicar las barreras [5]. Estas barreras pueden ser:

Barreras Psicológicas: Señales de advertencia, avisos, etc.

Barreras Electrónicas: Alarmas, CCTV, luces, etc.

Barreras Físicas: Muros, cajas fuertes, etc.

Barreras de Procedimientos: tarjetas de identificación, control de acceso, etc.

Los equipos deben incluir una configuración que ayude a los procesos forenses. Parte fundamental de la configuración es el monitoreo en tiempo real.

En el caso del Honorable Gobierno Provincial de Tungurahua se realiza monitoreo en tiempo real con la ip de la máquina, esto se hace solo en caso de ser necesario. Esta configuración es indispensable para dar apoyo a los procesos forenses, especialmente en el análisis forense informático activo.

Las políticas y procedimientos deben contemplar los procesos a seguir cuando se adquiere nuevos equipos tecnológicos, con el objetivo que éstos sean correctamente configurados y no se conviertan en una vulnerabilidad para la institución.

Para iniciar con el despliegue debemos saber dónde y como poner esas barreras que nos ayudarán a proteger la institución de posibles ataques o intrusiones informáticas, para esto se va a realizar hacking ético.

Investigación

Entender las debilidades y riesgos más comunes que pueden ser aprovechadas por los intrusos es la estrategia más inteligente para seguridades efectivas.

Dentro de los datos a investigar tenemos los siguientes:

- Conocer y documentar las ip asignadas en la red.
- Conocer la lista de equipos de usuario, sus direcciones MAC e IP, el nombre de cada usuario y su ubicación física[14].
- Identificar las herramientas adecuadas para realizar un análisis forense en caso de ser necesario.

Dentro de esta subfase se realizará un hacking ético, con la finalidad de identificar las vulnerabilidades que presenta la red, para corregirlas e implementar el sistema de detección de intrusos. Para esta tarea se va a utilizar principalmente Kali Linux, ésta herramienta cuenta con varios programas Open source dirigidos a pruebas de penetración y de auditoría de seguridad.

Para analizar las vulnerabilidades vamos a seguir la metodología OSSTMM por sus siglas en inglés “Open Source Security Testing Methodology Manual” o “Manual de la Metodología Abierta de Testeo de Seguridad”[26], que es la más utilizada para revisar la seguridad de los sistemas.

Comprende varios ámbitos:

Seguridad Física

Dentro de la seguridad física tenemos:

- Seguridad de la Información
- Seguridad de los Procesos
- Seguridad en las Tecnologías de Internet

- Seguridad en las Comunicaciones
- Seguridad Inalámbrica

Seguridad de la Información

Dentro de esta sección está el recolectar toda la información que sea posible, sin tener contacto directo con la institución. Para ello se utiliza Footprinting, que consiste básicamente en recolectar la información de carácter público sobre el Honorable Gobierno Provincial de Tungurahua y que más adelante será útil para realizar el hacking ético.

Si se tratase de un ataque real, al utilizar footprinting el atacante no estaría cometiendo ningún delito porque al ser una institución pública la información es de libre acceso.

Maltego ayudará a investigar las relaciones existentes que tiene el dominio "Tungurahua.gob.ec".

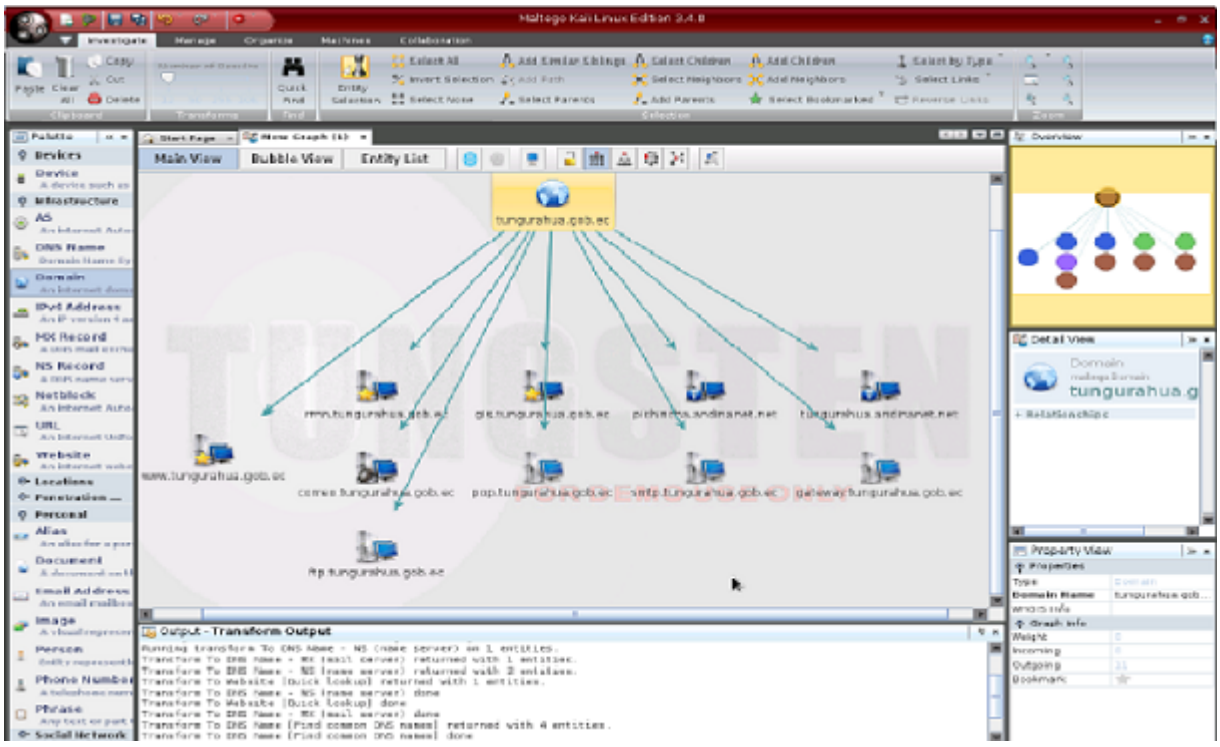

Figura 4.6: Análisis con Maltego, Dominio Tungurahua.gov.ec

En la figura 4.14 se puede observar las transformaciones DNS, para el dominio "Tungurahua. gob.ec", se muestra servidores DNS, servidores de correo y servidores relacionados. Las flechas indican que existe relación entre el objeto padre y los objetos hijos, las estrellas amarillas indican que el objeto provee servicios web.

Resultados obtenidos con maltego:

Nombre	Dirección IP	Servicio
www.tungurahua.gob.ec	174.142.242.142	Website
correo.tungurahua.gob.ec	181.112.146.3	MX Record
pop.tungurahua.gob.ec	181.112.146.3	DNS Name
gateway.tungurahua.gob.ec	181.112.146.4	DNS Name
gis.tungurahua.gob.ec	181.112.146.5	Website
ftp.tungurahua.gob.ec	181.112.146.14	DNS Name
rrnn.tungurahua.gob.ec	181.112.146.14	Website
smtp.tungurahua.gob.ec	181.112.146.8	DNS Name

Tabla 4.1: Listado de Servidores

En la tabla 4.1 está detallado los servidores del Honorable Gobierno Provincial de Tungurahua, sus respectivas IP y servicio.

Por ser una institución pública toda la información está al alcance de cualquier usuario por lo que es fácil conseguir datos que ayuden al atacante para utilizar ingeniería social. El buscador de Google, puede ser muy provechoso si se utiliza de la manera correcta para que filtre la información y reducir los resultados al máximo, esta técnica se la denomina “Google Hacking”.

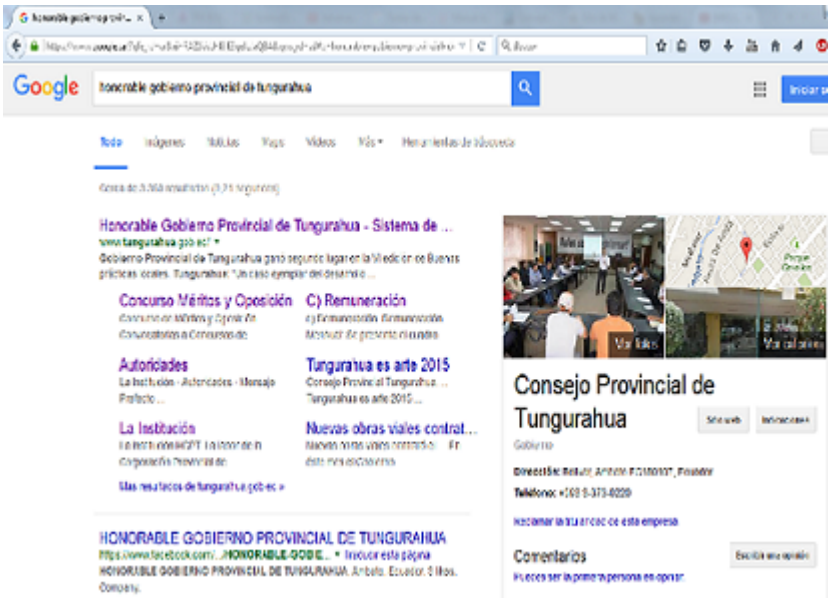

Figura 4.7: Búsqueda en Google del Honorable Gobierno Provincial de Tungurahua

En la figura 4.15 se observa la búsqueda de “Honorable Gobierno

Provincial de Tungurahua" en google, mediante "Google Hacking" se puede reducir los resultados.

Buscando información en NIC(Network Information Center), "NIC es la autoridad que delega los nombres de dominio a quienes los solicitan. Cada país en el mundo cuenta con una autoridad que registra los nombres bajo su jurisdicción".

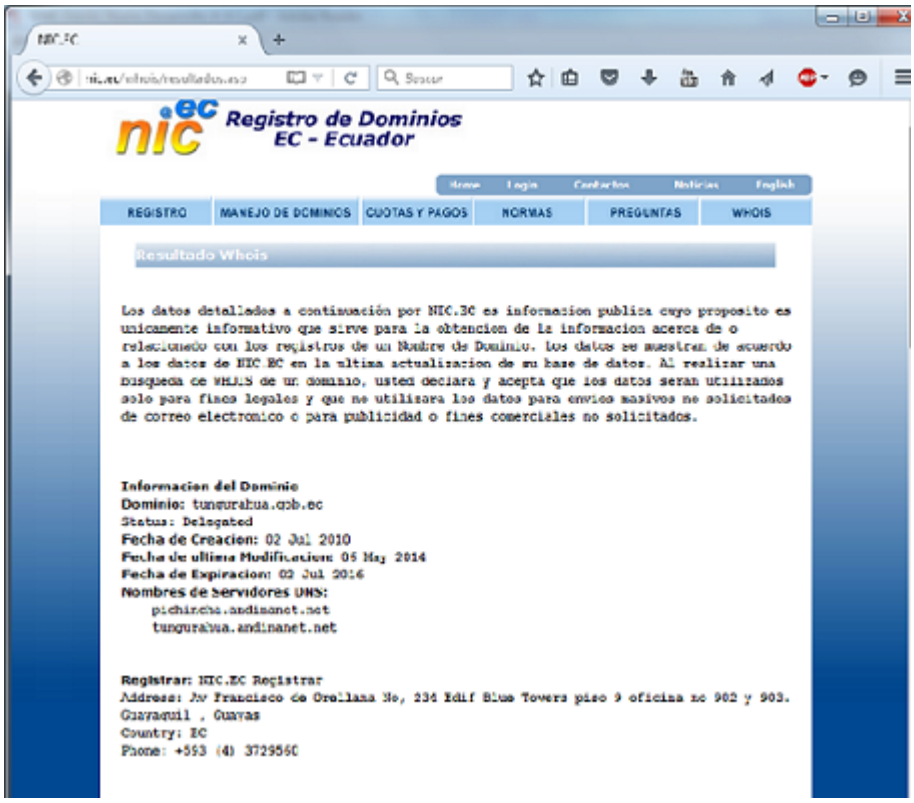

Figura 4.8: NIC del dominio tungurahua.gov.ec

En la figura 4.16 muestra la consulta del dominio tungurahua.gov.ec en la base de datos del NIC. Al estar expuesta datos como la información de empleados, mismos que pueden ser usados para un ataque de ingeniería social.

Datos obtenidos de consultar el NIC:

Registrante: Email: prefecto@tungurahua.gob.ec

Teléfono: 5933-2421355 Fax: 5933-2422297

Nombre: Luis Fernando Naranjo Lalama

Organización: H. Gobierno Provincial de Tungurahua

Dirección: Bolívar 491 y Castillo Ambato, Tungurahua 1801320

EC

Contacto Administrativo:

Email: tecnologiasinformaticas@tungurahua.gob.ec

Teléfono: 593-3730220 Fax: 593-32422297

Nombre: Xavier Francisco López Andrade

Organización: H.Gobierno Provincial de Tungurahua

Dirección: Bolívar 491 y Castillo Ambato, Tungurahua 1801320

EC

Contacto Técnico:

Email: proyectosti@tungurahua.gob.ec

Teléfono: 593-33730220

Nombre: Luis Alberto Bravo Moncayo

Organización: H. Gobierno Provincial de Tungurahua

Dirección: Castillo y Sucre Ambato, Tungurahua 1801320

EC

Contacto de Facturación:

Email: yolanda.pazmino@tungurahua.gob.ec

Teléfono: 5933-2421993 Fax: 593-2826419

Nombre: Econ. Yolanda Beatriz Pazmiño

Organización: H. Gobierno Provincial de Tungurahua

Dirección: Bolívar 491 y Castillo Ambato, Tungurahua 1801320

EC

En la página web del Honorable Gobierno Provincial de Tungurahua se puede obtener casi toda la información sobre la institución, sus empleados e inclusive de sus documentos sobre las funciones que desempeña, ya que por ser una institución pública tiene la obligación de difundir de manera transparente la información.

A través de toda la información recolectada se puede crear un Diccionario de datos para las pruebas posteriores.

Seguridad de los Procesos

Se realiza pruebas en las que el usuario atacante tiene algún privilegio, es decir tiene acceso a los equipos de comunicación y a la información, de igual manera se realizan pruebas desde fuera de la red, con el objetivo de probar la seguridad tecnológica de la institución.

Seguridad en las Tecnologías de Internet

- **Sondeo a las IP públicas de la institución**

  Para el análisis de las ip públicas se utilizarán varias herramientas dependiendo de lo que se desea averiguar mediante el análisis

  Utilizando Whatweb obtendremos la siguiente información:

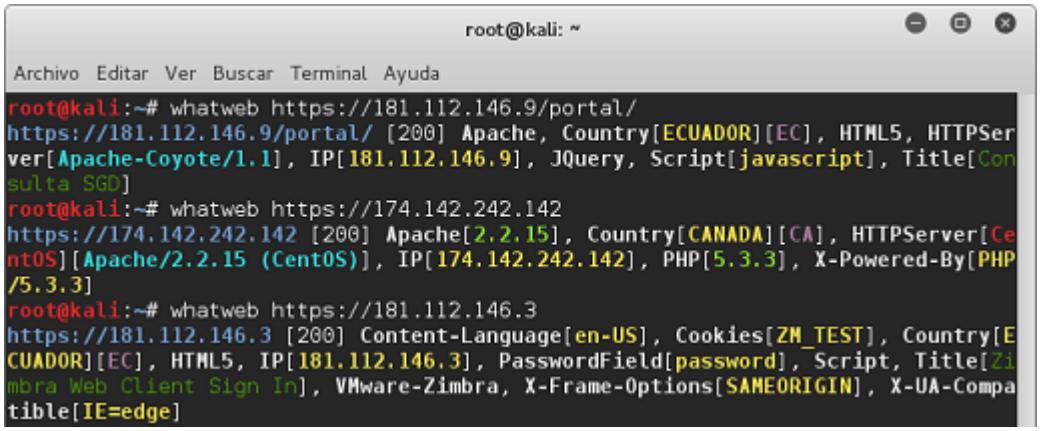

Figura 4.9: Sondeo de las IP públicas con whatweb

En la figura 4.17 se puede observar los análisis con whatweb a los servidores: 181.112.146.9, 174.142.242.142(Página web de la institución) y 181.112.146.3

De lo cual se puede concluir que la página web de la institución está almacenada en un servidor ubicado en Canadá, en una distribución Centos. Mientras que el resto de los servidores están ubicados en Ecuador.

Inyección SQL

Con la finalidad de encontrar vulnerabilidades en las IP públicas de la institución se realizó una prueba con SQLMAP para ver si son vulnerables a inyección SQL, es decir si se puede acceder a la base de datos de la aplicación, los resultados de ésta fueron los siguientes:

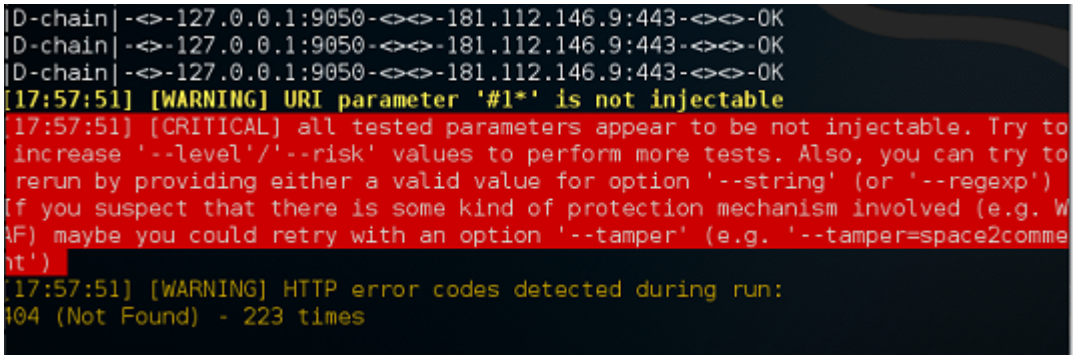

Figura 4.10: Inyección SQL en www.tungurahua.gov.ec

En la figura 4.18 muestra los mensajes de advertencia referente a la IP 181.112.146.9, indicando que no es inyectable y Critico: todos los parámetros analizados parecen no ser inyectable

Del análisis realizado se puede concluir que las web de la institución no son inyectables, es decir que tienen las seguridades necesarias para protegerse contra este tipo de ataques.

- **Sondeo de la Red**

  Se obtiene las direcciones IP de la institución y se realiza un reconocimiento de la red de manera detallada.

  Redes Internas de la institución

Red	Máscara	Área
172.16.0.0	255.255.255.224	Administrativa
172.16.1.0	255.255.255.224	Hídricos
172.16.2.0	255.255.255.224	Planificación
172.16.3.0	255.255.255.224	Red de Servicios

Tabla 4.2: Redes internas del Honorable Gobierno Provincial de Tungurahua

La tabla 4.2 muestra el listado de las redes internas del Honorable Gobierno Provincial de Tungurahua con su respectiva mascara y el área a la que están designadas las mismas.

  - **Servidores de la Institución**

Dirección	Nombre	Sistema Operativo
172.16.1.132	oracle.tungurahua.gob.ec	Red Hat 64 bits
172.16.1.133	gis.tungurahua.gob.ec	Centos 2.16.0
172.16.1.134	correo.tungurahua.gob.ec	Ubuntu Server 14.04 LTS
172.16.1.135	dchgpt01.tungurahua.gob.ec	Windows Server 2012
172.16.1.136	tramites.tungurahua.gob.ec	Ubuntu Server 14.04 LTS
172.16.1.140	central4760	Windows XP Profesional
172.16.1.141	symantec.tungurahua.gob.ec	Windows Server 2003
172.16.1.142	local_domain	CentOS
172.16.1.143	mapas.tungurahua.gob.ec	CentOS
172.16.1.144	bddespacial	CentOS
172.16.1.145	srvap01	CentOS
172.16.1.146	rrnn.tungurahua.gob.ec	CentOS
172.16.1.147	bdd_nr	CentOS
172.16.1.148	bdd_r	CentOS
172.16.1.149	ftp.tungurahua.gob.ec	CentOS
172.16.1.159	citrix	Citrix version 6.1
172.16.1.161	serwebcentos	Centos
172.16.1.162	hgpt-serverprue	Windows XP Profesional
172.16.1.169	vm-servidor1	Vmware Vmvisor 5.5 Update 2

Tabla 4.3: Servidores del Honorable Gobierno provincial de Tungurahua

La tabla 4.3 servidores del Honorable Gobierno provincial de Tungurahua con sus respectivas IP, nombres y el sistema operativo que tienen instalado.

◇ **Identificación de Servicios**

Lo primero es realizar un sondeo de puertos, con el objetivo de descubrir los servicios que se están ejecutando. Con la herramienta Zenmap (que es parte de Kali linux) se sondea los puertos y los servicios de cada equipo en estudio.

Esta herramienta dará el número del puerto, el protocolo que utiliza, estado, servicio y la versión o detalle del mismo.

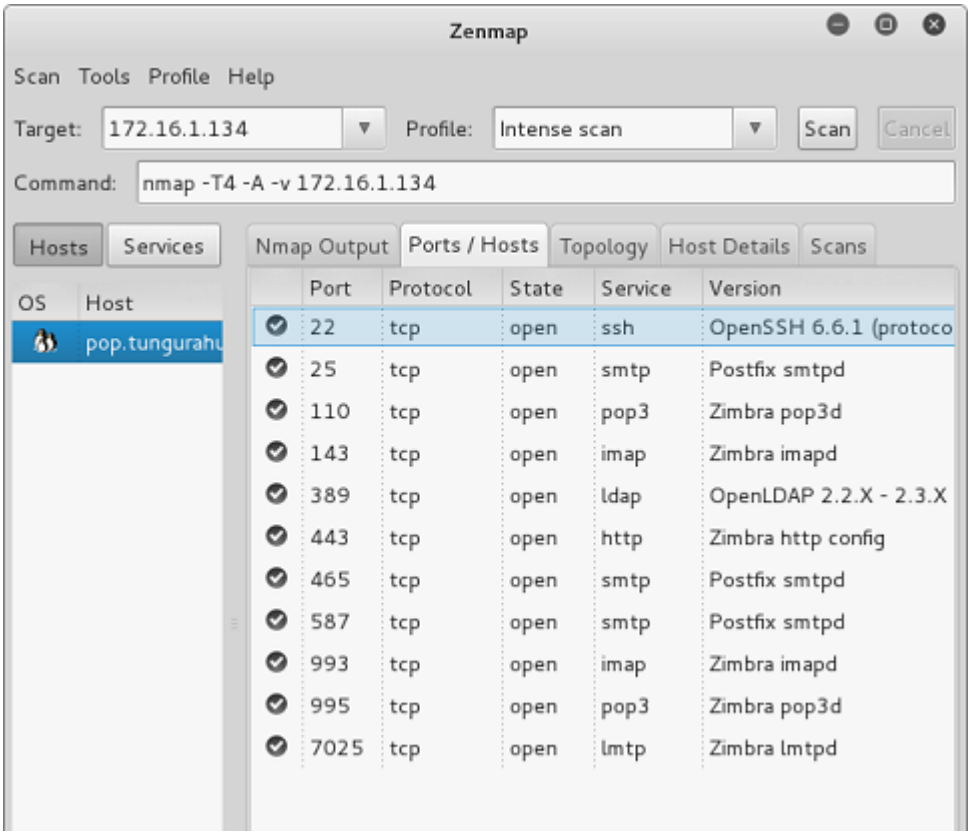

Figura 4.11: Sondeo de puertos NMAP Servidor correo.tungurahua.gob.ec

La figura 4.11 muestra el escaneo de puertos realizado con NMAP al servidor correo.tungurahua.gob.ec que tiene la IP 172.16.1.134

Puerto	Protocolo	Servicio	Detalle
22	tcp	ssh	OpenSSH 5.3 (protocol 2.0)
111	tcp	rpcbind	2-4 (RPC #100000)
1521	tcp	oracle-tns	Oracle TNS Listener

Tabla 4.4: Sondeo de puertos NMAP Servidor oracle.tungurahua.gob.ec

En la tabla 4.4 muestra los puertos abiertos del servidor oracle.tungurahua.gob.ec que tiene la IP 172.16.1.132, además del protocolo, el servicio y detalle de los mismos.

Puerto	Protocolo	Servicio	Detalle
22	tcp	ssh	OpenSSH 4.3
80	tcp	http	Apache httpd
111	tcp	rpcbind	2 (RPC #100000)
443	tcp	http	Apache httpd
5432	tcp	postgresql	PostgreSQL DB (Spanish)
6000	tcp	x11	
6001	tcp	x11	
10000	tcp	http	MiniServ 1.690 (Webmin httpd)

Tabla 4.5: Sondeo de puertos NMAP Servidor gis.tungurahua.gob.ec

La tabla 4.5 muestra los puertos abiertos del servidor gis.tungurahua.gob.ec que tiene la IP 172.16.1.133, además del protocolo, el servicio y detalle de los mismos.

Puerto	Protocolo	Servicio	Detalle
22	tcp	ssh	OpenSSH(protocol 2.0)
25	tcp	smtp	Postfix smtpd
80	tcp	http	Zimbra http
110	tcp	pop3	Zimbra pop3
143	tcp	imap	Zimbra imapd
389	tcp	Idap	OpenLDAP 2.3.X
443	tcp	ssl/http	Zimbra http
465	udp	ssl/smtp	Postfix smtpd
587	tcp	smtp	Postfix smtpd
993	tcp	ssl/imap	Zimbra imapd
995	tcp	ssl/pop3	Zimbra pop3

Tabla 4.6: Sondeo de puertos NMAP Servidor correo.tungurahua.gob.ec

La tabla 4.6 muestra los puertos abiertos del servidor correo.tungurahua.gob.ec que tiene la IP 172.16.1.134, además del protocolo, el servicio y detalle de los mismos.

Puerto	Protocolo	Servicio	Detalle
53	tcp	domain	Microsoft DNS
88	tcp	kerberos-sec	Windows 2003 kerberos
135	tcp	msrpc	Microsoft Windows RPC
139	tcp	netbios-ssn	Microsoft Windows 98 netbios-ssn
389	tcp	ldap	
445	tcp	microsoft-ds	(primary domain: HGPT)
464	tcp	kpasswd5	
593	tcp	ncacn_http	Microsoft Windows RPC over HTTP 1.0
636	tcp	tcpwrapped	
3268	tcp	ldap	
3269	tcp	tcpwrapped	
3389	tcp	ms-wbt-server	
49154	tcp	msrpc	Microsoft Windows RPC
49155	tcp	msrpc	Microsoft Windows RPC
49157	tcp	ncacn_http	Microsoft Windows RPC over HTTP 1.0
49158	tcp	msrpc	Microsoft Windows RPC
49165	tcp	msrpc	Microsoft Windows RPC

Tabla 4.7: Sondeo de puertos NMAP Servidor dchgpt01.tungurahua.gob.ec

La tabla 4.7 muestra los puertos abiertos del servidor dchgpt01.tungurahua.gob.ec que tiene la IP 172.16.1.135, además del protocolo, el servicio y detalle de los mismos.

Puerto	Protocolo	Servicio	Detalle
22	tcp	ssh	OpenSSH (Ubuntu Linux; protocol 2.0)
80	tcp	http	Apache httpd
443	tcp	http	Apache httpd
10000	tcp	http	MiniServ 1.690 (Webmin httpd)

Tabla 4.8: Sondeo de puertos NMAP tramites.tungurahua.gob.ec

La tabla 4.8 muestra los puertos abiertos del servidor tramites.tungurahua.gob.ec que tiene la IP 172.16.1.136, además del protocolo, el servicio y detalle de los mismos.

Puerto	Protocolo	Servicio	Detalle
80	tcp	http	Apache httpd
135	tcp	msrpc	Microsoft Windows RPC
139	tcp	Netbios-ssn	
389	tcp	ldap	(Anonymous bind)
445	tcp	Microsoft-ds	Microsoft Windows XP microsoft-ds
636	tcp	ssl/ldap	(Anonymous bind OK)
1025	tcp	giop	COBRA naming server
3389	tcp	ms-wbt-server	Microsoft Terminal Service
3998	tcp	ldap	(Anonymous bind OK)
5405	tcp	netsupport	NetSupport PC remote control
6005	tcp	tcpwrapped	
8009	tcp	ajp13	Apache Jserv (Protocol 1.3)
8090	tcp	http	Apache Tomcat/ Coyote JSP engine 1.1

Tabla 4.9: Sondeo de puertos NMAP central4760

La tabla 4.9 muestra los puertos abiertos del servidor central4760 que tiene la IP 172.16.1.140, además del protocolo, el servicio y detalle de los mismos.

Puerto	Protocolo	Servicio	Detalle
80	tcp	http	Apache httpd 2.2.21 (Win 32)
135	tcp	msrpc	Microsoft Windows RPC
139	tcp	Netbios-ssn	Microsoft Windows 98 netbios-ssn
445	tcp	microsoft-ds	Microsoft Windows Server 2008
1100	tcp	mctp?	
3389	tcp	ssl/ms-wbt-server?	
8443	tcp	ssl/http	Symantec Messaging Gateway smtpd
9090	tcp	http	Symantec Endpoint Protection manager
49152	tcp	msrpc	Microsoft Windows RPC
49153	tcp	msrpc	Microsoft Windows RPC
49154	tcp	msrpc	Microsoft Windows RPC
49175	tcp	msrpc	Microsoft Windows RPC

Tabla 4.10: Sondeo de puertos NMAP symantec.tungurahua.gob.ec

La tabla 4.10 muestra los puertos abiertos del servidor symantec.tungurahua.gob.ec que tiene la IP 172.16.1.141, además del protocolo, el servicio y detalle de los mismos.

Puerto	Protocolo	Servicio	Detalle
21	tcp	ftp	Vsftpd 2.0.5
22	tcp	ssh	OpenSSH 4.3 (Protocol 2.0)
111	tcp	rpcbind	2 (RPC #100000)
992	tcp	status	1 (RPC #100024)
5801	tcp	Vnc-http	RealVBC 4.0 (resolution: 400x250)
5901	tcp	vnc	VNC (protocol 3.8)
6001	tcp	X11	

Tabla 4.11: Sondeo de puertos NMAP local_domain

La tabla 4.11 muestra los puertos abiertos del servidor local_domain que tiene la IP 172.16.1.142, además del protocolo, el servicio y detalle de los mismos.

Puerto	Protocolo	Servicio	Detalle
22	tcp	ssh	OpenSSH 5.3 (protocol 2.0)
80	tcp	http	Apache httpd 2.2.15 (CentOS)

Tabla 4.12: Sondeo de puertos NMAP mapas.tungurahua.gob.ec

La tabla 4.12 muestra los puertos abiertos del servidor mapas.tungurahua.gob.ec que tiene la IP 172.16.1.143, además del protocolo, el servicio y detalle de los mismos.

Puerto	Protocolo	Servicio	Detalle
22	tcp	ssh	OpenSSH 5.3 (protocol 2.0)
5432	tcp	postgresql	PostgreSQL DB 9.2.0 – 9.2.2

Tabla 4.13: Sondeo de puertos NMAP bddespacial

La tabla 4.13 muestra los puertos abiertos del servidor bddespacial que tiene la IP 172.16.1.144, además del protocolo, el servicio y detalle de los mismos.

Puerto	Protocolo	Servicio	Detalle
22	tcp	ssh	OpenSSH 5.3(protocol 2.0)
111	tcp	rpcbind	
8009	tcp	ajp13	Apache Jserv(protocol v1.3)
8080	tcp	http	Apache Tomcat/Coyote JSJ engine 1.1
8081	tcp	http	Apache Tomcat/Coyote JSJ engine 1.1
8443	tcp	ssl/http	Apache Tomcat/Coyote JSJ engine 1.1
9999	tcp	jboss-remoting	JBoss Remoting

Tabla 4.14: Sondeo de puertos NMAP srvap01 45

La tabla 4.14 muestra los puertos abiertos del srvap01 que tiene la IP 172.16.1.145, además del protocolo, el servicio y detalle de los mismos.

Puerto	Protocolo	Servicio	Detalle
22	tcp	ssh	OpenSSH 5.3 (protocol 2.0)
80	tcp	http	Apache httpd
81	tcp	http	Apache httpd
111	tcp	rpcbind	2-4 (RPC #100000)
443	tcp	https	Apache

Tabla 4.15: Sondeo de puertos NMAP rrnn.tungurahua.gob.ec

La tabla 4.15 muestra los puertos abiertos del servidor rrnn.tungurahua.gob.ec que tiene la IP 172.16.1.146, además del protocolo, el servicio y detalle de los mismos.

Puerto	Protocolo	Servicio	Detalle
22	tcp	ssh	OpenSSH 5.3 (protocol 2.0)
80	tcp	http	Apache httpd 2.2.15 (CentOS)
111	tcp	rpcbind	2-4 (RPC #100000)
443	tcp	http	Apache httpd 2.2.15 (CentOS)
5432	tcp	postgresql	PostgreSQL DB

Tabla 4.16: Sondeo de puertos NMAP bdd_nr 47

La tabla 4.16 muestra los puertos abiertos del servidor bdd_nr que tiene la IP 172.16.1.147, además del protocolo, el servicio y detalle de los mismos.

Puerto	Protocolo	Servicio	Detalle
22	tcp	ssh	OpenSSH 5.3 (protocol 2.0)
80	tcp	http	Apache httpd 2.2.15 (CentOS)

Tabla 4.17: Sondeo de puertos NMAP bdd_r 48

La tabla 4.17 muestra los puertos abiertos del servidor local_domain que tiene la IP 172.16.1.142, además del protocolo, el servicio y detalle de los mismos.

Puerto	Protocolo	Servicio	Detalle
21	tcp	ftp	vsftpd 2.2.2
22	tcp	ssh	OpenSSH 5.3 (protocol 2.0)

Tabla 4.18: Sondeo de puertos NMAP ftp.tungurahua.gob.ec

La tabla 4.18 muestra los puertos abiertos del servidor ftp.tungurahua.gob.ec que tiene la IP 172.16.1.149, además del protocolo, el servicio y detalle de los mismos.

Puerto	Protocolo	Servicio	Detalle
22	tcp	ssh	OpenSSH 4.3 (protocol 2.0)
80	tcp	http	Citrix X en Simple HTTP Server
443	tcp	ssl/http	Citrix X en Simple HTTP Server

Tabla 4.19: Sondeo de puertos NMAP citrix

La tabla 4.19 muestra los puertos abiertos del servidor citrix que tiene la IP 172.16.1.159, además del protocolo, el servicio y detalle de los mismos.

Puerto	Protocolo	Servicio	Detalle
22	tcp	ssh	OpenSSH 4.3 (protolo 2.0)
80	tcp	http	Apache httpd 2.2.3

Tabla 4.20: Sondeo de puertos NMAP serwebcentos

La tabla 4.20 muestra los puertos abiertos del servidor serwebcentos que tiene la IP 172.16.1.161, además del protocolo, el servicio y detalle de los mismos.

Puerto	Protocolo	Servicio	Detalle
80	tcp	http	Apache httpd 2.2.11
3389	tcp	ms-wbt-server	Microsoft Terminal Service

Tabla 4.21: Sondeo de puertos NMAP hgpt-serverprue 62

La tabla 4.21 muestra los puertos abiertos del servidor hgpt-serverprue que tiene la IP 172.16.1.162, además del protocolo, el servicio y detalle de los mismos.

Puerto	Protocolo	Servicio	Detalle
22	tcp	ssh	OpenSSH 5.6 (protocol 2.0)
80	tcp	http	Vmware Esxi Server httpd
443	tcp	http	Vmware Esxi Server httpd
8000	tcp	http-alt	

Tabla 4.22: Sondeo de puertos NMAP vm-servidor1

La tabla 4.22 muestra los puertos abiertos del servidor vm-servidor1 que tiene la IP 172.16.1.169, además del protocolo, el servicio y detalle de los mismos.

◇ **Búsqueda de Vulnerabilidades**

Los sistemas operativos pueden tener fallos, errores o vulnerabilidades, es por esto que hacer un sondeo de vulnerabilidades es parte importante de la investigación para corregirlas, poner barreras o minimizar daños en caso de intrusiones.

Para la búsqueda de vulnerabilidades se ha utilizado varios programas, estos son: Vega y OpenVas de Kali linux, además con NESSUS, este puede usarse tanto desde Linux como windows.

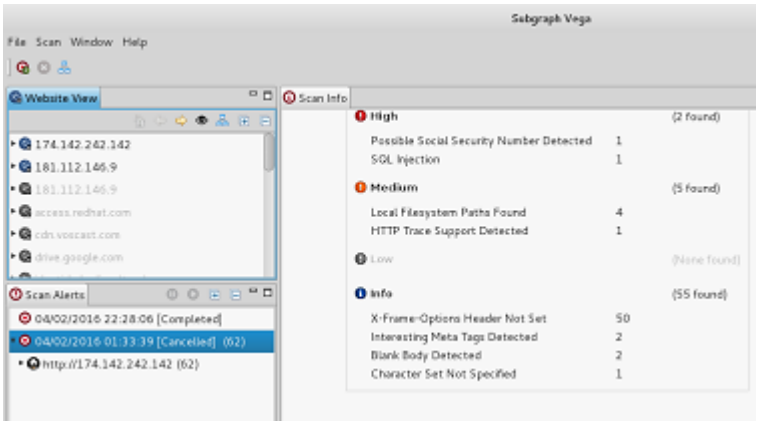

Figura 4.12: Análisis de vulnerabilidades con Vega

En la figura 4.12 se puede observar el análisis de vulnerabilidades a la IP 174.142.242.142(Página web) realizado con Vega, en ésta muestra las vulnerabilidades encontradas de acuerdo a su nivel de riesgo: 2 altas, 5 medias y 35 de tipo información.

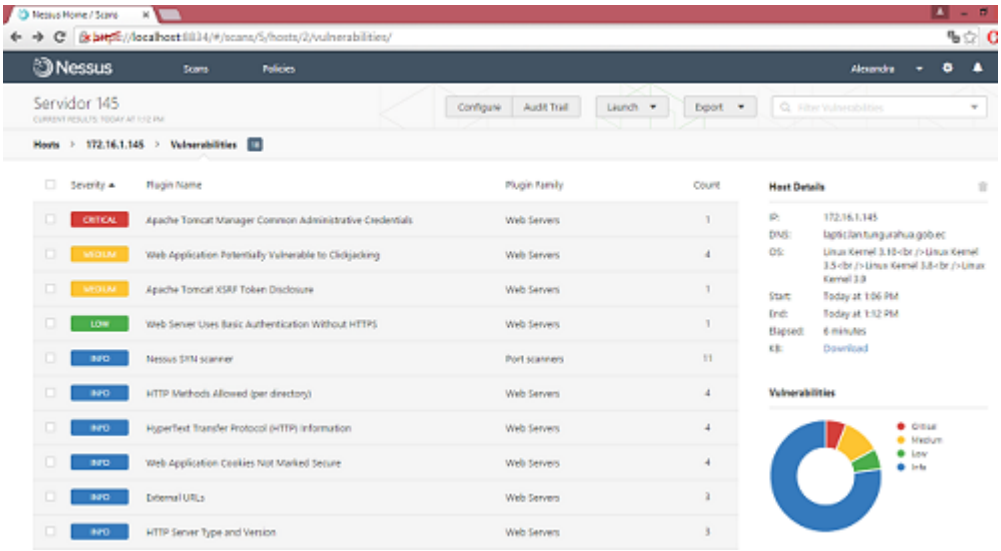

Figura 4.13: Análisis de vulnerabilidades con Nessus

En la figura 4.13 muestra el análisis realizado con Nessus a la IP 172.16.1.145, donde identifica 1 vulnerabilidad crítica, 2 medias, 1 leve y 6 de información.

Vulnerabilidades detectadas en los servidores institucionales

- **Servidor gis.tungurahua.gob.ec**

  Vulnerabilidad: Cuenta PostgreSQL por defecto

  Descripción: Es posible conectarse al servidor de base de datos PostgreSQL remota usando una cuenta por defecto, ya que por defecto la cuenta "postgresql" no tiene definida ninguna clave de acceso y cualquier usuario que tenga acceso a la máquina que este ejecutando PostgreSQL, podrá acceder a todas nuestras bases de datos como usuario "postgres" vía sockets. Esto podría permitir a un atacante lanzar nuevos ataques contra la base de datos.

  Solución: Acceder al host y establecer una contraseña para todas las cuentas afectadas utilizando “Alter usuario”.

  Configurar el archivo ’pg_hba.conf’ para que se requiera una contraseña de autenticación para todos los hosts remotos que tengan acceso legítimo a este servicio y para requerir una contraseña localmente usando la línea "local all password’.

  Vulnerabilidad: Certificado SSL no es confiable

  Descripción: Certificado X.509 del servidor no tiene una firma de una autoridad de certificación pública conocida. Si la máquina remota es un anfitrión pública en la producción, cualquier interrupción en la cadena hace que sea más difícil para los usuarios verificar la autenticidad y la identidad del servidor web. Esto podría hacer que sea más fácil de llevar a cabo ataques man-in-the-middle contra el host remoto.

  Solución: Generar o comprar certificados adecuados para el servicio.

  Vulnerabilidad: Detección de versión del Protocolo SSL 2 y 3

  Descripción: El servicio remoto acepta conexiones cifradas mediante SSL 2.0 y / o SSL 3.0, que al parecer sufren de varios defectos criptográficas. Un atacante podría ser capaz de aprovechar estas cuestiones para realizar ataques man-in-the-middle o descifrar las comunicaciones entre el servicio afectado y los clientes.

  Solución: Es necesario verificar la documentación de la aplicación para deshabilitar SSL 2.0 y 3.0. Usar solo TLS 1.0 o superior.

  Vulnerabilidad: Obtención de información mDNS (Red remota)

  Descripción: El servicio remoto entiende la Bonjour (también conocido como ZeroConf o mDNS) protocolo, permite que cualquiera

pueda descubrir la información del host remoto como su tipo de sistema operativo y versión exacta, su nombre de host, y la lista de servicios que se está ejecutando.

Solución: Si se desea, filtrar el tráfico entrante al puerto UDP 5353

- **Servidor correo.tungurahua.gob.ec**

  Vulnerabilidad: Certificado SSL no es confiable

  Descripción: Certificado X.509 del servidor no tiene una firma de una autoridad de certificación pública conocida. Si la máquina remota es un anfitrión pública en la producción, cualquier interrupción en la cadena hace que sea más difícil para los usuarios verificar la autenticidad y la identidad del servidor web. Esto podría hacer que sea más fácil de llevar a cabo ataques man-in-the-middle contra el host remoto.

  Solución: Generar o comprar certificado adecuados para el servicio.

  Vulnerabilidad: Vulnerabilidad de cifrado degradado (POODLE)

  Descripción: El host remoto se ve afectado por una vulnerabilidad MitM conocido como POODLE. La vulnerabilidad se debe a la forma en que SSL 3.0 se encarga de bytes de relleno cuando descifra mensajes cifrados usando el modo de encadenamiento de bloques de cifrado (CBC).

  Solución: Deshabilitar el soporte a las configuraciones SSL 3 en el lado del cliente y el servidor, es la solución más viable.

  Vulnerabilidad: Detección de versión del Protocolo SSL 2 y 3

  Descripción: El servicio remoto acepta conexiones cifradas mediante SSL 2.0 y / o SSL 3.0, que al parecer sufren de varios defectos criptográficas. Un atacante podría ser capaz de aprovechar estas cuestiones para realizar ataques man-in-the-middle o descifrar las comunicaciones entre el servicio afectado y los clientes.

  Solución: Verificar la documentación para deshabilitar SSL 2.0 y 3.0 en el sistema y aplicación. Usar solo TLS 1.0 y posteriores

  Vulnerabilidad: Certificado SSL autofirmado

  Descripción: La cadena de certificados X.509 para este servicio no está firmado por una autoridad de certificación reconocida. Si la máquina remota es un anfitrión pública en la producción, esto anula

el uso de SSL como cualquiera podría establecer un ataque man-in-the-middle contra el host remoto.

Solución: Generar o comprar un certificado adecuado para el servicio.

- **Servidor dchgpt01.lan.tungurahua.gob.ec**

  Vulnerabilidad: Servidor DNS divulgación de información a distancia

  Descripción: El servidor DNS remoto responde a las preguntas de los dominios de terceros que no tienen el conjunto de bits recursividad. Esto puede permitir a un atacante remoto determinar qué dominios recientemente se han resuelto a través de este servidor de nombres, y por lo tanto, que las páginas se han visitado recientemente.

  Solución: Contactar al proveedor del software de DNS para solucionarlo.

  Vulnerabilidad: Certificado SSL autofirmado

  Descripción: La cadena de certificados X.509 para este servicio no está firmado por una autoridad de certificación reconocida. Si la máquina remota es un anfitrión pública en la producción, esto anula el uso de SSL como cualquiera podría establecer un ataque man-in-the-middle contra el host remoto.

  Solución: Generar o comprar un certificado adecuado para el servicio.

- **Servidor Central4760**

  Vulnerabilidad: Apache Tomcat servlet / archivos predeterminados

  Descripción: Ejemplo JSP y servlets se instalan en el servlet contenedor remoto Apache Tomcat / JSP. Estos archivos deben ser removidos ya que pueden ayudar a divulgar información a un atacante acerca de Tomcat.

  Solución: Eliminar los archivos que no sean necesarios, como medida de seguridad y para mejorar el rendimiento de Apache.

  Vulnerabilidad: SSL Versión Detección 2 y 3 del Protocolo

  Descripción: El servicio remoto acepta conexiones cifradas mediante SSL 2.0 y / o SSL 3.0, que al parecer sufren de varios defectos criptográficas. Un atacante podría ser capaz de aprovechar estas cuestiones para realizar ataques man-in-the-middle o descifrar las comunicaciones entre el servicio afectado y los clientes.

Solución: Verificar la documentación para deshabilitar SSL 2.0 y 3.0 en el sistema y aplicación. Usar solo TLS 1.0 y posteriores.

- **Servidor symantec.lan.tungurahua.gob.ec**

  Vulnerabilidad: Denegación de servicio a Apache httpd

  Descripción: Una explotación exitosa podría permitir a atacantes ejecutar código arbitrario y los intentos fallidos probablemente resultará en condiciones de denegación de servicio.

  Solución: Las actualizaciones de Apache corrigen algunos errores, por lo que actualizarlo es la mejor opción.

  Vulnerabilidad: Escritorio remoto podría permitir la ejecución remota de código

  Descripción: Existe una vulnerabilidad remota de código arbitrario en la aplicación del Protocolo de Escritorio Remoto (RDP). La vulnerabilidad se debe a la forma en que RDP accede a un objeto en la memoria que se ha inicializado incorrectamente o se ha eliminado. Un atacante remoto no autenticado podría aprovechar esta vulnerabilidad para provocar que el sistema para ejecutar código arbitrario mediante el envío de una secuencia de paquetes RDP especialmente diseñados para ello.

  Solución: Microsoft ha publicado parches para todas las versiones de windows y soluciones provisionales para la vulnerabilidad en el Boletín de seguridad de Microsoft.

  Vulnerabilidad: Apache mod_info / server-info Divulgación de Información

  Descripción: Es posible obtener una visión general de la configuración del servidor web remoto Apache mediante la solicitud de la URL "/ server-info '. Este resumen incluye información como módulos instalados, su configuración y los ajustes de tiempo de ejecución surtidos

  Solución: Desactivar o limitar el acceso a mod_info(archivo de configuración de Apache).

  Vulnerabilidad: Múltiples vulnerabilidades (Man in the Middle)

  Descripción: El servidor web remoto utiliza una versión de OpenSSL 1.0.0 o inferior. La biblioteca OpenSSL está afectada por varias vulnerabilidades.

Solución: Actualizar a OpenSSL 1.0.1g, OpenSSL 1.0.0 y OpenSSL 0.9.8

Vulnerabilidad: Detección de versión PHP no compatible

Descripción: De acuerdo con su versión, la instalación de PHP en el host remoto ya no es compatible, lo que implica que no hay nuevos parches de seguridad para el producto por el proveedor. Como resultado, es probable que contenga vulnerabilidades de seguridad.

Solución: Actualizar la versión de PHP.

Vulnerabilidad: Apache 2.2 <2.2.28 Múltiples vulnerabilidades

Descripción: De acuerdo con la versión de Apache 2.2 instalado en el host remoto, es anterior a la 2.2.28.

Solución: Actualizar la versión de Apache.

Vulnerabilidad: MySQL Múltiples vulnerabilidades no especificadas (Windows)

Descripción: Es posible obtener una visión general de la configuración del servidor web remoto. Este resumen incluye información como módulos instalados, su configuración y los ajustes de tiempo de ejecución surtidos

Solución: Eliminar los archivos que no son necesarios.

- **Servidor mapas.tungurahua.gob.ec**

Vulnerabilidad: Apache httpd Métodos HTTP TRACE / TRACK permitidos

Descripción: El servidor web remoto es compatible con los métodos TRACE / TRACK. Son métodos HTTP que se utilizan para las conexiones del servidor de depuración web. El HTTP Trace es un método de solicitud (request method) usado para debuguear con echo's al usuario back-input-back (vuelta-entrada-vuelta)

Solución: Desactivar estos métodos, modificando el archivo de configuración de Apache

Vulnerabilidad: Certificado SSL autofirmado

Descripción: La cadena de certificados X.509 para este servicio no está firmado por una autoridad de certificación reconocida. Si la máquina remota es un anfitrión pública en la producción, esto anula

el uso de SSL como cualquiera podría establecer un ataque man-in-the-middle contra el host remoto.

Solución: Generar o comprar un certificado adecuado para el servicio.

- **Servidor srvap01**

  Vulnerabilidad: SSL Versión Detección 2 y 3 del Protocolo

  Descripción: El servicio remoto acepta conexiones cifradas mediante SSL 2.0 y / o SSL 3.0, que al parecer sufren de varios defectos criptográficas. Un atacante podría ser capaz de aprovechar estas cuestiones para realizar ataques man-in-the-middle o descifrar las comunicaciones entre el servicio afectado y los clientes.

  Solución: Verificar la documentación para deshabilitar SSL 2.0 y 3.0 en el sistema y aplicación. Usar solo TLS 1.0 y posteriores.

  Vulnerabilidad: Vulnerabilidad de cifrado degradado (POODLE)

  Descripción: El host remoto se ve afectado por una vulnerabilidad MitM conocido como POODLE. La vulnerabilidad se debe a la forma en que SSL 3.0 se encarga de bytes de relleno cuando descifra mensajes cifrados usando el modo de encadenamiento de bloques de cifrado (CBC).

  Solución: Deshabilitar el soporte a las configuraciones SSL 3 en el lado del cliente y el servidor, es la solución más viable.

  Vulnerabilidad: Apache httpd Métodos HTTP TRACE / TRACK permitidos

  Descripción: El servidor web remoto es compatible con los métodos TRACE / TRACK. Son métodos HTTP que se utilizan para las conexiones del servidor de depuración web.

  Solución: Desactivar estos métodos, modificando el archivo de configuración de Apache

- **Servidor rrnn.tungurahua.gob.ec**

  Vulnerabilidad: Vulnerabilidades de cadena de formato remoto múltiple

  Descripción: El anfitrión se está ejecutando el servicio statd y es propenso a múltiples vulnerabilidades de cadena de formato a distancia. Una explotación exitosa podría permitir a atacantes

ejecutar código arbitrario con los privilegios del proceso rpc.statd, normalmente root.

Solución: Actualizar a la última versión de nfs-utils.

Vulnerabilidad: Apache httpd Métodos HTTP TRACE / TRACK permitidos

Descripción: El servidor web remoto es compatible con los métodos TRACE / TRACK. Son métodos HTTP que se utilizan para las conexiones del servidor de depuración web.

Solución: Desactivar estos métodos, modificando el archivo de configuración de Apache

Vulnerabilidad: Certificado SSL no es confiable

Descripción: Certificado X.509 del servidor no tiene una firma de una autoridad de certificación pública conocida. Si la máquina remota es un anfitrión pública en la producción, cualquier interrupción en la cadena hace que sea más difícil para los usuarios verificar la autenticidad y la identidad del servidor web. Esto podría hacer que sea más fácil de llevar a cabo ataques man-in-the-middle contra el host remoto.

Solución: Generar o comprar un certificado adecuado para el servicio.

Vulnerabilidad: Detección de versión del Protocolo SSL 2 y 3

Descripción: El servicio remoto acepta conexiones cifradas mediante SSL 2.0 y / o SSL 3.0, que al parecer sufren de varios defectos criptográficas. Un atacante podría ser capaz de aprovechar estas cuestiones para realizar ataques man-in-the-middle o descifrar las comunicaciones entre el servicio afectado y los clientes

Solución: Verificar la documentación para deshabilitar SSL 2.0 y 3.0 en el sistema y aplicación. Usar solo TLS 1.0 y posteriores.

- **Servidor bdd_nr**

Vulnerabilidad: Apache httpd Métodos HTTP TRACE / TRACK permitidos

Descripción: El servidor web remoto es compatible con los métodos TRACE / TRACK. Son métodos HTTP que se utilizan para las conexiones del servidor de depuración web.

Solución: Desactivar estos métodos, modificando el archivo de configuración de Apache

Vulnerabilidad: Certificado SSL no es confiable

Descripción: Certificado X.509 del servidor no tiene una firma de una autoridad de certificación pública conocida. Si la máquina remota es un anfitrión pública en la producción, cualquier interrupción en la cadena hace que sea más difícil para los usuarios verificar la autenticidad y la identidad del servidor web. Esto podría hacer que sea más fácil de llevar a cabo ataques man-in-the-middle contra el host remoto.

Solución: Generar o comprar un certificado adecuado para el servicio.

- **Servidor bdd_r**

  Vulnerabilidad: Directorios Web explorables

  Descripción: Se identificaron directorios de este servidor web que son navegables.

  Solución: Asegurarse que los directorios navegables no expongan información confidencial o den acceso a los recursos sensibles. Además, utilizar las restricciones de acceso o desactivar la indexación de directorios.

  Vulnerabilidad: Apache httpd Métodos HTTP TRACE / TRACK permitidos

  Descripción: El servidor web remoto es compatible con los métodos TRACE / TRACK. Son métodos HTTP que se utilizan para las conexiones del servidor de depuración web.

  Solución: Desactivar estos métodos, modificando el archivo de configuración de Apache

  Vulnerabilidad: PHP expose_php Divulgación de Información

  Descripción: Al instalar El PHP en el servidor remoto está configurado de una manera que permite la divulgación de información potencialmente sensible a un atacante a través de una URL especial. Un enlace desencadena un huevo de Pascua integrado en el propio PHP.

  Solución: En el archivo de configuración de PHP, php.ini, establezca el valor de 'expose_php "a" Off "para desactivar este comportamien-

to. Reiniciar el demonio del servidor web para poner en práctica el cambio.

Vulnerabilidad: Aplicación Web potencialmente vulnerable a Clickjacking

Descripción: El servidor web remoto no establece un encabezado de respuesta X-Frame-Options en todas las respuestas de contenido. Esto podría exponer el sitio a un clickjacking. Un atacante puede engañar a un usuario para que haga clic en un área de la página vulnerable que es diferente a lo que el usuario percibe que la página sea. Esto puede dar lugar a un usuario realizar transacciones fraudulentas o maliciosas.

Solución: Devolver el Opciones X-Frame cabecera HTTP con la respuesta de la página. Esto evita que el contenido de la página sea prestado por otro sitio al usar las etiquetas HTML frame o iframe

- **Servidor ftp.tungurahua.gob.ec**

  Vulnerabilidad: Nessus SYN scanner

  Descripción: Este plugin es un escáner de puertos SYN 'semi-abierta'. Será bastante rápido, incluso frente a un objetivo con cortafuegos. Pueden causar problemas a los servidores de seguridad menos robustos y también dejan sin cerrar las conexiones en el destino remoto, si se carga la red.

  Solución: Proteja su objetivo con un filtro IP.

- **Servidor serwebcentos**

  Vulnerabilidad: Apache httpd Métodos HTTP TRACE / TRACK permitidos

  Descripción: El servidor web remoto es compatible con los métodos TRACE / TRACK. Son métodos HTTP que se utilizan para las conexiones del servidor de depuración web.

  Solución: Desactivar estos métodos, modificando el archivo de configuración de Apache

- **Servidor HGPT-SERVERPRUE**

  Vulnerabilidad: Base de datos Oracle no compatible

  Descripción: De acuerdo con su versión, la instalación de la base de datos de Oracle en el host remoto ya no es compatible. La falta

de apoyo implica que no hay nuevos parches de seguridad para el producto por el proveedor. Como resultado, es probable que contenga vulnerabilidades de seguridad.

Solución: Actualizar Oracle a una versión más reciente.

Vulnerabilidad: Detección de versión PHP no compatible

Descripción: De acuerdo con su versión, la instalación de PHP en el host remoto ya no es compatible, lo que implica que no hay nuevos parches de seguridad para el producto por el proveedor. Como resultado, es probable que contenga vulnerabilidades de seguridad.

Solución: Actualizar la versión de PHP.

Vulnerabilidad: Apache 2.2 <2.2.28 Múltiples vulnerabilidades

Descripción: De acuerdo con la versión de Apache 2.2 instalado en el host remoto, es anterior a la 2.2.28. Está, por lo tanto, afectada por las vulnerabilidades: CVE-2014-0.118, CVE-2014-0226 y CVE-2.014-0231. Tenga en cuenta que Nessus no ha probado para estas cuestiones, sino que se ha basado únicamente en el número de versión de auto-reporte de la aplicación.

Solución: Actualizar la versión de PHP.

Vulnerabilidad: Escritorio remoto podría permitir la ejecución remota de código

Descripción: Existe una vulnerabilidad remota de código arbitrario en la aplicación del Protocolo de Escritorio Remoto (RDP). La vulnerabilidad se debe a la forma en que RDP acceso a un objeto en la memoria que se ha inicializado incorrectamente o se ha eliminado. Un atacante remoto no autenticado podría aprovechar esta vulnerabilidad para provocar que el sistema para ejecutar código arbitrario mediante el envío de una secuencia de paquetes RDP especialmente diseñados para ello.

Solución: Microsoft ha publicado parches para todas las versiones de windows y soluciones provisionales para la vulnerabilidad en el Boletín de seguridad de Microsoft.

Vulnerabilidad: Oracle TNS Listener Envenenamiento remoto

Descripción: Vulnerabilidad conocida como TNS Listener Ataque veneno. La escucha de Oracle TNS remoto permite el registro de

servicios de un host remoto. Un atacante puede aprovechar este problema para desviar los datos de un servidor de base legítima o cliente a un sistema atacante-especificado. Ataques exitosos permitirán al atacante manipular las instancias de base de datos, lo que podría facilitar man-in-the-middle, secuestro sesión, o ataques de denegación de servicio en el servidor de base de datos legítimo.

Solución: Seguir las recomendaciones de soporte de oracle para solucionar esta vulnerabilidad.

Vulnerabilidad: Apache httpd Métodos HTTP TRACE / TRACK permitidos

Descripción: El servidor web remoto es compatible con los métodos TRACE / TRACK. Son métodos HTTP que se utilizan para las conexiones del servidor de depuración web.

Solución: Desactivar estos métodos, modificando el archivo de configuración de Apache

Vulnerabilidad: Servidor Microsoft Windows Remote Desktop Protocol con debilidad Man-in-the-Middle

Descripción: La versión remota del Escritorio remoto (Terminal Service) es vulnerable a un ataque man-in-the-middle. El cliente RDP no hace ningún esfuerzo para validar la identidad del servidor al configurar el cifrado. Un atacante con la capacidad para interceptar el tráfico desde el servidor RDP puede establecer el cifrado con el cliente y el servidor sin ser detectado. Un ataque MiTM de esta naturaleza permitiría al atacante obtener información sensible transmitida, incluyendo las credenciales de autenticación.

Solución: Forzar el uso de SSL y/o seleccionar las conexiones 'Permitir sólo desde equipos que ejecuten escritorio remoto con configuración de nivel de autenticación de red.

Seguridad Inalámbrica

Se realiza pruebas en búsqueda de configuraciones por defecto en dispositivos inalámbricos.

- **Explotación de vulnerabilidades**

  Para el posterior análisis forense, es necesario explotar vulnerabilidades con el objetivo de darles seguimiento.

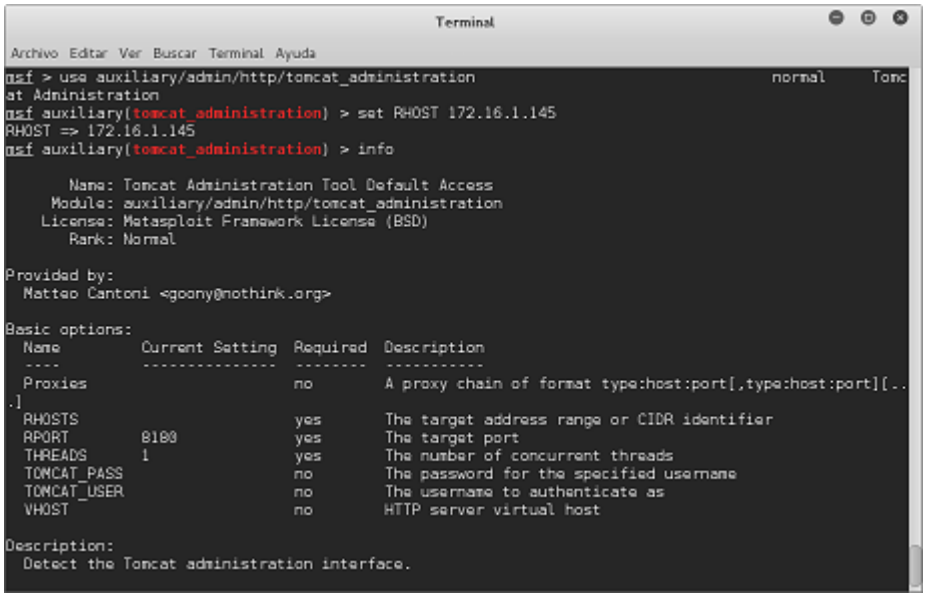

Figura 4.14: Explotación de vulnerabilidad de Apache con Metasploit

Se ha encontrado vulnerabilidades graves, las cuales permiten acceder, en este caso al servidor de apache sin la necesidad de utilizar una herramienta de hackeo, ya que al realizar el análisis de vulnerabilidades con Nessus ya da el error y la manera de acceder al servidor.

Explotando la vulnerabilidad encontrada con metasploit se obtendrá

En la figura 4.14 muestra la explotación de la vulnerabilidad encontrada en apache en el servidor 172.16.1.145 con metasploit.

Una vez explotado correctamente la vulnerabilidad se tendrá acceso al servidor de apache, en este caso como administrador por lo que se podrá realizar los cambios que se desee dentro de apache tomcat.

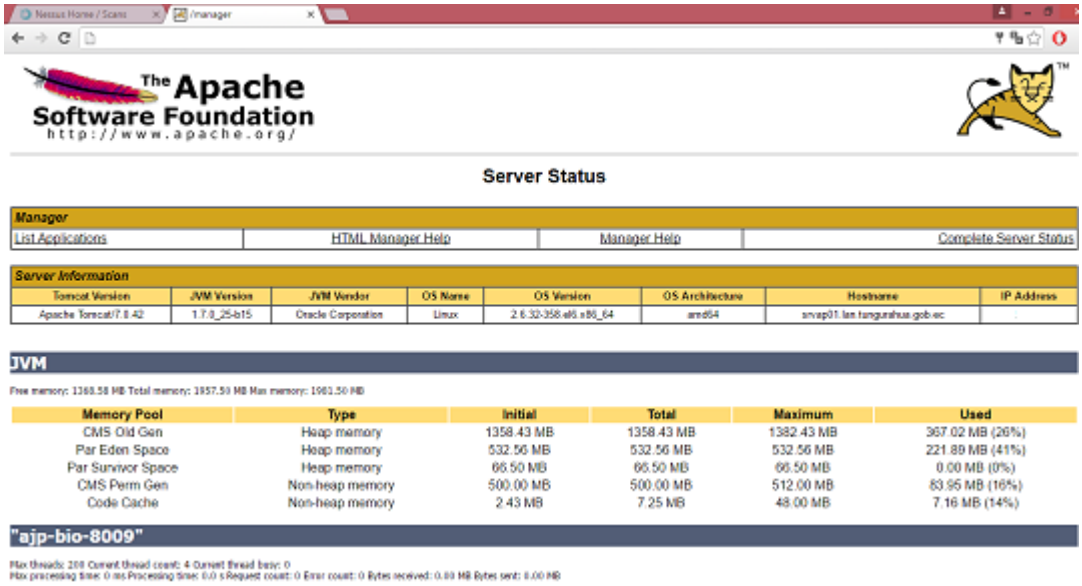

Figura 4.15: Ingreso al servidor de apache tomcat

La figura 4.15 muestra el ingreso exitoso a apache luego de explorar la vulnerabilidad crítica encontrada en el servidor 172.16.1.145.

Explotando esta vulnerabilidad se pudo acceder al servidor de Apache.

- **Herramientas adecuadas para un análisis forense**

  Cuando ocurre un incidente de seguridad, dependiendo de la gravedad del suceso, será necesario contar con las herramientas necesarias para el análisis. En el caso de las instituciones públicas, el gobierno promueve el uso de software libre, por lo cual se dará prioridad a este tipo de software para los análisis que sean necesarios.

Herramienta	Arquitectura	Características
CAINE 7 (Computer Aide Investigation Environment)	disponible en 32 bits y 64 bits i686 and x86_64	• Puede utilizarse como LiveCD e inclusive se puede ejecutar arrancando el sistema desde un pendrive • Compilación semiautomática para el informe final • Entorno interoperable que soporta el investigador digital durante las cuatro fases de la investigación digitales • Bloquea todos los dispositivos de bloque (por ejemplo, / dev / sda), en el modo de sólo lectura. Se puede utilizar una herramienta con un tipo llamado Bloque ON / OFF presente en el escritorio de Caine
Kali Linux	disponible en 32 bits y 64 bits	• Puede ser usado desde un Live CD, live-usb. • Preinstalados más de 600 programa, desarrollado en un entorno seguro. • Sirve para poner a trabajar las herramientas de software libre más populares en materia forense de forma rápida y sencilla • Es muy popular debido a que Kali está ampliamente disponible y es fácil de conseguir. • El disco duro no se utiliza en absoluto.
SIFT (SANS Investigative Forensic Toolkit)	Basado en Ubuntu LTS 14,04	• Tienen en cuenta operaciones como montado de imágenes, creación de líneas de tiempo, recopilación de memoria volátil o efímera y el uso de herramientas como Sleuthkit o Autopsy. • Es utilizado para algunos cursos, por lo cual hay muchas investigaciones desarrolladas por estudiantes en base a su uso.
DEFT Zero	Basada en Ubuntu 04/14/02 LTS soporta plataformas de 32 y 64 bits.	• Es utilizada en cursos sobre ciencias forenses digitales en varias universidades del mundo y también utilizada por las instituciones estatales jurídicas en diversos departamentos especializados. • Linux-Zero en vivo (modo de interfaz gráfica, memoria RAM de precarga) Linux-Zero en vivo (modo de interfaz gráfica, memoria RAM de precarga) • La política de protección de escritura ha sido ejecutada, a fin de evitar la manipulación accidental de dispositivos
Bugtraq	Basada en el kernel 3.2 y 3.4 disponible en 32 bits y 64 bits	• Disponible en 11 idiomas diferentes • Contiene más de 200 Herramientas Android y Linux (PRO) para pentesting y forense para smartphone o Tablet
Pentoo	Kernel 4.0.8 disponible en 32 bits y 64 bits	• Es posible instalarlo y usarlo en modo Live CD o USB. • Software experimental
BackBox Linux 4.4	kernel Linux 3.16	• Ha sido diseñado con el objetivo de conseguir el máximo rendimiento y mínimo consumo de recursos • Ofrece estabilidad y la velocidad
Parrot Security OS	Basada en Debian kernel Linux 4.3	• Utilizando los repositorios de Kali se puede hacer uso de la mayoría de sus aplicaciones, también posee repositorios propios para aplicaciones personalizadas. • sistema de protección contra escritura
Fedora Security Spin: Linux Hacker Distro	Disponible en 32 bits y 64 bits	• Puede ser utilizado para la enseñanza de metodologías de seguridad. • El propósito de este Linux es apoyar a los estudiantes y profesores con los servidores y servicios basados en Linux

Tabla 4.23: Herramientas

La tabla 4.23 muestra las herramientas más utilizadas en la actualidad para auditoría informática y análisis forense, con sus principales características

Revisión

Cada cierto tiempo es necesario probar que funcione correctamente el hardware y software, especialmente después de alguna actualización, parche o nueva configuración.

El firewall debe ser revisado y actualizado constantemente para evitar problemas de nuevas amenazas.

Se debe tener en cuenta que pueden haber elementos instalados sin que el administrador tenga conocimiento de esto, ya sean instalados por un compañero del área de sistemas o por un usuario.

Las políticas y procedimientos de la institución deben ser revisadas por lo menos cada año para mantenerlas al día de acuerdo a los avances tecnológicos y cambios institucionales.

Análisis Forense Digital Activo

Para la mayoría de las organizaciones sería una pérdida detener sus operaciones mientras se realiza un análisis forense por lo cual investigadores han buscado una alternativa a esto.

Esta opción se denomina análisis en caliente o análisis en tiempo real, es el análisis que se lleva a cabo de un sistema que se presume ha sufrido o está sufriendo un incidente de seguridad. Consiste en confirmar si existen actividades sospechosas y de ser el caso recolectar evidencia mediante procedimientos detallados para responder ante estos incidentes. La experiencia del profesional a cargo de la seguridad es un factor indispensable, esto le permitirá distinguir un ataque informático de un simple problema técnico [26].

Este análisis posee 4 subfases:

1. Confirmación y respuesta al incidente
2. Investigación
3. Reconstrucción y limitación del incidente
4. Finalizar la Investigación

Confirmación y Respuesta al incidente

La detección de actividades sospechosas está definida por alertas de medios digitales como firewalls e IDS.

- **Monitoreo de la actividad y activación del Protocolo de respuesta de incidentes**

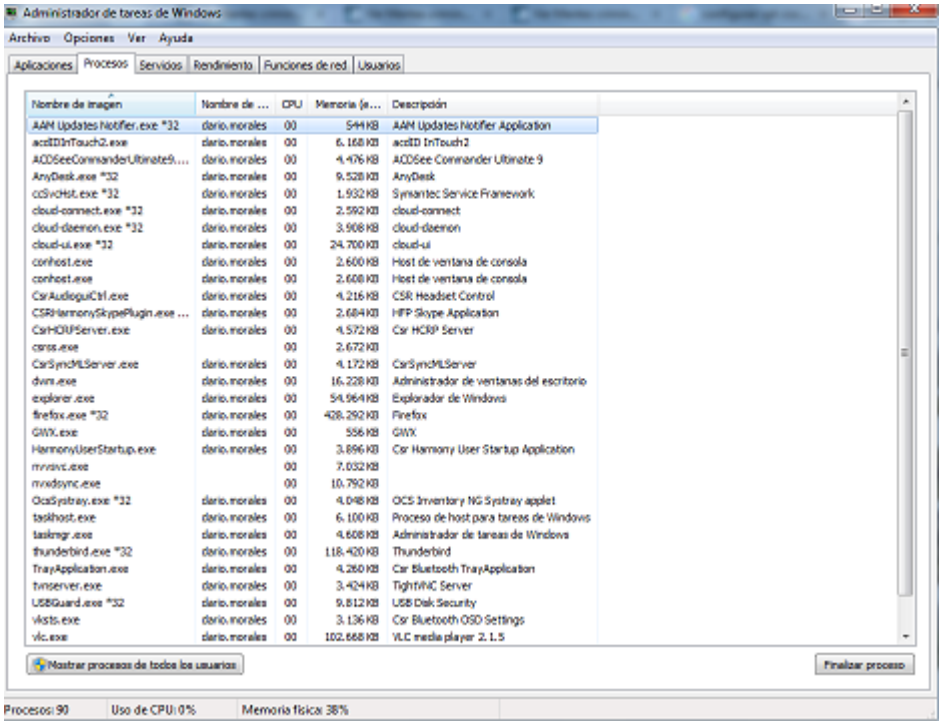

Figura 4.16: Procesos activos en equipo victima

La detección de intrusiones en su mayor parte está definida por las alertas del firewall e IDS. Para determinar si es necesario activar las alertas para que el equipo de respuesta de incidentes entre en acción, es conveniente que se realice un monitoreo de la actividad sospechosa.

En el análisis forense digital activo, Si la amenaza detectada es grave será necesario activar el protocolo de respuesta de incidentes, se debe empezar con los procedimientos adecuados para el análisis de incidentes en tiempo real.

Parte del monitoreo para determinar si determinada actividad es en realidad un ataque, es revisar y sacar imágenes de:

- Contenidos de la caché
- Contenidos de la memoria
- Tabla de enrutamiento
- Estado de los procesos en ejecución
- Contenido del sistema de archivos y de los discos duros
- Contenido de los dispositivos de almacenamiento conectados al equipo supuestamente atacado.
- Fecha y Hora

La figura 4.16 muestra una de las imágenes que se debe sacar al monitorizar alguna actividad sospechosa con el objetivo de determinar si es un ataque informático o no.

- **Controlar y contener el ambiente del incidente**

  La respuesta al incidente es seguir los procesos previamente desarrollados para controlar y contener el ambiente afectado. Poniendo énfasis en definir el alcance del incidente para evitar la propagación a otras áreas tecnológicas minimizando el impacto a la institución. Cabe resaltar que las acciones a seguir dependen del tipo de ataque del que seamos víctimas y la experiencia del profesional que esté a cargo en esta situación. Para esto entre los datos que se necesita recabar están:

  - Procesos activos
  - Conexiones de la red
  - Puertos TCP/UDP abiertos y aplicaciones asociadas a "la escucha".
  - Usuarios conectados remota y localmente

  Al escanear vulnerabilidades en cualquier equipo conectado a la red, dependiendo del antivirus y si está actualizado, podrá detectar que está siendo analizado como muestra en la siguiente figura.

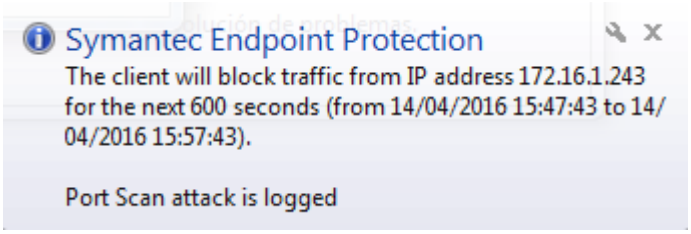

Figura 4.17: Detección de análisis a la PC por el antivirus

La figura 4.17 muestra la detección del antivirus de una actividad sospechosa.

El antivirus detecta el escaneo y lo bloquea, indicando la IP de la máquina que está intentando acceder.

En el caso del servidor que explotamos la vulnerabilidad de Apache Tomcat se puede revisar el log que está activado, lo que nos dará datos de la intrusión, como fecha, hora, IP de la que se ha accedido y a que características. En la figura 4.18 se muestra los detalles del log de apache tomcat con la fecha de la intrusión.

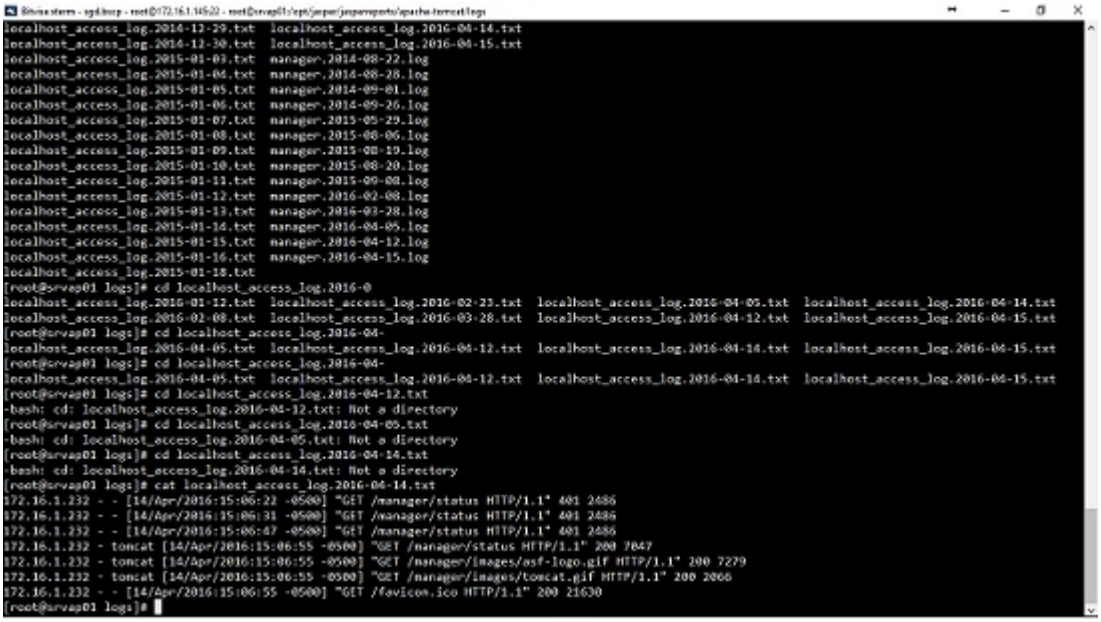

Figura 4.18: Acceso a Apache Tomcat

Investigación

Los procedimientos adecuados para el análisis forense activo del incidente en progreso se detallan en esta fase.

- **Identificar la evidencia digital**

  En este punto se realiza lo necesario para identificar la evidencia digital del ambiente afectado. Es indispensable tener en cuenta la documentación creada por el equipo del área de sistemas con el fin de conocer la configuración, sistemas operativos, registros, etc. de los equipos afectados.

- **Adquirir la evidencia en tiempo real**

  Para adquirir la evidencia en tiempo real puede ser necesario el uso de herramientas especialmente creadas para este fin.

- **Analizar la evidencia digital**

  Una vez obtenida la evidencia es necesario determinar si es tenemos la cantidad necesaria para continuar con la investigación, de ser necesario se plantea una hipótesis de lo ocurrido y se continua con la siguiente subfase.

  Siguiendo con el análisis del escaneo de un equipo de la red.

  El mensaje de advertencia del antivirus nos da la IP de la máquina que está intentando acceder al equipo victima al igual que en el servidor, en apache tomcat nos da la IP de la maquina atacante. Parte del análisis Forense Pro

activo es documentar los equipos que corresponden a la red, con su respectiva IP, ubicación física y los datos del usuario encargado del equipo. Mediante esta investigación podemos encontrar la ubicación del equipo atacante y posteriormente el posible culpable de realizar la intrusión.

Reconstrucción y limitación del Incidente

Luego de obtener la evidencia digital, el siguiente paso es reconstruir el incidente

- **Reconstruir el incidente**

  Dentro de esta fase se procura aclarar lo ocurrido realizando una reconstrucción del incidente de seguridad. Para confirmar la hipótesis de la investigación se utiliza la evidencia recolectada previamente.

- **Limitación del incidente**

  Luego de confirmar la hipótesis a continuación se mitiga la amenaza para calcular el daño causado y de ser posible identificar a los responsables del ataque.

  En el caso del equipo victima la limitación del incidente de seguridad es realizado por el antivirus, el mismo que da detalles del ataque que se intentó realizar.

  Con la fecha y hora del ataque se puede averiguar el usuario que ocupó el equipo atacante en ese momento y dependiendo de las circunstancias se puede determinar si el usuario logueado es la misma persona que realizó el ataque.

Finalizar la Investigación

Para finalizar con la investigación es necesario presentar los resultados obtenidos. Estos resultados deben estar formalmente documentados de acuerdo a las políticas de la institución y siguiendo los lineamientos necesarios para que sean avaladas ante un tribunal, de ser necesario.

Los resultados de la investigación forense activa deben incluir como mínimo:

- Proceso realizado por el equipo a cargo del análisis forense.
- Descripción del incidente de la manera más detallada posible.
- Impacto estimado que ha sufrido la institución.
- Lecciones aprendidas que serán de utilidad para evitar futuros ataques.
- Conclusiones

En caso de haber incidentes de seguridad se debe llenar el formulario de incidentes de seguridad, con la finalidad de llevar un registro de lo ocurrido con las respectivas lecciones aprendidas. (El formato del formulario se encuentra en anexos).

El formulario de ejemplo del incidente de seguridad (intento de intrusión de un equipo a otro de la misma red) esta detallado en anexos.

Dependiendo de la situación puede ser necesario continuar con un análisis reactivo.

Análisis Forense Digital Reactivo

Este análisis consta de fases genéricas (Basándose en la metodología CP4DF "Codes of Practises for digital forensics" , DFRWS y la metodología forense del Departamento de Justicia de los Estados Unidos).

Las principales etapas de un análisis reactivo son:

- Aseguramiento de la escena
- Identificación y Preservación
- Recolección y Análisis
- Finalización del Análisis y Presentación de Resultados

Cuando se confirma el incidente de seguridad y es necesario, se realiza un proceso post-mortem, que es el análisis del equipo dedicado específicamente para fines forenses, para examinar discos duros, datos o cualquier tipo de información recabada de un sistema que ha sufrido un incidente [26].

En muchos casos luego de haber realizado un análisis activo, se puede llegar a la conclusión que es necesario un análisis más profundo para mitigar el incidente de seguridad. Basándose en los resultados del análisis activo se puede minimizar el impacto ya que se procedería a un análisis reactivo enfocado directamente al problema.

El modelo de análisis Forense Digital Reactivo se puede dividir en varias subfases al igual que el análisis Digital Activo

Confirmación y Respuesta del Incidente de Seguridad

Antes de empezar cualquier procedimiento se debe estar seguro que ha ocurrido un incidente de seguridad para activar los protocolos necesarios para responder ante el ataque.

De ser necesario el equipo designado para realizar el análisis forense activará los procedimientos necesarios para la contención y mitigación del incidente de seguridad.

Lo más importante de esta fase es evitar la propagación del incidente a otras instancias de la infraestructura tecnológica, de esta manera minimizar el impacto.

Confirmado el incidente, lo siguiente es activar los protocolos para empezar con la investigación forense. De la activación de estos protocolos, deben estar notificados la prefectura y el área legal de la institución.

Investigación Física

Dependiendo del incidente, puede ser necesario una investigación que implique una escena física donde haya ocurrido el incidente.

Los procedimientos para ésta investigación son:

- **Aseguramiento de la escena**

  El aseguramiento de la escena es esencial para que la evidencia que exista no sea alterada

  Fotografiar el equipo sin desmontar y después de ser desmotado con el número de serie visible, la configuración del equipos.

  Anotar todos los pasos

  Imágenes del disco: copias o clones idénticos del contenido y estructura en un disco completamente nuevo (para garantizar que esté exactamente igual al original).

  Etiquetar el disco duro original y las 2 cintas (etiqueta, iniciales analista, acompañante, MD5): para mantener una identificación de los componentes físicos.

  Fotografiar el disco duro original y las 2 cintas juntas (se tiene que ver la fecha, hora y las etiquetas): para corroborar la existencia de las copias y originales entregados al custodio.

  Guardar el disco duro original y las cintas en un lugar seguro y bajo llave.

  Entregar las llaves al Jefe del área de sistemas o Autoridades.

  Desde este momento, cuando sea necesario, y bajo la supervisión del testigo adecuado, podrá extraer la copia necesaria para llevar a cabo los análisis para la obtención de las pruebas digitales necesarias.

  Una opción muy recomendable es seguir todos estos pasos con un testigo que dé fé que se han seguido todas las indicaciones para realizar las copias y no se ha realizado ninguna otra acción sobre los sistemas o los datos más que los estrictamente necesarios para realizar las copias imagen o clon de los discos duros[26].

- **Identificación y Preservación**

  De la lista de elementos extraídos después del aseguramiento de la escena se debe determinar si el elemento es relevante o no para la investigación y clasificarlo de acuerdo a eso para el posterior análisis. En caso de que se encuentre nueva evidencia lo primero que se debe hacer es detener la investigación e informar del hallazgo a la persona correspondiente para recibir nuevas instrucciones.

  Cada procedimiento que se realice con la evidencia debe ser documentado en una lista de "Datos Relevantes".

- **Recolección y análisis**

  Es una parte critica del análisis ya que si se realiza mal, todo el análisis e investigación posterior no serviría de nada, seria inválido pues la información extraída que pensaríamos que es del origen, no lo sería realmente.

- **Finalización del Análisis y Presentación de Resultados**

  Una vez realizado todos los análisis es necesario restaurar completamente los servicios que fueron comprometidos para que la institución pueda seguir con su funcionamiento normal.

  La evidencia que no ha sido útil en la investigación debe ser eliminada.

  Los resultados de la investigación deben estar documentados de acuerdo a las políticas creadas en el análisis proactivo.

  Los datos que deben tener los resultados son los siguientes:

  - Procesos realizados
  - Descripción del incidente
  - Impacto estimado
  - Lecciones aprendidas
  - Conclusión de la investigación

  El análisis Forense Reactivo se usará solo en casos extremos, es decir si los equipos han sido dañados o se ha perdido información, lo que requeriría seguir los procedimientos descritos anteriormente.

  El Honorable Gobierno Provincial de Tungurahua no ha sufrido ataques en los que se hayan perdido datos o dañado los equipos, por lo que no ha sido necesario el uso de este análisis. Por precaución a lo que pueda ocurrir en un

futuro, se deja desarrollado el análisis forense reactivo, con los procedimientos listos para usarse en caso de ser necesario.

Como una guía se desarrolló también un análisis de las herramientas más utilizadas en la actualidad, de tal manera que el profesional encargado de esté análisis puede hacer uso, si lo considera apropiado.

CAPÍTULO 5

Conclusiones y Recomendaciones

Con base en los resultados obtenidos se definen las siguientes conclusiones y recomendaciones conformes a los objetivos de estudio.

5.1. Conclusiones

- El modelo de análisis forense informático fue desarrollado de acuerdo a las necesidades del Honorable Gobierno Provincial de Tungurahua y basándose en metodologías que aplican los estándares internacionales en cuanto a seguridad informática y recolección de evidencia digital.
- El departamento de Sistemas del Honorable Gobierno Provincial de Tungurahua fue creado en Agosto del 2014, motivo por el cual a pesar de tener algunas políticas definidas verbalmente, no existía la documentación que las respalde, es por ello que se crearon y documentaron políticas y procedimientos que ayudan a mantener la seguridad en la institución y forman parte del análisis forense pro activo (primera fase del modelo diseñado para la institución).
- El hacking ético realizado en la institución ha sido de gran ayuda para identificar las vulnerabilidades tecnológicas y buscar soluciones apropiadas a las mismas, de esta manera se ha aplicado el análisis forense proactivo con mayor efectividad.
- Dentro del diseño del modelo de análisis forense de detalló conceptos importantes relacionados al tema, que son trascendentes para la aplicación del mismo y que sirven como base para una seguridad apropiada dentro de la institución.
- Las Herramientas para el análisis forense son muchas, en este proyecto se mencionan las más conocidas y que son software libre, el uso de las mismas

dependerá del personal encargado del análisis forense y de acuerdo a las necesidades, dependiendo de la fase de análisis en la cual se encuentre.

5.2. Recomendaciones

- Se recomienda al departamento de Sistemas del Honorable Gobierno Provincial de Tungurahua cumplir con las políticas y procedimientos de seguridad, creadas para la fase de análisis forense pro activo y su respectiva revisión de acuerdo a lo especificado en las mismas.

- Para un análisis forense proactivo más efectivo es recomendable que el departamento de Sistemas del Honorable Gobierno Provincial de Tungurahua implemente un Sistema de Prevención de Intrusos (IPS) en la institución, para bloquear inmediatamente las intrusiones.

- Para la aplicación del análisis forense activo es recomendable que el departamento de Sistemas del Honorable Gobierno Provincial de Tungurahua implemente un Sistema de Detección de Intrusos (IDS) en la institución, para alertar sobre posibles intrusiones e iniciar con los procesos correspondientes para hacerle frente a la situación.

- Para el uso apropiado de las herramientas para el análisis forenses es recomendable que el personal del área de sistemas a cargo del mismo esté capacitado, para evitar errores al manejar la evidencia que puedan comprometerla y por efecto sea inválida para un proceso judicial o que de falsos resultados.

- Se recomienda al departamento de Sistemas del Honorable Gobierno Provincial de Tungurahua realizar capacitaciones relativas a la seguridad tecnológica para todo el personal de la institución, teniendo en mente que la mejor seguridad de cualquier institución o empresa son los empleados.

Bibliografia

[1] Serra Ruiz Jordi y Rivas Lopez Jose Luis Rifa Pous Helena. Analisis forense de sistemas informaticos, 2009.

[2] Fernandez Javier. Web de la hora sufre varios ataques informaticos, 2015.

[3] Asanza Molina M. y Berrones Miguez M. Flores Villacres E. Ciberdelincuencia un mal que afecta a la sociedad actual, 2014.

[4] Juntamay Tenezaca Ana LucÃa y Macas Carrasco Nancy Patricia. Estudio y aplicacion de procedimientos de analisis forense en servidores de bases de datos sql server y mysql, caso practico desitel-espoch, 2011.

[5] Escobar Matamoros Ronal Almeida Avilas Andres. Modelo de analisis forense para una entidad bancaria, 2014.

[6] Bohada John Avella Rocio, Gil Manuel. Realidades de un delito informatico en boyaca, 2013.

[7] Ramos Alvarez Benjamin. *Avances en criptologia y seguridad de la informacion.* Madrid, 2004.

[8] Villacis Ruiz Viviana Marcela. Auditoria forense: metodologia, herramientas y tecnicas aplicadas en un siniestro informatico de una empresa del sector comercias, 2006.

[9] Eogan Casey. Digital evidence and computer crime, 3rd ed, 2011.

[10] Acurio del Pino Santiago. Informatica forense en el ecuador, 2009.

[11] Congreso Nacional. Registro oficial 17 de abril del 2002 suplemento, 2005.

[12] iso.org. Iso/iec 27037:2012, 2012.

[13] Lopez Delgado Miguel. Informatica forense, 2007.

[14] Royer Jean-Marc. Seguridad en la informatica de empresa: riesgos, amenazas, prevencion y soluciones, 2004.

[15] Edgar Vicente jimenez Avila. Cortafuegos y seguridad en el internet, 2014.

[16] Mieres Jorge. Ataques informaticos: Debilidades de seguridad comunmente explotadas, 2009.

[17] ISO. Iso/iec 27037:2012, 2016.

[18] Carles Gervilla Rivas. Metodologia para un analisis forense, 2014.

[19] PREMIER MINISTRE Secretariat general de la defense nationale Direction centrale de la securite des systemes d information Sous-direction des operations Bureau conseil. La defensa en profundidad aplicada a los sistemas de informacion, 2004.

[20] Hector y federico Jara y Pacheco. Ethical hacking 2.0, 2012.

[21] Lopez Lopez Erika. Seguridad informatica, 2015.

[22] Offensive Security. Kali linux official documentation, 2012.

[23] Jose Arquillo Cruz. Herramienta de apoyo para el analisis forense de computadoras, 2007.

[24] De Leon Huerta Francisco Javier. Estudio de metodologias de analisis forense digital, 2009.

[25] Pinto Diego. Metodologia de analisis forense orientada a incidentes en dispositivos moviles, 2014.

[26] Fernandez Bleda Daniel. Informatica forense, teoria y practica, 2004.

Glosario

A

Ataque por denegación de servicio (DoS, Denial of service).- Los ataques por denegación de servicio envían paquetes IP o datos de tamaños o formatos atípicos que saturan los equipos de destino o los vuelven inestables y, por lo tanto, impiden el funcionamiento normal de los servicios de red que brindan.

Ataque MiTM(o intermediario).- Ataque man-in-the-middle o JANUS. Es un ataque en el que se adquiere la capacidad de leer, insertar y modificar a voluntad, los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado. El atacante debe ser capaz de observar e interceptar mensajes entre las dos víctimas.

F

Footprinting.- Consiste básicamente en la búsqueda de aquella información de carácter pública sobre la entidad objeto del estudio y que más tarde puede ser necesaria y empleada para realizar el Test de Intrusión o una Auditoria de Caja Negra

FTP.- (del inglés File Transfer Protocol, "Protocolo de transferencia de archivos") es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red, basado en la arquitectura cliente-servidor. Desde un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo.

H

Hacking ético.- Es una forma de referirse al acto de una persona usar sus conocimientos de informática y seguridad para realizar pruebas en redes y encontrar vulnerabilidades, para luego reportarlas y que se tomen medidas, sin hacer daño.

La idea es tener el conocimiento de cuales elementos dentro de una red son vulnerables y corregirlo antes que ocurra hurto de información, por ejemplo.

HTML.- (Hypertext Markup Language, "Lenguaje de marcas de hipertexto") es el lenguaje de marcado predominante para la construcción de páginas web. Es usado para describir la estructura y el contenido en forma de texto.

HTTP.-(del Hypertext Transfer Protocol, "Protocolo de transferencia de hipertexto") es un protocolo usado en cada transacción de la web. Define la sintaxis y la semántica que utilizan los elementos software de la arquitectura web (cliente, servidor, proxy) para comunicarse. Es un protocolo orientado a transacciones y sigue

el esquema petición-respuesta entre un cliente y un servidor.

I

IDS (Sistema de detección de intrusiones).- Hace referencia a un mecanismo que, sigilosamente, escucha el tráfico en la red para detectar actividades anormales o sospechosas, y de este modo, reducir el riesgo de intrusión.

Intrusión.- Acción de introducirse sin derecho en un sitio.

IP.- (Internet Protocol, "Protocolo de internet") es un número que identifica de manera lógica y jerárquica a una interfaz de un dispositivo. Conjunto de reglas que regulan la transmisión de paquetes de datos a través de Internet. El IP es la dirección numérica de una computadora en Internet de forma que cada dirección electrónica se asigna a una computadora conectada a Internet y por lo tanto es única.

M

Maltego: aplicación para la recolección de información. Obtiene la información de diferentes fuentes en internet y la presenta de diferentes modos gráficos, con ella podemos investigar empresas, personas, sitios, etc. Así mismo permite una búsqueda con múltiples criterios (IP, zona o zonas geografías del objetivo, alias de redes sociales, etc).

MD5.- (del inglés Message-Digest algorithm 5, algoritmo asimilación de mensaje 5), es un algoritmo de reducción criptográfico de 128 bits ampliamente usado. En sistemas GNU-Linux se utiliza el algoritmo MD5 para cifrar claves de los usuarios. En la base de datos se guarda el resultado MD5 de la clave que se introduce al ser registrada por un usuario, y cuando éste quiere entrar en el sistema se compara la entrada con la que guardada en la base de datos, si coinciden, el usuario será autentificado.

Metadatos.- Dato estructurado sobre la información, o sea, información sobre información, o de forma más simple, datos sobre datos. Los metadatos en el contexto de la Web, son datos que se pueden guardar, intercambiar y procesar por medio del ordenador y que están estructurados de tal forma que permiten ayudar a la identificación, descripción clasificación y localización del contenido de un documento o recurso web y que, por tanto, también sirven para su recuperación.

Metasploit.- Metasploit proviene del término "explotar". Sigue una arquitectura modular, organizada alrededor de un núcleo que estructura la aplicación y ofrece las funcionalidades básicas de exploits. Es una plataforma de pruebas de penetración que le permite la búsqueda, explotación, y validar las vulnerabilidades.

N

Nmap.- Es un escáner de redes que permite descubrir objetivos ofreciendo información sobre puertos y servicios.

OpenVas.- Sistema de Evaluación de Vulnerabilidad Abierto (OpenVAS) es un marco de diversos servicios y herramientas que ofrecen una solución completa y potente de análisis de vulnerabilidades

O

OSSTMM .- Manual de metodología abierta de pruebas de seguridad. Se trata de conocer y medir que tan bien funciona la seguridad. A partir de esta metodología se obtiene una profunda comprensión de la interrelación de las cosas (personas, procesos, sistemas y software)

P

Protocolo SSL.- Para establecer una comunicación SSL es necesario que previamente el cliente y el servidor realicen un proceso de reconocimiento mutuo y de petición de conexión que, al igual que en otros tipos de comunicaciones, recibe el nombre de apretón de manos o Handshake, que en este caso está controlado por el Potocolo SSL Handshake, que se encarga de establecer, mantener y finalizar las conexiones SSL. Durante el mismo se negocian los parámetros generales de la sesión y los particulares de cada conexión.

S

SQLmap.- Es una herramienta escrita en Python que se encarga de realizar peticiones a los parámetros de una URL que se le indiquen, ya sea mediante una petición GET, POST, en las cookies y un largo etc... Buscando que la aplicación sea vulnerable a una posible SQLi y poder explotarla.

T

Tor.- The Onion Router. Proporciona conexiones anónimas que son muy resistentes tanto al espionaje como al análisis de tráfico. Sin modificar las aplicaciones de Internet pueden utilizar estas conexiones anónimas a través de servidores proxy. Los proxies también pueden hacer que la comunicación anónima mediante la eliminación de la información de identificación del flujo de datos.

V

Vega.- Está escrito en Java. Incluye un escáner automatizado para pruebas rápidas y un proxy de interceptación de la inspección táctico. Es una plataforma de escaneo y pruebas de seguridad en las aplicaciones web. El escáner Vega encuentra XSS (cross-site scripting), la inyección de SQL, y otras vulnerabilidades.

Vulnerabilidad.- Una vulnerabilidad es un agujero de seguridad en una pieza de software, hardware o sistema operativo que proporciona un ángulo de potencial de atacar el sistema. Una vulnerabilidad puede ser tan simple como contraseñas débiles o tan complejo como desbordamientos de búfer o vulnerabilidades de inyección SQL.

W

WhatWeb.- Reconoce tecnologías Web, incluyendo los sistemas de gestión de contenidos (CMS), plataformas de blogs, bibliotecas JavaScript, servidores web, etc.

Z

Zenmap.- Es la interfaz gráfica de usuario del escáner Nmap, que es un explorador de redes y puertos orientados a las auditorias de seguridad. Es una aplicación multiplataforma (Linux, Windows, Mac OS X, BSD, etc.) libre y de código abierto que tiene como objetivo hacer Nmap fácil de usar. Las exploraciones se pueden guardar como perfiles para que sean fáciles de ejecutar repetidamente.

Anexos y Apéndices

Anexo A

Anexo A

Políticas y Procedimientos

A.1. Políticas y Procedimientos

ÁREA DE OPERACIONES

- **Activos**

  Se debe evaluar el tipo de información y clasificarla para simplificar la implementación de políticas y su aplicación.

  Categoría de sistemas y controles mínimos

  El mínimo de requerimientos es:

  - **Asignar responsabilidades por la seguridad**

    Asignar responsabilidad de la seguridad de los sistemas al Director general provincial de la dirección de Sistemas.

  - **Revisión de Controles de Seguridad**

    Se deberá realizar una auto-evaluación de los controles de seguridad en cada sistema cuando se realicen modificaciones, si no se hiciera cambios por lo menos una vez al año para asegurarse que la seguridad sigue siendo efectiva a pesar de los cambios tecnológicos.

  Administración de Hardware/ software

  La administración de hardware / software es responsabilidad del área de tecnologías del Honorable Gobierno provincial de Tungurahua.

  - **Inventario de Activos**

    La documentación de cada sistema de Información del Honorable Gobierno Provincial de Tungurahua deberá incluir un inventario de todos los activos.

- **Adquisición de activos**

  Todo Hardware y software será adquirido, instalado y gestionado a través del área de tecnología del Honorable Gobierno Provincial de Tungurahua.

- **Alteración de activos**

  Solo el personal autorizado para esta actividad podrá alterar o agregar elementos (memoria expandida, procesador actualizado, etc.).

- **Uso de herramientas de hardware / software externas**

  Sin la respectiva autorización los usuarios no deberán poseer herramientas de hardware o software que comprometan la seguridad de la institución. Estas herramientas son las que identifican vulnerabilidades, descubren la topología de red, eliminan evidencia de uso o interceptan datos en tránsito.

Uso aceptable de los bienes

Los activos de la institución no se deberán utilizar para almacenar aplicaciones que no hayan sido adquiridas por o a nombre de la institución, ni que sirvan de apoyo a cualquier empresa comercial privada.

Correo electrónico

Los sistemas de correo electrónico están destinados para ser utilizados para los propósitos de servicio de la institución. No se deberá utilizar para actividades ilícitas.

- **Administración de Operaciones**

Procedimientos Documentados de Operaciones

Los procedimientos deberán especificar las instrucciones para la ejecución de cada actividad o tarea administrativa. Estos son:

- Procesamiento y manejo de la información.
- Procedimientos de reinicio y recuperación en caso de falla de cualquier sistema.
- Instrucciones el manejo de equipos fuera de las instalaciones en casos especiales, que sean requeridos.
- Procedimientos para mantención de los sistemas
- Procesamiento para respaldos sean estos de pc o servidores.

Gestión de Cambios

Los procedimientos de seguridad deberán estar documentados y disponibles para el personal que corresponda.

Separación de Ambientes

Por seguridad es necesario separar ambientes de prueba, desarrollo y producción, ya sea física o lógicamente.

Se deberá documentar y definir reglas para el cambio de software desde desarrollo al operativo. Los usuarios no deberán tener acceso a los compiladores, editores o cualquier utilidad que se utilice para modificar aplicaciones o sistemas.

- **Gestión de TI**

  Continuidad de la institución

  Es necesario prepararse contra desastres eventuales, creando planes para que la institución se recupere y continúe con las funciones de manera normal.

  La política de continuidad del negocio debe estar aprobada por el señor Prefecto

  Responsable del plan de continuidad del negocio

  La institución deberá contar con una persona responsable de mantener actualizado las políticas de continuidad del negocio.

  Condiciones para activar el plan de Continuidad del negocio

  Se deberá notificar a quien corresponda cada vez que el plan de continuidad del negocio se ha activado y los motivos.

  Todo el personal del área en la que se ha activado el plan deberá estar al tanto de esto, para pedir su colaboración y evitar cualquier incidente en el transcurso de la aplicación del plan.

ÁREA PERSONAS

- **Responsabilidades**

  Los usuarios son responsables de cuidar y mantener seguro su usuario y contraseña, no debe ser revelada bajo ningún concepto a otra persona, a excepción que sea necesario para reparación o mantenimiento y solamente al personal que sea asignado para dicha tarea, estos deben ser debidamente identificados. Posteriormente a ello es obligación del usuario cambiar su contraseña para mayor seguridad.

Si un usuario tiene sospechas de que su usuario y contraseña está siendo utilizado por otra persona, debe cambiar su contraseña y notificar al área de tecnología de la institución.

Es responsabilidad del usuario el cuidado y buen trato de los recursos informáticos asignados.

- Derechos y Deberes de los usuarios

  Son derechos de los usuarios:

  Recibir ayuda y asesoramiento por parte del personal del área de tecnologías.

  Acceder a información relacionada con su función.

  Utilizar el correo electrónico y otros servicios, locales o de internet, siempre que tengan relación directa con la función del usuario en la institución.

  Utilizar los recursos informáticos en forma limitada para su capacitación, sin que este uso interfiera con las actividades o funciones que el usuario cumple, ni con la misión y gestión oficial de la institución.

  Utilizar los recursos informáticos de conformidad con las presentes normas.

  Son deberes de los usuarios:

  Notificar al personal del área de tecnología de los cambios de funciones dentro de la institución, con la finalidad de modificar los permisos de usuario según corresponda su nueva función.

  Contribuir al cuidado y conservación de las instalaciones, equipos y sistemas.

  Notificar al personal del área de tecnologías de las irregularidades que se detecten, sean estas de software o hardware.

  Respetar las indicaciones que reciban de los responsables del área de tecnología respecto al uso y funcionamiento de los equipos.

  El cumplimiento de las normas y condiciones establecidas en la presente normativa.

  El usuario deberá enviar una solicitud para la instalación de cualquier software adicional necesario para su trabajo. La instalación del mismo será efectuada por el personal del área de tecnologías, previa verificación de los requerimientos necesarios para su instalación. Se deberá contar con la autorización del Director general provincial de la dirección de sistemas.

- **Administración de la Seguridad**

Las responsabilidades dependerán del nivel que ocupen dentro del organigrama estructural. Y serán las siguientes:

Planeamiento de Seguridad, revisión y aplicación.

Asignación de roles y seguridad

Inspeccionar que las políticas sean revisadas por lo menos una vez al año.

Revisar y aceptar las políticas de seguridad de la institución.

Confirmar que la institución implemente y mantenga las políticas de seguridad y sus respectivos procedimientos de control.

- **POLÍTICAS de RESTRICCIÓN DE LOS RECURSOS INFORMÁTICOS**

Usos Indebidos

Modificar o reubicar equipos de computación, software, información, periféricos y/o cualquier otro medio de soporte de información, sin la debida autorización del área de Tecnologías.

Modificar, alterar y/o borrar, sin la autorización correspondientes, la información o las configuraciones de sistemas operativos o aplicaciones instalados por el personal autorizado.

Vulnerar o eludir las verificaciones de identidad u otros sistemas de seguridad; Instalar o conectar cualquier equipamiento no autorizado.

Acceder al código fuente de cualquier software sin autorización explícita del autor con la finalidad de modificarlo.

Alterar, falsificar o de alguna otra forma usar de manera fraudulenta los archivos, permisos, documentos de identificación, u otros documentos o propiedades.

Intentar obtener otros derechos o accesos distintos a aquellos que les hayan sido asignados. Intentar acceder a áreas restringidas de los Sistemas de Información.

Intentar distorsionar o falsear los registros de los Sistemas de Información.

Intentar descifrar las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos.

Poseer, desarrollar o ejecutar programas que pudieran interferir sobre el trabajo de otros Usuarios, o dañar o alterar los Recursos Informáticos.

Usos Prohibidos

La sustracción de equipos o periféricos informáticos, y/o cualquier otro medio de soporte de información son considerados un delito.

Está estrictamente prohibido el uso de cualquier recurso informático para: Grabar, modificar o borrar software, información, bases de datos o registros de la institución, que no estén incluidas como tareas propias del usuario.

Inferir cualquier daño a los equipos o a la información, las configuraciones de sistemas operativos o las aplicaciones que se encuentren en ellos instalados.

Acceder sin autorización a los sistemas de información de las diferentes áreas.

Revelar o compartir contraseñas de acceso, propias o de terceros, con otros usuarios así como el uso de la identificación, identidad, firma electrónica o digital de otro usuario.

Introducir en los Sistemas de Información o la Red contenidos obscenos, amenazadores, inmorales u ofensivos.

Utilizar cualquier sistema de correo electrónico o cualquier tipo de comunicación electrónica con el objetivo de dañar o perjudicar de alguna manera los recursos informáticos.

Lanzar cualquier tipo de virus, gusano, macros, controles ActiveX o cualquier otro dispositivo lógico o secuencia de caracteres que afecte el funcionamiento de los sistemas o dispositivos informáticos.

Impedir el acceso a otros usuarios mediante el mal uso intencional de recursos comunes.

Alterar, falsificar o de alguna otra forma usar de manera fraudulenta los archivos, permisos, documentos de identificación u otros documentos.

Violar cualquier ley o norma, respecto al uso de los sistemas de información así como realizar cualquier conducta ilegal contraria a la legislación aplicable de cualquier país al que se pueda tener acceso por la Red.

Responsabilidades de Jefes de Direcciones y Prefectura

La implementación de políticas de seguridad de la información debe contar con el completo apoyo del señor prefecto, pues sin esto sería más difícil su implementación e incluso podría resultar en fracaso la seguridad.

Los jefes de cada área son los responsables de implementar las políticas de seguridad, hacer que los usuarios entiendan y cumplan con las políticas de seguridad. Cada área cumple un rol importante en la seguridad de la institución.

Dentro de las responsabilidades están:

- Planeamiento de seguridad, revisión y aplicación.
- Asignación de roles y responsabilidades.
- Coordinar la implementación de la seguridad.

Director General provincial de la dirección de Sistemas

El Director General provincial de la dirección de Sistemas es el responsable conservar la documentación original y del mantenimiento de las políticas de seguridad. Además deberá tomar decisiones, si las políticas existentes satisfacen las necesidades de la institución, y de revisarlas por lo menos una vez al año.

Es responsabilidad del director confirmar que las políticas de seguridad han sido implementadas.

Talento Humano

Talento humano en conjunto con el señor Prefecto será el responsable de determinar las acciones disciplinarias acordes a la infracción cometida.

Concientización sobre seguridad y capacitación

El departamento de Tecnología será el encargado de organizar la capacitación del personal en temas relacionados a la seguridad de la información, con la autorización del señor Prefecto.

Plan y equipo de respuesta a incidentes

El Gobierno provincial de Tungurahua deberá tener un equipo de respuesta a incidentes establecido, con procedimientos y planes desarrollados para responder a incidentes de seguridad.

Seguridad física

La institución es responsable de implementar controles de seguridad física. Parte de la seguridad física es mantener un inventario actualizado de todas las instalaciones aprobadas para alojar servidores.

Control de acceso físico

Controlar y limitar el acceso a las instalaciones de procesamiento de información, exclusivamente al personal autorizado.

Ubicación y protección del equipamiento informático

El equipamiento será ubicado y protegido de tal manera que se reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y las oportunidades de acceso no autorizado, teniendo en cuenta los siguientes puntos:

Ubicar el equipamiento en un sitio donde se provea un control de acceso adecuado (puertas con cerraduras, ventanas con protectores, etc.).

Poner controles adecuados para minimizar el riesgo de amenazas potenciales por: robo o hurto, incendio, humo, polvo, vibraciones, inundaciones o filtraciones de agua, efectos químicos, radiación electromagnética, derrumbes, interferencia en el suministro de energía eléctrica (cortes de suministro, variación de tensión).

Mantenimiento del equipamiento informático

Sólo personal autorizado y calificado del área de tecnologías, puede dar mantenimiento y llevar a cabo reparaciones en los equipos y/o periféricos informáticos.

En el caso de que la reparación implique el formateo y/o reemplazo de disco rígido, se deberá realizar previamente las respectivas copias de resguardo, salvo en el caso de que dicho dispositivo se encuentre inutilizado, y sea imposible.

Copias de Seguridad de la información

Los responsables de las diferentes áreas dentro del área de tecnologías serán responsables de sacar respaldos de la información a su cargo, por lo menos una vez a la semana o cuando lo consideren necesario(si existen cambios significativos).

Los respaldos deben ser comprimidos (recomendado) y resguardados en dispositivos externos.

Resguardar los respaldos en un sitio externo a la Institución, fuera del lugar en el que se encuentren los equipos aplicando los estándares de calidad para el almacenamiento de medios magnéticos.

Monitorización

Los usuarios que utilicen equipos de la institución para acceder a la red e Internet están sujetos a ser monitoreados, en sus actividades por personal del área de tecnologías, autorizado a tal efecto. Esto se realizará a través de los mecanismos formales y técnicos que se consideren oportunos, ya sea de forma periódica o cuando por razones específicas de seguridad o del servicio resulte conveniente, con el objetivo de garantizar el correcto uso de los recursos.

La información personal del Usuario a la que se tenga acceso durante la monitorización de las actividades de control, mejor funcionamiento o seguridad, no podrá ser difundida públicamente excepto que se trate de un uso no autorizado, indebido o prohibido y a los estrictos fines de la sanción correspondiente a la falta cometida.

Sanciones

El incumplimiento o violación de estas "Políticas de Seguridad de los Recursos Informáticos", constituirán elementos de juicio para graduar las sanciones estipuladas en el Reglamento Interno del Honorable Gobierno Provincial de Tungurahua, así como las civiles y penales dispuesta por ley, y siempre que se considere pertinente.

Conectividad a Internet

La autorización de acceso a Internet se concede exclusivamente para actividades de trabajo. Por lo tanto todas las actividades que se realice en internet deben estar relacionadas con las tareas del trabajo a desempeñar.

Protección de datos de carácter personal

Todos los funcionarios están obligados a respetar la intimidad personal y familiar de todas las personas a cuyos datos tengan acceso, derivado de la actividad de la institución.

- **ÁREA DE TECNOLOGÍA**

Gestión de perfiles

Los perfiles de usuario deben ser creados de acuerdo a las los cargos del personal.

La creación, modificación o eliminación de perfiles únicamente pueden ser solicitadas dependiendo de la creación, rediseño de procesos, nuevas o cambio de funcionalidades, debe ser solicitado a través del sistema de tickets.

Todo perfil de usuario y su contraseña es responsabilidad de su “propietario”.

Seguridad de la RED

El área de tecnologías deberá mantener control permanente en la red, con el fin de estar protegidos de las amenazas y mantener la seguridad para los sistemas y aplicaciones, incluyendo la información en tránsito.

Controles de Red

El responsable de la administración de red, deberá implementar los controles necesarios para mantener la seguridad de los datos de la red.

- Toda la red del Honorable Gobierno Provincial de Tungurahua deberán estar configuradas y habilitadas a través de medios apropiados, me modo que puedan prevenir y/o detectar intentos de establecer conexiones o ingresos no autorizadas.
- Todos los dispositivos de la institución deberán contar con mecanismos de control y una configuración de seguridad de acuerdo a los requerimientos establecidos.
- No se deberá conectar ningún dispositivo externo a la red de la institución, a menos que este sea aprobado por el personal del área de tecnología.
- Toda conexión hacia el exterior debe hacerse a través del firewall.

Seguridad de Aplicaciones

Todas las aplicaciones se deben revisar periódicamente

- **Aplicaciones Comerciales/Estándar**

  Se debe realizar un escaneo en busca de vulnerabilidades en las aplicaciones que son adquiridas comercialmente.

- **Aplicaciones Desarrolladas por el área de tecnologías**

  Las aplicaciones que se desarrollen en la institución deberán pasar por un proceso de escaneo de vulnerabilidades antes de ser puestas en producción como de manera semestral. Adicional a esto se deberá la aplicación deberá ser revisada por una persona distinta a la desarrolladora antes de ser aprobada por el director general provincial de la dirección de sistemas del Honorable Gobierno Provincial de Tungurahua.

Seguridad de Servidores

Es responsabilidad del departamento de tecnología del honorable Gobierno Provincial de Tungurahua asegurar el acceso físico a los servidores. El acceso a los servidores debe estar controlado por usuario y contraseña, el cual debe ser asignado por el director del departamento de tecnologías.

Seguridad de Sistemas Operativos

Con el objetivo de minimizar riesgos, se deberá:

- La actualización de los sistemas operativos solo se podrá realizar por la persona designada por el área de tecnologías.
- El personal de desarrollo no podrá poner en ejecución ningún software sin la respectiva autorización.

- El acceso a los sistemas operativos deberá estar controlado por inicio de sesión con contraseña.

Seguridad de la información

Según la LEY ORGANICA DE TRANSPARENCIA Y ACCESO A LA INFORMACION PUBLICA, El acceso a la información pública es un derecho de las personas que garantiza el Estado. Por lo cual toda la información del Honorable Gobierno Provincial de Tungurahua, al ser una institución pública es de libre acceso.

Anexo B

Formulario de Incidentes de seguridad

Formulario de Incidentes de Seguridad			
Fecha	Hora	Número de incidencia	H. GOBIERNO PROVINCIAL DE TUNGURAHUA
Usuario que notifica			
Receptor de la notificación			
Descripción del incidente			
Tipo de incidencia			
() Intrusión		() Perdida de datos	
Otro tipo de incidencia (especificar)			
Descripción detallada del incidente			
Efectos en el sistema			
Notificante		Responsable de seguridad	
Firma		Firma	

Tabla B.1: Formulario de Incidentes de Seguridad

Anexo C

Formularios de Incidentes de seguridad

Formulario de intento de escaneo a uno de los usuarios

Formulario de Incidentes de Seguridad			
Fecha 14/04/2016	Hora 16:10 pm	Número de incidencia 01	H. GOBIERNO PROVINCIAL DE TUNGURAHUA
Usuario que notifica		Ing. Dario Morales	
Receptor de la notificación		Alexandra Pineda	
Descripción del incidente		Alerta del antivirus Port scan attack logged	
Tipo de incidencia			
() Intrusión		() Perdida de datos	
Otro tipo de incidencia (especificar)			
Intento de escaneo de puertos			
Descripción detallada del incidente			
el antivirus bloqueo el escaneo de la IP 172.16.1.243 (Fecha 14/04/2016 15:47:43)			
Efectos en el sistema			
Ningun efecto por detección oportuna del antivirus			
Notificante		Responsable de seguridad	
Firma		Firma	

Tabla C.1: Formulario de Incidente de Seguridad en equipo de la red

Formulario de ingreso al servidor apache tomcat

Formulario de Incidentes de Seguridad			
Fecha 14/04/2016	Hora 15:06	Número de incidencia 01	H. GOBIERNO PROVINCIAL DE TUNGURAHUA
Usuario que notifica		Ing. Mario Torres	
Receptor de la notificación		Alexandra Pineda	
Descripción del incidente		Acceso no Autorizado a Tomcat	
Tipo de incidencia			
(x) Intrusión		() Perdida de datos	
Otro tipo de incidencia (especificar)			
Descripción detallada del incidente			
Acceso no autorizado a tomcat desde la IP 172.16.1.232			
Efectos en el sistema			
Navegación dentro de las características de Tomcat			
Notificante		Responsable de seguridad	
Firma		Firma	

Tabla C.2: Formulario de incidente de seguridad en apache tomcat